Work Type	Subreddits examined	Posts collected	Posts coded	Relevant posts
Crowdwork	r/mturk	208	208	90
Freelancing	r/upwork	229	229	111
Ridesharing	r/lyftdrivers, r/uberdrivers	864	229	185
Delivery	r/doordash_drivers, r/postmates, r/shiptshoppers, r/grubhubdrivers, r/instacartshoppers, r/ubereats, r/amazonflexdrivers, r/couriersofreddit	1,388	229	106
Total		2,689	895	492

Table 1: Subreddits examined for each type of gig work, along with posts collected, coded, and coded as relevant.

Because online platforms change rapidly [15], we excluded posts submitted before 2018 to capture discussions that are more likely to reflect current platform designs. We also omitted posts that were deleted or removed, AutoModerator posts, and duplicate crossposts. This led to a dataset containing 2,689 Reddit posts representing 12 subreddits from 1/1/18 to 7/26/20, as shown in Table 1. Data were collected using the third-party Pushshift Reddit API [4] in 2020 when all three authors were at Cornell University.

3.2 Analysis

We used an inductive, qualitative approach to explore our dataset, drawing on principles of grounded theory [66]. The analysis was conducted by three researchers with varying degrees of experience observing activity on gig work subreddits prior to beginning the study (ranging from zero to four years).

Upon exploring our dataset, we found that some posts were not related to privacy or surveillance; for example, the search term "mic" returned several posts using the idiom "mic drop". Thus, we developed inclusion criteria to filter posts; posts were considered relevant to the analysis if (a) the post author indicated that they were a gig worker and (b) the post discussed a privacy- or surveillance-related worker concern, behavior, tool, or consequence. To check that we were not inadvertently excluding relevant posts, we independently coded relevance for 50 posts each, and measured inter-rater reliability (IRR) using Fleiss' Kappa, a measure for IRR between multiple coders for categorical data [22], which indicated that we had strong agreement (Fleiss' Kappa = .77).

Once we were confident we had a strong shared understanding of what constitutes inclusion in our dataset, we began the process of independently open coding our data. We analyzed posts separately according to work type, using the constant comparison method to compare similarities and differences between work types for each concept that emerged [11]. The open coding process revealed a range of privacy and surveillance issues across platforms.

Then, through axial coding, we collaboratively identified connections between concepts and broader categories, drawing on Corbin and Strauss' Coding Paradigm that defines a number of categories to understand a phenomenon, including causation, strategies, and consequences [11]. Based on these rounds of coding, we established a codebook that reflected the conceptual categories in our data; we used the codebook to apply focused codes to relevant posts. We did not calculate IRR when identifying and coding the concepts in our data, as IRR is rarely needed for inductive approaches informed by grounded theory [51].

We met regularly to discuss themes in the data and assess whether we were approaching theoretical saturation. After several rounds of coding and iterative updates to the codebook, we reached saturation, i.e., coding additional posts reinforced earlier findings and no new concepts emerged. Overall, we coded all posts on crowdwork (N = 208) and freelancing (N = 229), and a similar number of posts in ridesharing (N = 229) and delivery (N = 229) for a total of 895 unique posts across contexts. Of these, we classified a total of 492 posts as related to privacy and surveillance, and thus relevant to our analysis; these formed the basis for the themes we report below.

3.3 Ethical Considerations

Since this study is based on publicly available online posts, Cornell University's IRB deemed it to not constitute human participant research as defined by U.S. federal regulations. However, there are still potential harms from using public online data [59]. Thus, we considered harms that could emerge from collecting, analyzing, and publishing these data, drawing both from our IRB's resources for working with publicly available data and discussions of Internet research ethics and best practices [16, 47]. While most of our data are not particularly sensitive, workers occasionally described potential violations of recording laws or a platform's terms of service, and we also felt it important to maintain workers' anonymity.

Thus, we took the following steps: (1) we do not include usernames or other identifying information in the paper, (2) we do not provide quotes for particularly sensitive cases, and (3) we paraphrased all quotes to reduce the searchability of the source posts. We did this as the final step after the data had been analyzed and the paper had been written, to ensure the reporting of our findings followed the original data as closely as possible. Our paraphrasing largely constitutes surface-level changes such as using synonyms, changing word order, and the like, in order to preserve the authors' meaning. To validate the process, one author paraphrased all quotes while a second author independently reviewed the paraphrased and original quotes to ensure that meanings were preserved, and iterated on the paraphrasing as needed.

3.4 Limitations

Although collecting data from Reddit forums has many benefits as discussed earlier, it also raises some limitations. For instance, the analysis does not include workers who don't participate in the forums, including workers who do not know about them, who participate in forums outside of Reddit, or who have left the market entirely. It also focuses on the kinds of concerns and strategies that workers are likely to express in these forums. We also did not analyze comments, given our interest in the types of issues being raised by posters, and not necessarily how the community responded to them. A future analysis of comments might reveal new dimensions around the issues identified in this paper.

Our choices of forums and keywords also likely miss at least some parts of the story. Although we captured a variety of common types of gig work, some job types (such as charging electric bikes) were too niche to have large, active online forums; this was also true of household services such as TaskRabbit and Handy. As a result, we excluded some of these smaller, less active subreddits, though understanding the privacy implications of these specific platforms (and household services more broadly) is a potential avenue for future work. We also tried to have a wide range of privacy and surveillance-rated keywords, but still likely missed some posts addressing concerns or strategies we did not encounter.

4 FINDINGS

We start by describing the types of posts workers made when discussing privacy and surveillance issues, followed by two sections that explore the challenges faced by workers that stem from platforms and customers as surveillance agents, respectively. Then, we turn our focus to workers' responses to these challenges, including their self-protective surveillance strategies. Findings we report below are based on codes and themes that occurred frequently in the dataset. Each quote is labeled with an abbreviation that denotes its work context (CW = crowdwork, FL = freelancing, RS = ridesharing, and DS = delivery services) and the post's row in our dataset.

4.1 Discussing Privacy and Surveillance Online

4.1.1 Seeking advice. Across gig types, workers turned to the forums to ask for advice about privacy and surveillance-related matters. Many questions were a reaction to a specific privacy-concerning situation, as with this crowdworker's question about the risks of a specific job (jobs are called Human Intelligence Tasks, or HITs, on MTurk): *"I'm clicking the recording button but it won't stop recording during this HIT. Is this normal? Or is the requester a creep who wants permanent access to my webcam? I'm scared because I don't know how to complete this HIT, please help!"* (CW 33).

Beyond reacting to incidents, workers also turned to the forums for proactive privacy advice. New workers sometimes asked fairly general questions, as with this one from a beginning freelancer: *"I'm looking at the time tracker desktop app and it seems kind of intrusive! Do I need to look out for anything?"* (FL 216). More often, proactive questions focused on the risks of specific actions: *"Should I be providing my ID during HITs? Do requesters already have my ID, I'm not sure. I don't know how much personal information I should leave out and how much requesters actually need to know"* (CW 171).

Workers also asked others to comment on privacy and surveillance strategies they were considering, as with this ridesharing driver: *"Does anyone use any virtual debit cards for privacy when using Uber's instant pay cash out? I tried to use one but unfortunately it failed when I tried to cash out"* (RS 46).

The questions above focused on *practical* advice grounded in individual workers' experiences. Workers also often sought *prescriptive* advice, trying to assess broader community opinions and best practices on risks (*"Does downloading software to complete HITs worry anyone else?"* (CW 130)) as well as strategies (*"Will using airplane mode prevent my speed from being tracked?"* (DS 212)).

4.1.2 Giving advice. Posts that gave advice also had the reactive-proactive, general-specific, and practical-prescriptive dimensions described above. Further, the kinds of advice workers gave was influenced by their degree of choice around which jobs to do. In crowdsourcing and freelancing platforms, where workers can often choose their customers, advice tended to focus on specific concerns about particular customers, as illustrated by the following warning:

> *"I advise you all to avoid these HITs if you can. It looks like one person posting HITs using several requester names including [redacted names]. Clearly something sketchy is happening and when sketchy people are successful on MTurk, it encourages them."* (CW 22)

They also shared information about customers who wronged them: *"I've done thousands of deliveries, but this one was the worst. Be careful since one angry customer can ruin everything"* (DS 63).

In ridesharing and delivery services, which typically give workers limited ability to choose customers, advice tended to be about proactive, general privacy strategies, such as the following solution shared by a delivery worker: *"Here's a workaround to prevent the app from accessing your contact info: run a clone of it inside [a different app] that allows it to request permissions but then gives it blank data"* (DS 118). We discuss these privacy-protective behaviors in more detail in Section 4.4.

4.1.3 Venting and commiseration. Some posts served mainly as a way for workers to vent about privacy issues, and many advice-seeking and advice-giving posts also had a healthy dose of commiseration, as with this post about the need to protect against scammy customers: *"Sick of passengers claiming they paid in cash when they didn't. This is why I use a dash cam"* (RS 128). Some posts were characterized by a caustic sense of humor, where workers shared examples of particularly egregious issues. For example, a crowdworker posted a screenshot of an MTurk task that asked for "1 hour of video of baby in crib or sleeper", along with the following commentary: *"BEST EVER VIOLATION OF TERMS OF SERVICE? GIVE UP YOUR BABY'S PRIVACY FOR TWENTY BUCKS"* (CW 136).

Together, these observations about advice-seeking, advice-giving, and venting behavior paint a high level picture of how gig workers discussed privacy and surveillance issues in the forums. We now discuss in more detail the specific concerns and strategies that workers raised. Following high level themes in our codebook, we divide the concerns between ones that arose primarily from platforms (4.2) and those that arose primarily from customers (4.3), and the strategies between ones focused on privacy-protective behaviors (4.4) and self-surveillance (4.5).

4.2 Platforms as Surveillance Agents

Platforms do have legitimate interests in validating workers' identities and verifying that they are doing the work efficiently and effectively, which requires some data collection and tracking . However, platforms' policies and applications often collect more data than workers were comfortable with. Across gig work contexts, workers had privacy concerns stemming from the amount and appropriateness of personal identifiable information that platforms require during both sign-up and the work itself, and the ways platforms could surveil them.

4.2.1 Questions about necessity, intrusiveness, and appropriateness of data collection. Workers often called out data collection that felt unnecessary, intrusive, or inappropriate with respect to the job. For instance, MTurk workers who want to be paid through a bank account rather than Amazon gift cards are sometimes required to disclose deposit and withdrawal history for the account, which felt excessive for establishing a payment method:

> *"Trying to connect my bank account to Amazon Payments, but I'm concerned about what they're requesting. I submitted just the top of my bank statement but they rejected it. I'm not comfortable sharing all the details of my spending. Do I have to share a picture of my entire statement?"* (CW 37)

Repetitive and intrusive identity verification also raised concerns, especially given how much information companies already collect:

> *"Upwork verification seems excessive. Constantly asking for video calls for no reason and blocking my account if I don't comply. They have my passport, driver's license, bank information, picture, email address, video calls, and excellent client reviews. I'm losing my confidence. We deserve more respect."* (FL 207)

4.2.2 Questions about data and device security. Workers also raised questions about companies' ability and desire to secure their data, and about the risks of granting various device permissions requested by platform apps.

Workers expressed mistrust that platforms *could* and *would* keep their data secure, given media reports about security breaches and misuse of customer data: *"If customers' data is being sold online, how secure do you think ours really is?"* (DS 184). Privacy policies were also not convincing on this score:

> *"Upwork is asking me for a bank statement or credit card and a photo of my government ID. Seriously? There's nothing on their Privacy Policy page that gives me any confidence they'll keep my data secure, and I have no trust in them to do so."* (FL 17)

Workers also took exception to unexplained requests for device permissions. Upwork raised red flags for several different types of requests, including permissions for audio, video, and settings on workers' personal devices: *"Does it sound normal for Upwork to request access to my computer's privacy and security settings? I haven't used the app for a while, but I don't remember this"* (FL 2).

4.2.3 Concerns about covert and overt surveillance. Permissions were the tip of the iceberg when it came to platforms that require workers to install apps (typical in freelancing, ridesharing, and delivery services, but not crowdwork). Workers were concerned about being spied on and tracked through the apps, and used the forums to theorize about the platforms' surveillance activities.

Particularly in ridesharing and delivery jobs that took place offline and required installing mobile apps, workers wondered whether the platform apps could be running in the background and covertly collecting data at all times:

> *"Conspiracy theory time! What if Lyft is spying on us? It would be so easy for them to do that. They have access to the mic and camera on our phones so I'm sure they could snoop on us if they want to."* (RS 65)

These theories were sometimes backed by strong circumstantial evidence, such as location tracking notifications while apps were closed, high battery consumption, and alarming data usage: *"After allowing access to my phone's storage, my mobile data was immediately maxed out"* (DS 16). A particularly concerning case occurred when a platform suggested that a worker log in while they were using a competing platform. This felt like a violation of boundaries:

> *"I don't have an issue with occasional suggestions to start working. I do have an issue with GH tracking my location even when I'm offline and don't have the app open. It's a disrespectful use of my data. It's clear that they're tracking my location, detecting I'm working for their competition, and responding to that."* (DS 8)

The prior concerns focused on covert surveillance, but even open and transparent surveillance sometimes raised issues. As noted before, expected-but-repetitive identity verification was seen as intrusive and risky. Workers also speculated that platforms were deliberately harvesting personal information ancillary to the job through features such as Upwork's time tracker:

> *"I think they're spying on us! Us personally, not only the work we're doing. Upwork always seems to be taking screenshots exactly when I'm accessing sensitive or personal documents, like logins and passwords. Does this happen with anyone else?"* (FL 199)

Although it is not clear to what extent these theories about platform privacy, security, and surveillance are actually the case, they indicate concerns that workers feel based on how the platforms are designed and how they communicate about these issues.

4.3 Customers as Surveillance Agents

Customers, like platforms, have legitimate goals that might require some personal information about workers. Knowing a driver's first name to support social interaction, knowing when a delivery or pickup is likely to happen, checking that a crowdworker is attentively completing tasks, and being able to verify that hours billed by a freelancer are project-related are all things customers might reasonably want and that workers might reasonably provide.

However, customers sometimes ask for additional information, and the design of gig platforms often reveals a good deal of both workers' personal information and fine-grained tracking data to customers. Thus, workers also had privacy concerns about customers stemming from direct and indirect requests for unnecessary personal information and from asymmetrical monitoring.

4.3.1 Questions about necessity, intrusiveness, and appropriateness of requests for personal information. Customers often asked for personal information beyond what was necessary for the task. For instance, some delivery and rideshare customers want a level of social interaction that made some workers uncomfortable:

> *"Just dropped off a large order and the customer started asking me about Instacart and if I have another job before I could leave. It was annoying and intrusive, but because we work for tips and ratings I was polite and answered his questions."* (DS 129)

Other customers, however, asked for task-irrelevant information as a condition of work, and sometimes did not disclose this in advance. This led to negative consequences:

> *"My client told me that they won't pay until I sign an NDA and submit a photo ID, which I don't want to do because of privacy reasons. I wouldn't have worked for them if I knew they required this, but they didn't mention it before I started."* (FL 91)

Even when requested information was germane to the task and disclosed up front, workers sometimes wondered whether the information might be used for unrelated nefarious purposes:

> *"The HIT requires all of your personal info like your full name, email, address, and even what schools you attended. The requester says the info is used to improve people search. But with all this info, it's easy for him to pose as you for identity theft, or sell your information on the dark web, or make a fake ID."* (CW 16)

4.3.2 Concerns about asymmetry and transparency of platform data sharing. Platforms often provide customers with unnecessary information about and access to workers, with minimal transparency and in ways inconsistent with reasonable worker expectations. For instance, a delivery worker noted that customers can track workers even before they pick up the food: *"A couple of customers recently suggested that they were able to track me before I arrived at the restaurant. Am I crazy or has anyone else heard of this?"* (DS 127). As long as the driver is there when the order is ready for pickup, details before that are not so relevant to the task.

Similarly, how platforms manage customer-worker communication was not transparent and sometimes inconsistent with norms. Rideshare platforms allow drivers and customers to call each other while a ride is active to support coordination. However, sometimes customers were able to call drivers well after the ride: *"Just got a call from a passenger twelve hours after the ride ended. How did Lyft manage to connect us? What the hell happened? This is concerning for privacy and security, etc."* (RS 143). While this was possibly a technical glitch rather than a design decision, this case highlights the uncertainty workers have about customers' access to them.

Finally, power asymmetries between customers and workers are sometimes reproduced even in the sharing of personal information, as noted by this driver: *"Did you know that Uber discloses your full name to customers? Drivers only get the first name and last initial of customers, so this feels wrong"* (DS 210).

4.3.3 Consequences of over-tracking. When platforms give customers surveillance powers that are not needed for the task, either because they are not relevant or because they are overly fine-grained, workers can suffer the consequences. For instance, irrelevant data can be used to make erroneous inferences. A canonical case in crowdwork is when requesters decide to reject work done "too quickly", assuming that this means the worker did a poor job. This can penalize efficient workers:

> *"The requester rejected it because she said that I completed the survey in under 10 minutes, and so the quality of the work is questionable. But I passed every attention check and there wasn't anything in the study that was difficult to understand."* (CW 87)

Further, it's often not clear to workers how customers use the surveillance tools at their disposal. On Upwork, workers were acutely aware that clients can monitor them using Upwork's time tracker feature, which captures screenshots of workers' screens every 10 minutes, along with keystrokes, scroll actions, and mouse clicks. Workers can opt out, but then Upwork doesn't guarantee payment for tracked hours. This raises difficult choices in balancing job security against surveillance that are made harder because there is a lack of transparency around the tracker and its use:

> *"I'm curious about the time tracker taking screen shots, recording mouse clicks, tracking key strokes, etc. Is there a way to see whether my client has viewed my screen shots and which ones they've seen?"* (FL 150)

Overall, many concerns workers had about privacy and surveillance by customers boiled down to data transparency: what is collected, what it can be used for, when it is actually used, and how it impacts customers' evaluations of workers.

4.4 Workers' Responses to Privacy and Surveillance Challenges

These concerns lead workers to adopt many strategies to navigate challenges around privacy and surveillance. In this section we discuss privacy-protective strategies, their costs and difficulties, and the positive and negative consequences of adopting them.

4.4.1 Assessing, Avoiding, and Abandoning Risky Customers and Tasks. Many workers vet customers and tasks in crowdwork and freelancing platforms where they have choices about their work. Turkopticon, where Turkers rate and review requesters, is a popular vetting tool: *"Some requesters are just trying to get free data or not pay. You can mostly figure this out by looking at their Turkopticon ratings"* (CW 21).

Not all risks can be assessed up front, however. In these cases, some crowdworkers abandon invasive tasks partway through, resulting in lost wages through invisible labor [64]:

> *"I've tried at least five HITs that have all had serious terms of service violations just in the past few hours. It's so frustrating wasting time on these. One even asked for my social security number. Others didn't ask for my personal info until I had spent several minutes on them. So much time wasted."* (CW 126)

Unlike crowdwork, where there is generally no way to negotiate task requirements, freelancers were more likely to discuss issues with clients instead of abandoning tasks, reducing the risk of abandoned work but still requiring compromise and invisible labor:

> *"The time tracker app is the only way to guarantee hourly payment, but it's a hassle to use effectively. I suggest avoiding it if you can. You really have to be*

> *'on' for every minute since it takes screenshots of your work. For clients who've wanted it, after tracking ten to twenty hours of work, I've requested manual time instead with my reasons. They've all agreed without disputing hours, but I realize this is risky."* (FL 229)

4.4.2 Withholding or Obscuring Personal Information.

Both online and offline workers used withholding and obscuring strategies to navigate challenges around personal information. While some crowdworkers completely withheld such information, others used "privacy lies" [63] to complete invasive tasks without losing out on wages: *"For HITs asking to create a unique code with your name and date of birth, I never use my real information but it freaks me out. Seems super shady"* (CW 118). Privacy lies were also a common strategy in ridesharing to prevent customer dissatisfaction or retaliation; some drivers described creating entirely "false personas" to respond to uncomfortable questions from passengers to avoid jeopardizing their ratings and tips.

When faced with challenges around personal information from platform companies, some workers took more extreme measures to obscure their personal information, such as using stock images as profile photos and fabricating government IDs for verification purposes. Some who did this were worried about being eventually caught, but felt caught up in the lie and unable to rectify it by providing the correct information. This left them at risk of losing established accounts that they had used to earn significant amounts of money.

Others considered quitting platforms that required sensitive personal information:

> *"I'm going to have to stop using Upwork. They want me to connect my PayPal and they're asking for pretty personal data, and I'm not going to give it to them, so they'll put my account on hold... but now my issue is that I currently have a contract in progress, and Upwork could take my money hostage."* (FL 211)

These quotes show some limitations of privacy lies: they require deception, which some workers find uncomfortable or unacceptable [63], and which leave workers vulnerable to detection and reprisal from customers and platforms.

4.4.3 Using technology to reduce surveillance risks.

A third set of strategies revolve around using technology to reduce both platforms' and customers' ability to surveil workers. Some online workers used VPNs to make it hard for platforms to trace their devices, identities, and information—though as with deception, they worried that these measures might lead to reprisals:

> *"I've been using a VPN since I'm concerned about keeping my personal info safe. I haven't had any issues, but I'm worried my account will be suspended and all my time and effort will be for nothing."* (CW 125)

Offline workers sometimes modified device settings to prevent platforms from accessing information outside of work hours: *"My phone notified me that the app was trying to access my location even though it wasn't even open. So I changed the settings to only allow location tracking while the app is in use"* (DS 134). However, changing these settings is labor-intensive and inconvenient, particularly for settings that must be toggled for every work session:

> *"I noticed that when I'm signed out of the app, the Location Services icon on my phone stays on, indicating the app is still tracking my location. I can turn it off manually by going into my phone settings, then clicking 'location', then 'Uber driver', then 'permissions' and then turning the location sharing off and back on, though it's a nuisance to do each time. But it's still better than being tracked all the time."* (RS 72)

Workers also used platform features to reduce their availability to customers, reducing the chances of interruptions or intrusion: *"I keep Upwork on in the background when I'm working on other projects. But I set my chat status to offline since I don't want clients thinking I'm always available to talk"* (FL 83).

4.5 Self-Protective Surveillance in the Face of Unequal Power Dynamics

Thus far, we've talked about surveillance when it is a problem for workers. However, we found that workers sometimes also use their own forms of surveillance as a protective strategy against both platforms and customers.

4.5.1 Protection from platforms.

Workers often engaged in self-surveillance by tracking their work, in terms of hours worked, tasks completed, miles driven, and so on. This helped them maintain an accurate picture of their earnings and expenses (for themselves and for tax purposes). It also gave them evidence to contest pay discrepancies and ensure they received appropriate compensation:

> *"I'm tired of constantly monitoring my earnings and tracking every payout all because I'm working with a very untrustworthy company. When you're missing pay, you have to provide them with a detailed account for them look into the issue (but that's if you're smart enough to monitor all your earnings)."* (DS 71)

These discrepancies could arise when platforms' trackers did not match workers' own experience of the work:

> *"We all know that the time tracker on Upwork doesn't always log time correctly. I measured it recently. I switched it on for 4 hours but the tracker only recorded 2.5. My internet connection was stable and I spent all 4 hours working. Of course I didn't tap on the keyboard the entire time. I only wrote code after thinking through problems. That's typical for a programmer."* (FL 15)

Tracking one's own work, though, imposes additional invisible labor that could interfere with the work itself and require investing in external tools:

> *"I don't trust Uber's mileage tracking based on my experience and reviews on this forum. They use a lot of trickery and disclaimers in their propaganda so I can't take their word for anything. I'm buying a good mileage tracker next year to double check because scribbling notes by hand at red lights is impossible."* (DS 224)

Together, these concerns about platforms failing to compensate workers fairly, accurately, and transparently led to the frustration and lack of trust expressed in the quotes above.

4.5.2 Protection from customers. Workers also used surveillance to protect themselves against customers. Just as delivery and ridesharing workers documented their work to resolve pay disparities with platforms, online crowdworkers and freelancers often *"go into evidence collection mode"* (FL 12) around their work activities. They discussed using tools outside the platform itself to protect themselves in pay disputes with customers:

> *"Here's a tip: Don't be afraid to take screenshots, save webpages, and take notes about long surveys that pay a lot or you have a funny feeling about. Copy stuff into a Word document. Save everything. I have a folder with all of this and hope I never need it, but I can't tell you how many times it's saved me when it comes to rejections. It's been incredibly useful and definitely worth the time."* (CW 21)

Delivery drivers also used self-surveillance to protect against customers who falsely claimed the job wasn't done:

> *"I saw a post about using dashcams to prove you've delivered an order that a customer later said you didn't. Thanks for the tip! I just used my dashcam footage to prove the same thing. I also texted the customer and left a voicemail about it."* (DS 23)

Beyond individual customers, workers also self-surveilled their work and pay to decide how concerned they should be about different aspects of customer payment, as demonstrated by this case of promised but undelivered bonuses for completing tasks in MTurk:

> *"How long does it take to get bonuses that have been promised to us? I recently started some tracking. Out of 31 studies that promised a bonus, I've only received payments for 11, and it's been three weeks."* (CW 141)

Workers didn't just surveil for their own benefit; as described earlier, they would share their observations on the forums, often pointing to Turkopticon and Upwork profiles to tell other workers about risky customers. This public monitoring helped protect the gig worker community from wrongfully rejected work and other risks such as identity theft.

In driving gigs, where customers often enter a worker's personal space, drivers surveilled customers as well as themselves. Dashcams were key to this surveillance, protecting workers against risks such as claims of theft:

> *"Having a dashcam is awesome! A passenger said she lost some expensive jewelry in my car. So I looked up my recording. Saw that she wasn't wearing that jewelry when she got in my car. The end. Has anyone else had a passenger make a false claim about a lost item and try to pin it on them?"* (RS 114)

Dashcams are also seen as a way to dissuade unruly passengers and to provide evidence to platform support teams when reporting customers' bad behavior or refuting allegations of bad behavior:

> *"A passenger spilled his drink in my backseat. I heard him open the drink and curse when it spilled. So later I took photos of the mess and filed for a cleaning fee, but then I got a message that the passenger had submitted a complaint about me driving unsafely. So I looked up my dashcam footage and submitted some screenshots...Next thing, I get an email saying the passenger has been suspended from the platform."* (RS 55)

Choosing and using dashcams, however, demands effort. Drivers asked many questions about the mechanics of using dashcams, including recommendations about which dashcams were best, installation issues, ways to repurpose phones as dashcams, best practices around archiving, using, and sharing dashcam data, and legal considerations around recording customers. All of these impose invisible labor on drivers that is compounded by the cost of dashcams: *"I DO NOT want to shell out a hundred bucks, or anything close to it, for a dashcam. I thought dashcams were a luxury, but no, now I realize that if you're a driver you NEED to own one because Lyft is not going to be there for you if anything bad happens"* (RS 18).

Beyond mechanics, drivers also discussed customers' opinions of dashcams. This was especially important because using dashcams could lead to negative customer evaluations:

> *"A couple of passengers got really upset and raised their voices at me for having a dashcam. One guy said things like, 'This is America and I have a choice over whether I'm recorded. What the hell is your problem? Don't you want to make money?' And then his friend threatened to give me a negative rating."* (RS 24)

Despite these costs, drivers saw dashcams as an important tool not just for resolving disputes but also for improving safety:

> *"Being a young, female Uber driver in a big city has its risks. Last weekend, late at night and in the middle of nowhere, this passenger really creeped me out. He kept asking me questions to try to figure out if I had a dashcam. I don't have one, but I pretended that I did. Now I keep a pocket knife in my car and I'm trying to work out the Share Trip safety feature."* (RS 63)

Beyond dashcams, offline workers considered other kinds of surveillance to protect themselves. Uber and Lyft provide some features such as the ability to share location with friends and family in case of trouble. However, the platforms elide route details to protect passenger privacy, leading some workers to look for off-platform solutions that would allow trusted others to look out for them in case anything happened:

> *"I'm afraid for my life. But I have a plan. I've set up a discreet tracking app that gives my whole family full location access. I also set up a hidden dashcam. So if anything bad happens, I'm covered."* (RS 135)

Another worker, frustrated and worried by passenger allegations that they were driving under the influence, considered using a breathalyzer to test themselves for alcohol use as an even more intrusive form of self-protective surveillance:

> *"I'm thinking about getting a breathalyzer and recording myself using it with my dashcam every time I get in the car. Then there won't be any loopholes when it comes to false accusations from customers. Investing in this setup will take a day of work, but it could save me later on. Drivers have to protect themselves because the companies won't."* (RS 44)

5 DISCUSSION

We now consider the implications of our findings for our three main research questions around (1) advancing knowledge of gig workers' experiences of privacy and surveillance, (2) understanding what workers do in the face of those experiences, and (3) understanding how the design of gig work platforms, policies, and power dynamics affect both the issues workers experience and their ability to manage them, based on key concepts that emerged from our findings.

5.1 Advancing Understanding of Gig Workers' Privacy and Surveillance Experiences

One of our main contributions is to address the open calls for research on privacy and surveillance risks in the gig economy writ large [68]. We find that these risks are unfortunately numerous and cross platforms:

- Invasive, repetitive identity verification, as described by freelancing, ridesharing, and delivery drivers.
- Excessive surveillance induced by overzealous permission requests and platform apps running in the background on workers' devices, further blurring work/home boundaries as described in digital surveillance work [54].
- Exposure of unnecessary personal information to customers, including worker IDs in crowdwork [41], excessive ability to contact drivers in ridesharing, screenshots taken without warning in freelancing, and gratuitous location data in delivery gigs.
- Risks of customers demanding personal information from workers. In crowdwork, many tasks involve sharing personal data [64, 75]; in freelancing, providing personal information could be a post-hoc condition for being paid; in ridesharing, customers have sometimes innocent but sometimes threatening conversations about drivers' personal lives.
- Risks around inappropriate use of personal data, such as evaluating workers unfairly based on time taken (crowdwork), interpretations of work tracking diaries (freelancing), or location (ridesharing and delivery), as well as concerns about the potential for identity theft.
- Risks of personal data being sold to or stolen by third parties, a theme previously identified in the context of crowdwork [64, 75] and that we saw across all platforms.

Most notably, workers' posts show that they experience surveillance and accompanying privacy risks from both the platforms themselves and the customers they serve, though the relative degree of concern varied based on the design of the platform and the nature of the gig. The more directly the worker interacted with the customer, the higher the sense that the main privacy threats came from customers rather than the platform itself. For instance, delivery drivers, who often have minimal interaction with customers, tended to see platforms as the primary source of concern. Crowdworkers, on the other hand, rarely described privacy concerns arising from the platform because their main interactions are with customers who design the task requirements that cause privacy and surveillance risks [64]. Meanwhile, freelancers and ridesharing drivers expressed serious concerns about both platforms and customers, likely because these work contexts share two key characteristics: intrusive tracking by the platform software that plays a central role in the work, and the potential for high customer engagement and demand for information.

Calling this dual privacy threat out is an important addition to critiques of the role played by customers in the gig economy. These critiques identify customers as part of a broader system of digital management, overseeing workers' job performance with wide discretion [62, 65]. Our observations show that not only do customers perform a managerial role in the gig economy [65], but in doing so, they also engender *new* privacy threats and work-related risks for workers. Our data revealed that many platforms provide customers with access to fine-grained metrics about workers' performance including indirect performance indicators such as screenshots, time spent on tasks, and location traces. These findings highlight the need for researchers, designers, and policy-makers to not just scrutinize work platforms but also the power they afford to customers, and the repercussions of these decisions.

5.2 Self-Protective Surveillance: A Necessary Response to Imbalances in Power

Next, we reflect on our findings around our second question, about how workers respond to these concerns. Workers used a number of strategies, including careful vetting of gigs and customers (when platform designs and gig descriptions make this possible), privacy protective behaviors such as withholding or lying about personal information, and technical tools ranging from privacy settings to VPNs. As with our findings around risks, many of these observations are not entirely new, having been described in other work on privacy protective behaviors both in particular gig platforms (e.g., [41, 55, 60, 64, 75]) and more generally around privacy requests when online (e.g., [63]). Still, our findings add evidence toward the pervasiveness of these strategies, demonstrating their use across both different sources of surveillance and a variety of platforms.

We were more surprised to see how often workers described using surveillance practices to protect themselves from risks. We know from prior work that ridesharing drivers use dashcams to record rides for two main purposes: (1) to resolve potential customer disputes with the platform, and (2) to protect their physical safety by having a visual marker that deters customer misbehavior [2]. Our findings suggest that this behavior is part of a much wider set of practices around what we call *self-protective surveillance*, which includes elements of both sousveillance [45] and self-surveillance [49] and is pervasive across the gig economy.

While surveillance involves a hierarchical structure where a dominant power keeps watch over a relatively vulnerable individual or group, *sousveillance* occurs when the vulnerable attempt to counter this power dynamic by watching the powerful [45]. In the context of the gig economy, we saw several instances of sousveillance that occurred in response to *customer* power. By using dashcams to record passengers and delivery customers, workers who drive are often able to push back against customers who unfairly evaluate their work performance based on the surveillance capabilities platforms give customers. Similarly, by aggregating reviews of customers in a shared repository such as Turkopticon [30], crowdworkers can use collective surveillance [71] to develop customer profiles to protect themselves and their community against bad actors.

Workers' ability to surveil platforms to keep them accountable is much more limited. We contend that this dynamic encourages workers to engage in *self-surveillance*, i.e., when people monitor some aspect of their own activities [49]. Research has examined how self-surveillance can help people optimize various aspects of their lives (e.g., [42, 50]), though even this self-tracking can raise privacy issues [35]. Moore observes that self-surveillance can also be a response to precarious work conditions [53]; in our findings, we saw workers tracking their work to contest inaccurate platform time trackers as well as customers' promised but often-unpaid bonuses. Workers also used dashcams to not just record customers but to record their own behavior, allowing them to contest customer complaints. In this way, self-surveillance is one of the few ways workers can maintain a check on both platforms and customers.

Together, these practices of sousveillance and self-surveillance allow workers to protect themselves against power exerted by both customers and platforms acting as surveillance agents, defending themselves against a wide variety of risks. However, self-protective surveillance practices are burdensome and costly. In prior work, Sannon and Cosley show that privacy management on Mechanical Turk imposes a large amount of invisible labor that workers must shoulder [64]. Dashcams also pose costs, both in terms of the cost of the camera itself and the potential for negative customer responses that may impact drivers' ratings, leading some drivers to forego dashcams even when they are aware of the benefits they offer [2].

Our findings show that many self-protective surveillance strategies impose costs around time, effort, wages, customer perception, and even safety, which adds to the invisible labor already rife on these platforms [64, 70]. Further, almost every effective example required workers to use tools outside the platform. The tools that platforms do provide for self-protective surveillance were not well-trusted; Upwork's screenshotting time tracker was a notable source of serious privacy concerns, while Uber's feature for sharing location with trusted third parties was unfit for guaranteeing safety because it intentionally obscured locations and omitted route information (ironically, in the name of protecting *customer* privacy).

This lack of platform support for self-protective surveillance is part of a more endemic problem in platform design. We argue that workers are compelled to shoulder the burden of both privacy-protective behaviors and self-protective surveillance out of necessity, because the ways platforms are designed and structured leave them few other options for protecting themselves from potential risks or seeking recourse around disputes. Mann describes "surveillance hypocrisy" as a state where dominant powers freely engage in top-down surveillance but prohibit other parties from conducting their own surveillance [44]. In a similar way, the designs of most gig platforms enable platforms and customers to track workers, but do not offer workers ways to monitor platforms or customers themselves. Together, these overt or unspoken constraints on workers' abilities to surveil platforms and customers also contribute to the profound power asymmetries in the gig economy.

5.3 Guiding Questions for Evaluating Worker Privacy in Gig Platforms

In this section, we distill our findings into a set of guiding questions about how the design of gig platforms impacts workers' privacy. We organize them broadly around the concepts of transparency, necessity, and accountability as means to the end of worker autonomy. Table 2 provides an overview of the questions, which we discuss in more detail below.

The structure of the guiding questions is loosely inspired by the idea of privacy impact assessments (PIAs) that assess the privacy implications of projects and systems [9, 74]. However, most such assessments ask questions that require internal knowledge of the company and system; here, we emphasize questions that external parties—designers, researchers, auditors, and workers themselves—could use to assess platform privacy and surveillance.

There is still some overlap between our questions and existing PIAs, as well as with more general discussions of workplace privacy and digital surveillance (e.g., [3]) and with principles for technological design called out by privacy by design efforts [8]. By grounding the questions in how the design of the gig economy, its platforms, and its jobs raise particular concerns for worker privacy and surveillance, along with examples and design ideas for gig platforms that look to implement these concepts in positive ways, we seek to provide a gig economy-specific resource for assessing current platforms and informing future platform designs that more carefully account for worker privacy.

5.3.1 *Transparency and Education.*

A main driver of many workers' concerns was a lack of transparency around personal data use, collection, and surveillance. Not knowing when and how data were collected, when customers could observe or contact them, or what platforms would do with the data eroded workers' ability to manage privacy and surveillance risks and their trust in the platforms. Our analysis here is that better communication could go a long way to increase transparency, trust, and autonomy.

Communication with workers around privacy and surveillance is limited and largely comes from a "notice and consent" point of view. This treats data collection as primarily something to be legally justified and disclosed through policies, even though the shortcomings of privacy policies' comprehensibility and usefulness are well-studied [20, 61]. Amazon Mechanical Turk's help document for workers, for instance, mentions privacy exactly once, and points workers to the general privacy policy for all of Amazon.com.

Instead, platforms might be better-served to think about data collection and surveillance through an education-focused lens. Because not knowing companies' actual data practices led workers to speculate about the platforms and mistrust them, it might be to companies' advantage to be straightforward about privacy by detailing what is commonly collected and what it is commonly used for. Inspired by principles of social translucence [18], this might involve allowing workers to see themselves from the point of view of other roles that use their data. Knowing what a ride, worker profile, history, or dispute looks like from the perspective of the platform support team and the customer—as with Upwork's work diary feature, which shows similar views to workers and customers—might help workers better understand and appropriately calibrate trust in the collection and use of their personal data. Clearly discussing surveillance-related considerations would also help workers; Uber's help page on dashcams, for instance, provides several important considerations for drivers who are thinking about using them (and

Transparency and Education: Improving Communication around Privacy
• How well does the platform communicate with workers about privacy and surveillance issues? • Do workers know what kinds of data are collected by both the platform and customers? • To what extent can workers tell when they're being surveilled and by whom? • Can workers understand how data are used?
Necessity and Accuracy: Tightly Linking Surveillance with Management Goals
• Are the data being collected/surveilled required for facilitating the overall work process and individual gigs? Are there alternatives? • Are collected data accurate and in accordance with workers' own activity and expectations? • How likely is the surveillance to lead to (negative) misinterpretations or inferences? • Are there safeguards against accidental or unwarranted collection, distribution, use, aggregation, and inference of workers' data?
Accountability and Safety: Proactive Versus Reactive Mechanisms
• Does the platform provide tools for addressing disputes around privacy and surveillance (involving both customers and platform)? • Do dispute remedies appropriately address root causes? • Can workers collaborate to mitigate shared privacy and surveillance threats? • Is worker safety appropriately considered in the context of privacy and surveillance?
Autonomy and Empowerment: Meaningful Choices, not Difficult Ones
• To what extent do workers have a say in policy and design decisions about what is collected, how it is shared, and how it is used? • What tools do workers have to protect themselves against privacy and surveillance risks posed by particular tasks or customers? • How well can individual workers control specific kinds of data collection or surveillance at specific times? • How much control do workers have around interactions with customers? • What trade-offs do workers face when exerting control over surveillance and personal information?

Table 2: Conceptual categories and guiding questions for external assessments of worker privacy on gig work platforms.

would be even better if it included some of the insights drivers provided in the forums).

As for customers, in some platforms they determine the conditions of a given job, including data to be collected and expectations around privacy, interaction, and surveillance. When these conditions are not clear up front, workers can experience nasty surprises that lead to hard choices between privacy and income [64]. Platforms could help customers do a better job with up-front disclosure. Crowdwork task templates that address personal information, freelancing contract language examples around verifying identity and proof of work, and community guidelines about appropriate interaction between customers and drivers could improve workers' privacy and raise all parties' awareness of privacy and surveillance issues. These in turn would reduce platforms' support costs and friction in the market.

Further, workers' concerns were not just about data collection and use in the abstract, but also about knowing when platforms or customers are actively surveilling them. Webcam-like indicators that a surveillance tool is "on" are a direct way to address this; for instance, platform apps might add indicators when a customer, platform support person, or trusted third party is actively looking at a driver's location. Helping workers reflect on prior surveillance would also be useful; an interface that helped workers review their screenshots and know when they were accessed by other parties could help workers better-assess both specific customers and general tradeoffs around using such tools. These reflection tools might act like the Timeline feature in Google Maps, or the features for auditing assistants' reading of emails in EmailValet [40].

5.3.2 Necessity and Accuracy. Another cluster of concerns revolved around cases where workers saw surveillance and data collection as not needed for the task. As with lack of transparency, both workers' trust and their ability to work were damaged by surveillance that was unnecessary or unexpected, discrepancies between the data collected by platforms and by workers themselves through self-protective surveillance, and unwarranted uses of that data in assessment. Our general prescription here is that tight, clear connections between surveillance, data, and management goals will reduce privacy risks and increase trust.

Many management goals focus on spotting problems that may not be salient to honest workers, such as poor-quality work or ineffective workers. For instance, according to Lyft's privacy policy, the platform uses smartphone sensors to capture details of driving behavior that a driver might not see as necessary for completing tasks. But platforms may have strong interests in using driving behavior to weed out drivers that could put their customers, reputation, and finances at risk. There may be similar dynamics around identity verification: legal requirements that a worker is who they say they are may lead platforms to frequently verify identity, even though it frustrates and annoys workers who play by the rules. As with transparency, communicating clearly about how these considerations affect the jobs could help workers understand why they are being monitored.

Once those management goals are clear, platforms should consider less intrusive and granular ways to collect and share data to accomplish the goals. For identity verification, platforms could offer methods where data stays local to workers' devices (such as device-based fingerprint authentication); this might be both less work and less intrusive than regularly submitting a face photo. For identifying bad drivers or inattentive workers, platforms could do initial data analysis on the worker's device, only sending recent, relevant behavioral data back to the platform's servers when the analysis suggests risks. Freelancing workers might still have their screens and activity surveilled, but rather than making the data visible to customers by default as in Upwork's work diary feature, the platform company might treat it with the privacy associated with real diaries, escrowing it and only sharing with customers when disputes arise. Delivery customers and passengers probably don't need to see an arriving driver's location until the driver is close to the meeting point; knowing the arrival ETA, and whether it is changing, would be less intrusive and just as useful for the management goal of ensuring timely service.

Companies should also address the reliability of the link between data collection and management decisions. When data collection and analysis don't serve management goals because of errors in how humans or algorithms collect, analyze, and make inferences from the data, it can harm workers. Upwork's work diary interface, for instance, practically invites customers to infer that a work block without mouse or screen activity is "not work", a particularly bad choice for many freelance gigs that involve thinking, sketching, and other work that may not translate directly into on-device activity.

Guardrails to reduce those errors are important. Showing appropriate contextual information might reduce the chances of inaccurate customer inferences. For instance, knowing that a crowdworker tends to complete tasks faster than other workers, but at similar quality levels, could reduce the chance customers inappropriately reject good work done "too fast". On delivery platforms, seeing traffic information might help customers understand a slower-than-expected ETA or an unusual route. More generally, it would be good to give customers a "sense of the job" that might help them understand workers' conditions. Upwork's work diary might present guides to interpreting the information, while a delivery app might scroll through issues that are out of workers' control (high traffic, food not ready at restaurant) and make clear the distinction between rating the worker versus rating the company or experience as a whole, to reduce the chance of unwarranted negative evaluations of workers.

5.3.3 *Accountability and Safety.*

Accountability is the third main construct we saw fueling worker concerns. When platforms and customers can't be held accountable for erroneous data or inferences, when they have policies or platform bugs that put workers' privacy and safety at risk, or when they violate agreements and expectations, workers suffer and so does their trust. Here, our recommendation is that good accountability mechanisms will tend to be reciprocal and proactive. We see dispute resolution processes that focus on repairing the harm from an individual incident as too reactive. Although workers are individually happy to receive wrongly withheld pay, or to be unmatched with a problematic customer, incident-focused responses are unlikely to solve fundamental privacy and surveillance issues.

Workers need reciprocal, proactive protection against customers who intrusively or inappropriately surveil them. Lyft, Uber, and Upwork all allow workers to rate customers, but though one worker described seeing a customer banned, it's unclear what platforms' general policies are for handling poorly rated customers. Turkopticon plays a similar role for MTurk workers, though because it is external to the platform it helps only that fraction of workers who know about and participate in it. Delivery platforms, on the other hand, often provide no way to rate customers and thus leave their workers vulnerable to customers who leave negative ratings based on sometimes-incorrect inferences.

Another useful path to proactive accountability is helping workers forestall incorrect inferences from surveilled data. Parallel to earlier suggestions around providing context for surveilled data, workers should be able to annotate tracked work traces with justifications. Workers should also be able to correct factual errors in tracked data and inferences, just as UbiFit Garden allowed users to correct errors made by machine learning algorithms in recognizing fitness activities [10]. Workers also need to be able to contest negative inferences proactively, before they affect their livelihoods. Upwork's 14-day feedback period that allows workers and customers to reciprocally rate each other and discuss those ratings before they are finalized is an interesting starting point around ideas for providing space for workers and customers to negotiate.

Beyond managing known harms, platforms should also proactively identify and mitigate unintended consequences of surveillance. For instance, screenshots of workers' computers can capture personal information that might be exploited by customers or platforms. Similarly, location traces risk identifying people's homes, workplaces, and identities [24]; this is part of why driving platforms' "share my ride" type features try to protect customer privacy by eliding route information. Workers should get the same respect.

5.3.4 *Autonomy and Empowerment.*

Our final set of concerns pertain to autonomy: to what extent privacy and surveillance issues reduce workers' ability to "be their own boss". Such autonomy is more likely when workers know what to expect around data collection, when platforms and customers abide by those expectations, when workers' privacy interests are well-balanced with other stakeholders' needs, and when workers can hold customers and platforms to the same kinds of accountability they are held to. However, transparency, necessity, and accountability are as necessary but not sufficient for workers' autonomy. To complete the picture, workers need meaningful, empowering choices related to privacy and surveillance issues—choices that don't impose unreasonable burden and that are not just workarounds.

Many privacy-related choices currently provided by platforms fail these tests. Disabling location permissions can cause drivers to miss work; it would be better for apps to clearly indicate when location tracking is active and track only when necessary. Upwork workers can choose not to use Upwork's time diary, but at the cost of losing platform support in disputes; it would be better to design the tools to reduce privacy risks that pose hard tradeoffs.

Many of our suggestions aim to provide more meaningful choices. Improving up-front disclosure of privacy and surveillance aspects of tasks—when paired with interfaces that support task choice and algorithms that don't penalize it—would be quite empowering. So would helping workers more clearly know when, why, and how data are collected and used, along with reducing erroneous inferences made by customers based on the data they can access.

Beyond providing better choices, platforms should try to eliminate costly, difficult choices. Workers might more confidently opt into Upwork's surveillance if its work diary were designed with more restricted access and contextualized tracking as described above. As a more radical example, why should drivers have to weigh the benefits of dashcams against the costs in both dollars and sometimes-angry customers? In terms of reducing risks, bad behavior, and support and complaint costs, it would likely be in all parties' interest if driving-related platform companies *required and paid for* dashcams. If designed to treat dashcam footage with respect for both worker and customer privacy, expectations that rides will be temporarily recorded could solve some of these issues while reducing the power asymmetry between workers and customers.

Worker representation in platform-level decisions that impact privacy and surveillance is the longer term solution. Participatory design, value-sensitive design, and privacy by design frameworks would all be well-suited to guiding this task. However, given the current employer-leaning tilt in most legal frameworks for reasoning about workplace privacy (well-described in Katsabian's analysis of privacy, telework, and the COVID-19 pandemic [37]), platforms have little incentive to include workers in these discussions.

6 CONCLUSION

Our analysis of workers' discussions around privacy and surveillance issues makes several advances in areas related to privacy in the gig economy. One is answering the calls for research that focuses on gig workers' privacy as part of the larger set of power imbalances faced by workers. Demonstrating the breadth of concerns and strategies workers discuss across a wide range of platforms helps show how pervasive the issues are in the gig economy, making contributions beyond existing studies of privacy in gig work. We also see our observations about the many privacy risks customers pose (abetted by platform designs) and workers' extensive use of self-protective surveillance as novel, important phenomena around privacy in gig work.

Our guiding questions also provide an accessible, platform-neutral assessment rubric for privacy in the gig economy that both platform companies and external stakeholders could use to make choices about platform participation, design, and regulation. Many of the concepts and examples have implications beyond surveillance: accountability, transparency, and accuracy of data collection are important for workers' pay, power, and potential.

Finally, digital surveillance is increasingly injected into existing workplaces or enabled through remote work arrangements. Our work contributes to a broader understanding of how such forms of digital surveillance impact both workers and work when digital platforms are central to the job being performed.

ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation (Award #2031951). Note that the third author is an employee of the National Science Foundation; this paper is written in his personal capacity and does not necessarily reflect the views of the NSF.

REFERENCES

[1] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz. 2017. Limitless worker surveillance. *California Law Review* 105 (2017), 735–776.

[2] Mashael Yousef Almoqbel and Donghee Yvette Wohn. 2019. Individual and collaborative behaviors of rideshare drivers in protecting their safety. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–21.

[3] Kirstie Ball. 2010. Workplace surveillance: An overview. *Labor History* 51, 1 (2010), 87–106.

[4] Jason Baumgartner, Savvas Zannettou, Brian Keegan, Megan Squire, and Jeremy Blackburn. 2020. The Pushshift Reddit dataset. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 14. AAAI, Palo Alto, CA, USA, 830–839.

[5] William S Brown. 1996. Technology, workplace privacy and personhood. *Journal of Business Ethics* 15, 11 (1996), 1237–1248.

[6] Eliane Léontine Bucher, Peter Kalum Schou, and Matthias Waldkirch. 2021. Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy. *Organization* 28, 1 (2021), 44–67.

[7] Juan Carlos Alvarez de la Vega, Marta E. Cecchinato, and John Rooksby. 2021. "Why lose control?" A study of freelancers' experiences with gig Economy platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–14.

[8] Ann Cavoukian. 2009. *Privacy by design: The 7 Foundational Principles*. Technical Report. Office of the Information and Privacy Commissioner.

[9] Roger Clarke. 2009. Privacy impact assessment: Its origins and development. *Computer Law & Security Review* 25, 2 (2009), 123–135.

[10] Sunny Consolvo, David W McDonald, Tammy Toscos, Mike Y Chen, Jon Froehlich, Beverly Harrison, Predrag Klasnja, Anthony LaMarca, Louis LeGrand, Ryan Libby, Ian E. Smith, and James A. Landay. 2008. Activity sensing in the wild: a field trial of UbiFit Garden. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1797–1806.

[11] Juliet Corbin and Anselm Strauss. 2014. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications, Thousand Oaks, CA, USA.

[12] Valerio De Stefano. 2015. The rise of the just-in-time workforce: On-demand work, crowdwork, and labor protection in the gig-economy. *Comparative Labor Law & Policy Journal* 37, 3 (2015), 471–504.

[13] Kurt H Decker. 1987. Employment Privacy Law for the 1990s. *Pepp. L. Rev.* 15 (1987), 551.

[14] Tawanna R Dillahunt, Xinyi Wang, Earnest Wheeler, Hao Fei Cheng, Brent Hecht, and Haiyi Zhu. 2017. The sharing economy in computing: A systematic literature review. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–26.

[15] Brooke Erin Duffy, Annika Pinch, Shruti Sannon, and Megan Sawey. 2021. The nested precarities of creative labor on social media. *Social Media + Society* 7, 2 (2021).

[16] Brianna Dym and Casey Fiesler. 2020. Ethical and privacy considerations for research using online fandom data. *Transformative Works and Cultures* 33 (2020).

[17] Lilian Edwards, Laura Martin, and Tristan Henderson. 2018. Employee Surveillance: The road to surveillance is paved with good intentions. (2018). Available at SSRN.

[18] Thomas Erickson and Wendy A Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM Transactions on Computer-Human Interaction (TOCHI)* 7, 1 (2000), 59–83.

[19] Worker Info Exchange. 2021. ADCU & WIE demand Microsoft suspend Uber's Face API license. https://www.workerinfoexchange.org/post/adcu-wie-demand-microsoft-suspend-uber-s-face-api-license. Accessed: 2021-07-12.

[20] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence*. ACM, New York, NY, USA, 18–25.

[21] Alek Felstiner. 2011. Working the crowd: Employment and labor law in the crowdsourcing industry. *Berkeley Journal of Employment & Labor Law* 32 (2011), 143.

[22] Joseph L Fleiss. 1971. Measuring nominal scale agreement among many raters. *Psychological Bulletin* 76, 5 (1971), 378.

[23] T Marx Gary. 2017. I'll be watching you: reflections on the new surveillance. In *Surveillance, Crime and Social Control*. Routledge, New York, NY, USA, 3–11.

[24] Philippe Golle and Kurt Partridge. 2009. On the anonymity of home/work location pairs. In *International Conference on Pervasive Computing*. IEEE, New York, NY, USA, 390–397.

[25] Kotaro Hara, Abigail Adams, Kristy Milland, Saiph Savage, Chris Callison-Burch, and Jeffrey P Bigham. 2018. A data-driven analysis of workers' earnings on Amazon Mechanical Turk. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–14.

[26] Richard Heeks. 2017. *Digital Economy and Digital Labour Terminology: Making Sense of the Gig Economy, Online Labour, Crowd Work, Microwork, Platform Labour, Etc.* Working paper 70. Global Development Institute.

[27] Jaap-Henk Hoepman. 2014. Privacy design strategies. In *IFIP International Information Security Conference*. Springer, Cham, Switzerland, 446–459.

[28] Robert Howard. 1986. *Brave New Workplace*. Viking Press, New York, NY, USA.

[29] Ursula Huws. 2015. *A Review on the Future of Work: Online Labour Exchanges, or "Crowdsourcing": Implications for Occupational Safety and Health.* Technical Report. European Agency for Safety and Health at Work (EU-OSHA).

[30] Lilly C Irani and M Six Silberman. 2013. Turkopticon: Interrupting worker invisibility in Amazon Mechanical Turk. In *Proceedings of the CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, 611–620.

[31] Rabih Jamil. 2020. Uber and the making of an Algopticon-Insights from the daily life of Montreal drivers. *Capital & Class* 44, 2 (2020), 241–260.

[32] Mohammad Hossein Jarrahi, Will Sutherland, Sarah Beth Nelson, and Steve Sawyer. 2020. Platformic management, boundary resources for gig work, and worker autonomy. *Computer-Supported Cooperative Work (CSCW)* 29, 1 (2020), 153–189.

[33] Arne L Kalleberg and Michael Dunn. 2016. Good jobs, bad jobs in the gig economy. *Perspectives on Work* 20, 2 (2016), 10–14.

[34] Thivya Kandappu, Vijay Sivaraman, Arik Friedman, and Roksana Boreli. 2013. Exposing and mitigating privacy loss in crowdsourced survey platforms. In *Proceedings of the CoNEXT Student Workshop.* ACM, New York, NY, USA, 13–16.

[35] Jerry Kang, Katie Shilton, Deborah Estrin, and Jeff Burke. 2011. Self-surveillance privacy. *Iowa Law Review* 97 (2011), 809–847.

[36] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of Mechanical Turk workers and the US public. In *10th Symposium On Usable Privacy and Security (SOUPS 2014).* USENIX, Berkeley, CA, USA, 37–49.

[37] Tammy Katsabian. 2020. The Telework Virus: How the COVID-19 pandemic has affected telework and exposed its implications for privacy and equality. (2020). Available at SSRN.

[38] Eliscia Kinder, Mohammad Hossein Jarrahi, and Will Sutherland. 2019. Gig platforms, tensions, alliances and ecosystems: An actor-network perspective. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–26.

[39] Aniket Kittur, Jeffrey V Nickerson, Michael Bernstein, Elizabeth Gerber, Aaron Shaw, John Zimmerman, Matt Lease, and John Horton. 2013. The future of crowd work. In *Proceedings of the 2013 Conference on Computer-Supported Cooperative Work.* ACM, New York, NY, USA, 1301–1318.

[40] Nicolas Kokkalis, Thomas Köhn, Carl Pfeiffer, Dima Chornyi, Michael S Bernstein, and Scott R Klemmer. 2013. EmailValet: Managing email overload through private, accountable crowdsourcing. In *Proceedings of the 2013 Conference on Computer-Supported Cooperative Work.* ACM, New York, NY, USA, 1291–1300.

[41] Matthew Lease, Jessica Hullman, Jeffrey Bigham, Michael Bernstein, Juho Kim, Walter Lasecki, Saeideh Bakhshi, Tanushree Mitra, and Robert Miller. 2013. Mechanical Turk is not anonymous. (2013). Available at SSRN.

[42] Deborah Lupton. 2014. Self-tracking cultures: towards a sociology of personal informatics. In *Proceedings of the Australian Computer-Human Interaction Conference on Designing Futures.* ACM, New York, NY, USA, 77–86.

[43] Ning F Ma, Chien Wen Yuan, Moojan Ghafurian, and Benjamin V Hanrahan. 2018. Using stakeholder theory to examine drivers' stake in Uber. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, 1–12.

[44] Steve Mann. 2020. Wearables and sur(over)-veillance, sous(under)-veillance, co(so)-veillance, and metaveillance (veillance of veillance) for health and well-being. *Surveillance & Society* 18, 2 (2020), 262–271.

[45] Steve Mann, Jason Nolan, and Barry Wellman. 2003. Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society* 1, 3 (2003), 331–355.

[46] James Manyika, Susan Lund, Jacques Bughin, Kelsey Robinson, Jan Mischke, and Deepa Mahajan. 2016. *Independent Work: Choice, Necessity, and the Gig Economy.* Technical Report. McKinsey Global Institute.

[47] Annette Markham. 2012. Fabrication as ethical practice: Qualitative inquiry in ambiguous Internet contexts. *Information, Communication & Society* 15, 3 (2012), 334–353.

[48] Randi Markussen. 1994. Constructing easiness—historical perspectives on work, computerization, and women. *The Sociological Review* 42, 1 (1994), 158–180.

[49] Gary T Marx. 2015. Surveillance studies. *International Encyclopedia of the Social & Behavioral Sciences* 23, 2 (2015), 733–741.

[50] Nora McDonald and Helena M Mentis. 2021. Building for 'We': Safety settings for couples with memory concerns. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, 1–11.

[51] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[52] Brian McInnis, Dan Cosley, Chaebong Nam, and Gilly Leshed. 2016. Taking a HIT: Designing around rejection, mistrust, risk, and workers' experiences in Amazon Mechanical Turk. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, 2271–2282.

[53] Phoebe V Moore. 2017. *The Quantified Self in Precarity: Work, Technology and What Counts.* Routledge, New York, NY, USA.

[54] Phoebe V Moore, Martin Upchurch, and Xanthe Whittaker. 2018. Humans and machines at work: Monitoring, surveillance and automation in contemporary capitalism. In *Humans and Machines at Work*, Phoebe Moore, Martin Upchurch, and Xanthe Whittaker (Eds.). Springer, New York, NY, USA, 1–16.

[55] Sarah Mosseri. 2020. Being watched and being seen: Negotiating visibility in the NYC ride-hail circuit. *New Media & Society* 22, 10 (2020), 1–21.

[56] Mozilla 2020. *Internet Health Report.* Mozilla. https://2020.internethealthreport.org

[57] Gemma Newlands. 2021. Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space. *Organization Studies* 42, 5 (2021), 719–737.

[58] Aiha Nguyen. 2021. *The Constant Boss: Work under Digital Surveillance.* Technical Report. Data & Society Research Institute.

[59] Nicholas Proferes, Naiyan Jones, Sarah Gilbert, Casey Fiesler, and Michael Zimmer. 2021. Studying Reddit: A systematic overview of disciplines, approaches, methods, and ethics. *Social Media + Society* 7, 2 (2021).

[60] Giulia Ranzini, Michael Etter, Christoph Lutz, and Ivar Vermeulen. 2017. Privacy in the sharing economy. (2017). Available at SSRN.

[61] Joel R Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia McDonald, Thomas B Norton, and Rohan Ramanath. 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal* 30, 1 (2015), 39.

[62] Alex Rosenblat and Luke Stark. 2016. Algorithmic labor and information asymmetries: A case study of Uber's drivers. *International Journal of Communication* 10 (2016), 3758–3784.

[63] Shruti Sannon, Natalya N Bazarova, and Dan Cosley. 2018. Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, 1–13.

[64] Shruti Sannon and Dan Cosley. 2019. Privacy, power, and invisible labor on Amazon Mechanical Turk. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19).* ACM, New York, NY, USA, 1–12.

[65] Luke Stark and Karen Levy. 2018. The surveillant consumer. *Media, Culture & Society* 40, 8 (2018), 1202–1220.

[66] Anselm Strauss and Juliet Corbin. 1990. *Basics of Qualitative Research.* Sage Publications, Thousand Oaks, CA, USA.

[67] Will Sutherland, Mohammad Hossein Jarrahi, Michael Dunn, and Sarah Beth Nelson. 2020. Work precarity and gig literacies in online freelancing. *Work, Employment and Society* 34, 3 (2020), 457–475.

[68] Zhi Ming Tan, Nikita Aggarwal, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. 2021. The ethical debate about the gig economy: A review and critical analysis. *Technology in Society* 65 (2021), 101594.

[69] Julia Ticona, Alexandra Mateescu, and Alex Rosenblat. 2018. *Beyond Disruption: How Tech Shapes Labor across Domestic Work & Ridehailing.* Technical Report. Data & Society.

[70] Carlos Toxtli, Siddharth Suri, and Saiph Savage. 2021. Quantifying the invisible labor in crowd work. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2, Article 319 (Oct 2021), 26 pages.

[71] Sarah Vieweg and Adam Hodges. 2016. Surveillance & modesty on social media: How Qataris navigate modernity and maintain tradition. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing.* ACM, New York, NY, USA, 527–538.

[72] Alex J Wood, Mark Graham, Vili Lehdonvirta, and Isis Hjorth. 2019. Good gig, bad gig: autonomy and algorithmic control in the global gig economy. *Work, Employment and Society* 33, 1 (2019), 56–75.

[73] Alex J Wood, Vili Lehdonvirta, and Mark Graham. 2018. Workers of the Internet unite? Online freelancer organisation among remote gig economy workers in six Asian and African countries. *New Technology, Work and Employment* 33, 2 (2018), 95–112.

[74] David Wright. 2012. The state of the art in privacy impact assessment. *Computer Law & Security Review* 28, 1 (2012), 54–61.

[75] Huichuan Xia, Yang Wang, Yun Huang, and Anuj Shah. 2017. "Our privacy needs to be protected at all costs": Crowd workers' privacy experiences on Amazon Mechanical Turk. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–22.

[76] Ming Yin, Mary L Gray, Siddharth Suri, and Jennifer Wortman Vaughan. 2016. The communication network within the crowd. In *Proceedings of the 25th International Conference on World Wide Web.* IW3C2, Geneva, Switzerland, 1293–1303.

[77] Shoshana Zuboff. 1988. *In the Age of the Smart Machine: The Future of Work and Power.* Basic Books, New York, NY, USA.