Workplace Monitoring: Data Collection Practices and Emerging Risks for Low Wage Workers in India

Iona Eckstein and Zothan Mawii

FRIEDRICH EBERT STIFTUNG

Workplace Monitoring: Data collection practices and emerging risks for low wage workers in India

Iona Eckstein and Zothan Mawii

December 2020

FRIEDRICH EBERT STIFTUNG

Contents

List of abbreviations

CCTV	Closed-circuit television
EU	European Union
GDPR	General Data Protection Regulations
IFAT	Indian Federation of App-Based Transport Workers
ILO	International Labour Organisation
IT Act	Information Technology Act
ITUC	International Trade Union Confederation
MeitY	Ministry of Electronics and Information Technology
OSH	Occupational Safety and Health
PDP	Personal Data Protection Bill (2019)
PDPA	Personal Data Protection Act (2012)
SC/ST	Scheduled Caste and Scheduled Tribes
SPDI	Sensitive Personal Data and Information
TLC	Taxi Limousine Commission
USA	The United States of America

List of figures

Foreword

Workplace monitoring has been practised by employers across businesses to improve employee productivity, track time spent on actual work, evaluate employee performance, and safeguard the company against data theft. Come the 21st century, and this practice is now aided by technological advancement as employers collect increasing amounts of employee data. The information gathered aids in the quantification of activities and gives insight into an individual's personal qualities that may not have been tracked at the workplace previously. The precision, scale and tempo of data collection are reaching new highs.

The rapidly growing platform economy has introduced new means of monitoring, including fitness apps, biometric systems, remote monitoring, and algorithm-based tools. These sophisticated workplace monitoring and surveillance measures have the potential to feed automated decision making and make predictions about individual workers' future behaviour, skills and even the status of their health.

Simple practices of ensuring workplace efficiency, monitoring and surveillance have advanced leaps and bounds due to technology advances, and now tend to encroach individual privacy. Workers are disadvantaged by the relative ease with which employers can combine data from several sources. This monitoring by employers can further contribute to shifting the power dynamics between employees and employers as the imbalance of access to worker data can reduce their negotiating power.

Although privacy and data protection laws exist in several forms in many countries, workers' data may not be specifically covered by these laws. As of today, there are no global standards for transparent governance of employee data. In 1999, the International Labour Organisation (ILO) developed a code of practice on the protection of workers' personal data. The crux of the ILO's code of practice has remained to evolve data protection mechanisms, which could ensure the dignity of workers, protect their privacy and ensure their right to determine who may use which data and for what purposes.

In the Indian context, more than 90 per cent of the workforce is employed in the informal economy, which includes self-employed, contractual / sub-contractual workers, and the rising gig and platform workforce who do not fall within the traditional notion of the employer-employee relationship. How data protection regulations can be provided for them remains to be seen. The Government of India has undertaken major labour reforms and drafted the Personal Data Protection Bill 2019 (PDP). These reforms should potentially serve as opportunities to frame laws that respect both individual and collective rights to data protection.

Friedrich-Ebert-Stiftung (FES), India Office is thankful to Iona Eckstein and Zothan Mawii of Tandem Research for preparing this research paper, which forms part of FES's research paper series *Shaping the Future of Workers in Asia.* We hope this paper will contribute in shaping the debate on data protection, privacy issues, rights and ultimately, in evolving a robust data governance system in India.

Anup Srivastava
Program Adviser
Friedrich-Ebert-Stiftung, India Office
December 2020

Acknowledgements

This paper was produced with the support of the Friedrich-Ebert-Stiftung, India Office. We are very grateful to the experts we interviewed for the paper, who generously shared their insights.

1. Introduction

The monitoring of workers by employers is an age-old practice, but advances in technology have enabled this monitoring to become more widespread and comprehensive than ever before (Ajunwa et al., 2017). Technological advances—such as big data analytics, communication capture, the design and widespread availability of mobile devices, and biometrics—have allowed employers to monitor the workforce through various means. These monitoring practices enable comprehensive and granular data to be collected on workers, whether they are at the workplace or working remotely.

The COVID-19 (Coronavirus Disease) pandemic has also legitimised new forms of health-related data collection. Employers are introducing invasive data collection practices, often with no indication of when these measures may be stopped. The pandemic has forced those who are able—mostly white-collar workers—to work from home (Singh, 2020). On the other hand, essential workers, a large proportion of whom are low-income, blue-collar workers, continue to go to work under increased monitoring and restrictions (Pundir, 2020).

The COVID-19 pandemic has forced mostly white-collar workers to work from home while a large proportion of blue-collar workers continue to go to work under increased monitoring and restrictions.

This paper analyses data protection issues related to low-income workers in India. First, workplace data collection and surveillance practices are outlined. Following this, the paper presents and analyses the experience of several groups of low-income workers who are subject to problematic monitoring and data collection policies and the consequent risks they face. Following this, there is a discussion around India's data protection policy, and its shortfalls related to worker's data protection. The paper concludes by suggesting pathways towards protecting workers' data privacy and rights.

For this paper, information was drawn from both expert interviews and desk research to understand the landscape of worker surveillance and data collection. Four experts were interviewed around data protection risks for specific groups of workers: Basudev Barman, a researcher and organiser affiliated with the International Transport Workers' Federation[1]; Parvathi C.M, programme officer at Cividep India[2]; Suhasini Singh[3], the India country representative for the Fair Wear Foundation; and Rakhi Sehgal[4], founder of Gurgaon Shramik Kendra (Gurgaon Workers' Centre).

The research methodology did have its limitations. There was no direct communication with workers but instead, expert interviews with organisers and researchers working on labour issues were used as primary insights. The paper focuses mainly on the experience of gig workers and garment workers; however, this is not a comprehensive representation of all low-income workers in India. The experiences of less organised workers, like sanitation and domestic workers, are missing from the analysis.

Data protection and surveillance issues for low-wage workers is an emerging area of research. Thus this paper does not aim to provide a comprehensive analysis of the issue; instead, it serves as a starting point for discussion by identifying key issues for future research and policy attention.

2. Mechanisms of surveillance in the 21st-century workplace

Lyon (2001) defines surveillance as "any collection and processing of personal data, whether identifiable or not, for the purpose of influencing or managing those whose data have been garnered." Some employers integrate technologies that allow them to collect vast amounts of data on their workforce, enabling them to make managerial decisions based on the data collected (Ajunwa et al., 2017). These workplace monitoring practices can be considered employee surveillance.

Before the 21st century, employers mostly relied on human agents to undertake employee surveillance (Ajunwa et al., 2017). However, digital technologies have now become the primary means of monitoring (Ajunwa et al., 2017; Lyon, 2001). These technologies now enable employers to track workers' bodily movement, health status, location, keystrokes and online activities, and even their mental state (Tandem Research, 2020). Current surveillance practices are unique because of how comprehensive, invasive, and ubiquitous they are.

Mateescu and Nguyen (2019a) categorise recent worker surveillance strategies under four categories: prediction and flagging tools designed to identify and deter perceived rule-breaking; biometric and health tracking that challenge the boundaries of worker privacy; remote monitoring and time tracking that track workers' productivity; and algorithmic management tools that nudge and control worker behaviour. Technologies such as thermal scanners, CCTV cameras, movement sensors, keystroke logging software, screen monitoring software, time management tools, and GPS trackers are used to monitor workers' productivity, health, and wellbeing (Mateescu & Nguyen, 2019a; Tandem Research, 2020).

Data collection and surveillance technologies are inextricably linked, with each feeding into the other. These technologies collect data extensively and can be used to develop automated decision making systems to monitor, evaluate and direct worker behaviour (Mateescu & Nguyen, 2019a). As the lines between workplace and personal space become increasingly blurred, workers' data is no longer confined to workplaces and work activities. Workers are being monitored even at home and during leisure time. As Ajunwa et al. (2017) emphasise, this is a novel development compared with previous worker monitoring that only covered working hours and is of real concern to privacy laws. Wearable technological devices, mobile devices, and software installed on computers collect worker data well after they have left the 'workplace' (Satariano, 2020). Additionally, data can be combined from different sources, including social media, personal devices, and publicly available sources, to create a comprehensive profile of workers. These profiles could reveal sensitive personal information that the workers may not have authorised to be collected.

With increasing employee surveillance, workers' data is no longer confined to workplaces and work activities. Workers are being monitored even at home and during leisure time.

Data collected through monitoring and surveillance systems are used to develop algorithmic management systems (Mateescu & Nguyen, 2019b). These are then used to inform hiring and management decisions, insurance premiums, and even credit scores. For example, corporate wellness programmes require workers to wear health tracking devices like Fitbits (Ajunwa et al., 2016). The readings from these devices are then used to determine health insurance premiums and employer contributions to health benefits (Ajunwa et al., 2016). Fintech companies in India are increasingly using social media activity, call logs, message histories and spending habits to determine interest rates for their products (Saleem, 2019).

Algorithms and automated systems are fast complementing, and in some cases, even replacing some functions of human resource departments (Duggan et al., 2019). Job applications are run through automated systems to determine an applicant's suitability. Gamification tactics used by on-demand ride-hailing platforms determine a worker's access to earning

opportunities. Grievance redressal systems—sometimes the only direct point of contact between worker and employer—are being replaced by technological interventions (Lee, 2016). Time management systems and other productivity tracking tools are used to monitor workers' performance (Lecher, 2019).

Tracking can take place through mobile phones, laptops, or fitness trackers—devices that workers use for both work and leisure. The algorithms that run these systems are socio-technical systems shaped by both the technology underpinning them and the social and economic conditions within which they are used. The algorithms are trained on historically available data, and data is inherently biased (Crawford, 2013). The objectivity of algorithms and mathematical models has come under intense criticism in recent years. There is a rich body of literature on these systems, exacerbating discriminatory practices against already marginalised groups (Ajunwa & Greene, 2019; Benjamin, 2019; Noble, 2018; O'Neill, 2016).

Workers have to cede increasing amounts of data to remain employed as the uptake of these monitoring and surveillance technologies increases. Much of this monitoring takes place without the ostensible consent of the workers. Ajunwa et al. (2017) state that privacy cannot be treated as an economic good that is exchanged for employment. They question the adequacy of legal frameworks to protect workers' privacy in the face of pervasive surveillance technologies.

In addition to the weakening of privacy, these monitoring practices also chip away the workers' ability to organise and collectively bargain. Data traces left by workers can ascertain a worker's movements and interactions on the shop floor. Amazon-owned Whole Foods installed monitoring systems that tracked workers' intention to collectivise and then devised ways to undercut their efforts at collective action (Peters, 2020). New forms of data collection and surveillance methods make it easier for employers to prevent collectivisation, even as labour standards deteriorate (ITUC, 2020).

Workers have to cede increasing amounts of data to remain employed as the uptake of these monitoring and surveillance technologies increases.

Worker privacy is at risk in the face of pervasive and invasive workplace surveillance; however, it is not the only thing. Workers' agency and autonomy are severely at risk as opaque algorithms are used to make managerial decisions and even direct their work. Existing legal frameworks that safeguard worker interest vis-a-vis employers are no longer adequate to cover the risks and implications of these new practices (Ajunwa et al., 2017). Workers' ability to organise and their bargaining capacity, already weakened with increasing contract work and non-standard employment globally, is also under threat (ITUC, 2020). Additionally, workers' access to financial services, employer-provided benefits, and other social protection measures could be heavily curbed by surveillance mechanisms.

Much of the employee monitoring takes place without the ostensible consent of the workers.

3. Workplace monitoring in India: What is at risk for workers?

This section focuses on two groups of low-income workers in India and demonstrates how, despite the differing monitoring, surveillance and data collection measures exerted over them, they face common issues related to the protection of their data and privacy. The research focuses on gig workers and garment factory workers as they face different forms of invasive surveillance mechanisms and data collection. Additionally, they represent workers from different demographic groups, so as to compare the experience of worker surveillance, intersecting with socio-economic characteristics, such as gender and migrant-status.

Worker privacy is at major risk in the face of pervasive and invasive workplace surveillance. Existing legal frameworks do not suffice in safeguarding.

On-demand gig workers—who provide food delivery, ridesharing, or domestic services—access their work through the company's app on their smartphone. Through this app, they find earning opportunities, accept a job, communicate with clients and the platform company, and receive ratings and payments. In other words, their phone is essential for all elements of their work. However, "phones leak traces of our activities all the time such as our location, usage patterns, and habits" (Privacy International, 2017). This means that, when accessing the app, gig workers' data is being collected. The data collected is then used by algorithmic management systems that assign 'gigs' and determine workers' access to earnings (Aneja et al., 2019). This allows platform companies to collect large amounts of data on workers, extending far beyond what is usually collected by a contracting company (Privacy International, 2017). In India, gig workers are largely male, with a range of educational levels migrating to larger cities (Rao, 2019). The high rate of youth unemployment and the slow rate of job creation has led many young, educated people to join the gig economy (Rao, 2019). Women are also joining the gig economy, but usually at a lower pay level than men (Kar, 2019).

Garment workers in India are also vulnerable to workplace surveillance. Although surveillance and data collection is not as technologically advanced as in other sectors, garment workers are monitored and surveilled through older technologies. As well as collecting basic demographic information about workers, the two main forms of data collection in the garment sector are CCTV surveillance and biometric fingerprint scanning, as told by Parvathi C.M (programme officer at Cividep India). Garment workers may be asked to provide a biometric fingerprint scan when they enter and leave the factory. They will then be under CCTV surveillance during their working day, meaning any socialising or toilet breaks can be recorded; in other words, "maximising their production time by minimising downtime like chatter and laughter" (Kaur, 2017).

Approximately 60 per cent of workers in the Indian garment industry are women (Kane, 2014). However, as pointed out by Suhasini Singh (India Country Representative at Fair Wear), many workers are hired on a contractual basis and not included in official records; so this percentage could be much higher. Migrant workers make up 80 per cent of garment workers in Bengaluru, and often come from impoverished states such as Bihar, Jharkahand, Odisha and West Bengal (The Hindu, 2012). Suhasini Singh emphasised that there was a preference for hiring women from marginalised groups such as Scheduled Caste or Scheduled Tribe communities (SC/ST). These women are then housed in factory-provided hostels near their workplace. It is important to highlight these socio-economic characteristics as young female migrant workers living away from their families can be considered more vulnerable than other worker demographics.

Across both groups of workers, there are similar risks related to data collection and surveillance methods. These are expanded on below.

3.1 Information asymmetry exacerbates power asymmetry

Certain companies deliberately conceal information around data collection practices from workers (Maatescu & Nguyen, 2019). New systems of workplace surveillance technologies enable the collection of large volumes of granular data, compared to older forms of monitoring, and advances in computing technologies allow this data to be stored and processed more efficiently. This has created cases of severe information asymmetries between workers and employers (Maatescu & Nguyen, 2019).

For gig workers, their smartphone app constantly records data about both the device and the worker. This can include GPS data such as the route they took and speed with which they completed the journey, as well as how long a food delivery worker waited in a restaurant or at a customers' house. Privacy International (2017) reports that Uber can record data on how fast a driver accelerates or breaks through the app. However, gig workers often have no knowledge of this constant and invasive data collection strategy. Basudev Barman, a labour researcher specialising in the platform economy, stated in an interview that in the case of Uber in India, any change to the working contract that may cover data policies will be phrased in complex language. This detracts a worker from reading through the details before confirming their acceptance. He expanded on this, saying that sometimes workers are not even required to accept changes to their contract; instead, changes are automatically 'accepted' if they continue to use the app.

In their analysis of gig work and data protection, Privacy International (2017) also emphasised that workers are unable to challenge data collection processes because of their opacity. Thus, platform companies' data policies can be viewed as deliberately opaque, which creates an information asymmetry between gig workers and platforms about what data is collected, how it is stored, and how it is used. This information asymmetry leaves workers unable to dispute how the platform makes algorithmic decisions around work allocation, pricing and account deactivation and contributes to the power asymmetry between workers and companies.

Workers are unable to challenge data collection processes because of their opacity.

Information asymmetry is also an issue for garment workers. Parvathi C.M highlighted that garment workers are rarely given a copy of their working contract, let alone a document outlining data collection and usage policies. This means garment workers are given no information regarding how their data may be used or shared. Regarding CCTV monitoring, Suhasini Singh stated that CCTV cameras are often introduced following an instance of harassment or abuse against workers, who are told it is being installed to improve their safety. However, Singh stated this was a 'superficial response' as installing cameras does not really result in sensitising (potential) perpetrators, nor does it actually lower the incidences of abuse or harassment within factories (Ranganathan, 2017). Although nominally, it is installed to reduce harassment in factories; the footage is often used to monitor workers' movements and toilet breaks. Arguably, the true nature of surveillance is being concealed by companies.

Ranganathan (2017) further supports this, stating, "CCTV cameras are popular solutions for those forging 'women's safety' agendas, but it can come at great cost to women's movement and privacy." Workers are unlikely to have the operational knowledge around the working of CCTV systems, such as when they are turned on, what areas they cover and where the recorded footage is stored. This could potentially lead to management staff abusing their positions of power due to their knowledge of how the systems work, compared with workers' lack of knowledge. For example, abuse or harassment could simply be displaced by CCTV instead of being stopped, if management staff know exactly where cameras are placed and where there are subsequent blindspots (Ranganathan, 2017).

Information asymmetry also extends to companies concealing data that is crucial for workers' collectivisation. During an interview, Rakhi Sehgal (founder of Gurgaon Shramik Kendra) gave the example of workers working for an Indian processing plant company, who were not allowed to access the results of their medical tests. The Occupational Safety and Health (OSH) legislation mandates employers to provide high-risk workers with routine health check-ups and medical treatment. The

company arranged these health-checks for workers, but refused to disclose the results to them.

This information asymmetry has a profound impact on workers and their ability to advocate for better working conditions. Companies are obligated to publish their financial records listing their earnings and profit by the Ministry of Corporate Affairs in India. Sehgal pointed out that some companies consistently refuse to share their annual filings with workers' organisations in the run-up to negotiation for long-term settlements or wage settlements to avoid any concessions to workers. Without the company's financial records, workers are unable to negotiate better terms for themselves.

Access to data and information is crucial for workers to advocate for their rights.

Access to data and information is therefore crucial for workers to advocate for their rights. It is equally important for workers to be able to make sense of the data or information they gain access to.

3.2 Risk of individual targeting

Companies' ability to target individual workers is enabled through granular data collection and surveillance methods. Individual workers can be singled out and reprimanded for anything ranging from lower productivity or slower speeds, to speaking with a colleague or taking too many breaks (Ranganathan, 2017).

Referring to gig workers, Basudev Barman stated that an immediate risk of data collection is persecution; if granular data is available about exactly what actions an individual has taken, it becomes easy to single them out. This was evident in a recent legal case between Uber and a driver in the United Kingdom. James Farrar brought a legal claim against Uber regarding his declining earnings despite his increasing hours of work. During his time working as an Uber driver, the app collected data on his activities, "it noted how many rides he accepted and how many he cancelled, mapped where trips started and ended, and how long it took him to wind through traffic to get there" (Holder, 2019). Uber could therefore access all of Farrar's Uber-related data and use it as ammunition against him during the trial (Holder, 2019).

Persecution is an immediate risk of data collection. Workers who talk back in factories are often targeted with surveillance cameras and isolated from their co-workers.

For garment workers, there are also instances where surveillance has been used to punish individual workers. During her research, Ranganathan (2017) found, "it is very common for women who talk back in factories to be vindictively targeted with surveillance cameras, and isolated from their co-workers."

Garment workers are also targeted by employers using the demographic details they are required to submit. Sehgal recalled instances when garment workers' details, such as their names, photos and mobile numbers were shared by companies and recruitment agencies to ensure they are not hired in a specific area. This usually happens as punishment for workers who challenge the authority of management or "misbehave."

3.3 Data sharing risks

The possibility that a company may share data on workers with a third party (such as a government agency, private business, or data analytics company) is a serious risk that could undermine workers' future attempts to change employers, access credit and insurance, or be involved in activism or protest movements.

During an interview regarding gig workers, Basudev Barman stated that, although there is little evidence that platform companies share data in India, there have been examples of this happening in other countries with stronger data protection policies. One example of this is the American home service platform TaskRabbit, whose policy is to share data with law enforcement authorities without a warrant and without providing notice to users when their data is sought by such authorities (Cardozo et al., 2016). It is possible that similar data sharing could also be happening covertly in India.

Concerning the COVID-19 pandemic, companies' strategies to ensure workers could return to work following the lockdown demonstrate some of these data-sharing risks. To comply with health and safety

standards, companies have introduced new methods of monitoring workers' health and movements. A number of on-demand gig companies in India have made it mandatory for their delivery workers to download the Indian government's contact tracing app, Aarogya Setu, for them to continue accepting jobs through the app (IFAT, 2020). Before COVID-19, platform companies could collect workers' data only while using the app or while the app was running in the background (IFAT, 2020). The Indian Federation of App-Based Transport Workers (IFAT) has stated their concerns around tying Aarogya Setu to workers' ability to access platforms and services and recording their movements (Agrawal, 2020). IFAT noted that the linking of Aarogya Setu and platform apps creates the risk of data sharing, which could lead to retaliatory action against workers who collectivise. Additionally, access to work is now assigned on the basis of health status, and income has become contingent upon the download of the app, which constitutes coercion (Agrawal, 2020). Barman stated that mandating the download of Aarogya Setu allows different actors to collect ever-increasing data about workers' movements as the contact tracing app monitors the concerned workers and their location data even when they are not working.

Besides extended data collection, there is scope for further control of the worker by platforms that mandate the download of Aarogya Setu. As was stated in a recent report by the Indian Federation of App-based Transport Workers (IFAT), "In addition to workers' pay, availing benefits and protection schemes offered by the platform could also be tied to installing the Aarogya Setu app and be predicated upon the result shown by the app" (IFAT, 2020). Apps such as Aarogya Setu enhance the quality of information available to platform companies and could potentially provide them with new information that was previously unavailable such as health-related data. This could lead to the "datafication of the workforce that was hitherto outside its scope" (IFAT, 2020).

Data protection policies should remain central to a worker's right to livelihood and income, even during a pandemic situation.

Despite the unique working situation that the pandemic has prompted, workers should not be forced to sacrifice their privacy and risk their data being shared amongst companies and institutions to continue working and earning an income. Thus, data protection policies should remain central, even during a pandemic situation.

3.4 Limiting opportunities for worker collectivisation

Historically, workers were monitored and surveilled by employers and management to limit collectivisation through specific 'union-busting' services such as the Pinkerton Agency[5] in the late 19th and early 20th century (Jones, 2018; Ajunwa et al., 2017). This continues today, with far more sophisticated technological forms of monitoring practices. Sehgal stated that factory workers' interactions with each other on and off the shop floor may be monitored through CCTV footage. Data traces from emails and devices are already being used to prevent collectivisation in the USA (Peters, 2020). This may not be applicable in the Indian context yet, but it could become a reality in the near future.

The garment sector makes a concerted effort to limit collectivisation, with only three per cent of garment workers belonging to a workers' organisation, meaning collective, large-scale resistance to surveillance and monitoring is non-existent (Ranganathan, 2017). Any individual resistance to data collection processes would simply lead to workers being banned from work, which is not a viable option for garment workers who rely on this income.

4. Workers' data: What does the law say?

Indian workers currently have a few legal protections in case of privacy violations by employers. Some provisions under the Information Technology Act, 2000, cover citizens against workplace surveillance.

Employers must collect employees' Sensitive Personal Data and Information (SPDI), which may include health records, financial records, and other details to process payrolls and other processes related to fulfilling employment contracts. Section 43-A of the IT Act, 2000, requires employers to put in place reasonable information security practices to protect employees against "unauthorised access, damage, use, modification, disclosure, or impairment" (MeitY, 2000).

Section 72-A of the IT Act, 2000, protects citizens against disclosure of SPDI against breach of lawful contract or without consent (MeitY, 2000). The IT Ministry has also adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules since 2011(MeitY, 2011). The Rules require corporates entities, body corporates, or anyone collecting, processing and storing personal data to comply with certain procedures (Phophalia, 2016).

The IT Act, 2000, applies to the whole country and therefore covers anybody who may suffer a data breach (MeitY, 2000). This is a glaring omission in the Personal Data Protection Bill 2019 (PDP). The PDP only covers legally defined employees covered by an employer-employee relationship (PDP, 2019). This leaves out self-employed workers, daily wage workers, or those in non-standard employment relationships (such as contractual workers or gig workers) who make up 81 per cent of the Indian workforce (ILO, 2018).

The PDP has been criticised on many counts. One critique is the lack of protection specifically for workers. Clause 13 of the PDP Bill 2019 exempts employers from seeking consent for collecting, processing, and storing personal data from employees (Mukhopadhyay, 2020). This exemption allows employers to collect, process, and use employees' data without their explicit consent and removes liability in any case of a data breach or misuse of data (Mukhopadhyay, 2020).

Crucially, worker collectivisation groups are not categorised as SPDI. Employers can, therefore, force employees to disclose their affiliations.

There is a lacuna regarding workers' data and data rights in the PDP and the new Labour Codes. The Indian legislature has passed legislation to reform the country's expansive and outdated labour laws. Protections for labour have been brought under four codes: Code on Wages; Code on Occupational Safety, Health, and Working Conditions; Code on Social Security; and Code on Industrial Relations (PRS Legislative Research, 2019). While this would have been an ideal time to establish workers' data rights and place limits on workplace surveillance and data collection, the codes fail to address any of these crucial issues.

Data protection regulations from other regions could serve as an example for India to follow. Personal data is defined quite broadly and includes names, personal identifiers, location data, even physical, physiological, genetic, mental, economic, cultural, or social identity under the General Data Protection Regulations (GDPR). Consent from the data subject is key to collecting processing and storing such data in both jurisdictions. The GDPR does allow employers to process employees' personal data "to perform an employment contract," "fulfill legal obligations," or to "further legitimate interests of the employer." However, these conditions are defined quite narrowly and require employers to weigh their interests against employees' privacy interests (Jodka, 2018).

Singapore's Personal Data Protection Act 2012 (PDPA) requires an employee individual's consent to collect, use, or disclose personal data. However, explicit consent is not required under certain circumstances. Data regarding an individual's employment, including management and termination, may be collected, processed, and disclosed if the individual is informed. However, explicit consent is not required from workers if data is for "evaluative purposes" (Lim et al., 2019). Additionally, employee data can be disclosed to a third party without the individual's consent in business transactions. However, employers

must notify employees about the transaction and personal data that was shared. Organisations are not required to notify or seek consent if personal data is to be used for investigation or proceedings. Proceedings generally relate to civil, criminal, administrative proceedings before a court, tribunal, or regulatory authority. Investigations, on the other hand, most likely refer to internal investigations within an organisation. Below is a table that compares India's PDP bill, with the EU's GDPR and Singapores' PDPA for a direct comparison around definitions and inclusions related to employee data.

	India PDP	European Union (EU) GDPR	Singapore PDPA
Eligibility	All Indians	All EU residents	All Singaporeans
Consent	Employers do not require consent to process workers' personal data.	Employers need informed consent from workers to process personal data. In the absence of consent must weigh employers interests against employees' privacy.	Employers need informed consent to collect, use, and disclose personal data but are exempted from gaining consent under a few conditions.
Employment Status	Only for workers covered by formal employer-employee relationships.	Personal data can be processed without consent to fulfill the employment contract. For all other -non-standard workers, consent is required.	All employees covered, even at the recruitment stage. Some sections do not cover -non-standard employment relationships.
Definition of personal data	Personal data defined as "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information."	Personal data defined broadly, and includes: names, ID numbers, location data, online identifiers, and even physical, physiological, genetic, mental, economic, cultural, or social identity.	Personal data is defined as "data, whether true or not, about an individual who can be identified from that data; or, from that data and other information to which the organisation has or is likely to have access."

	India PDP	European Union (EU) GDPR	Singapore PDPA
Definition of sensitive personal data	Sensitive personal data is defined as passwords, financial data, health data, official identifier, sex orientation, biometric and genetic data, trans or intersex status, tribe or caste, religious or political belief or affiliation.	Sensitive personal data is defined as racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, worker collectivisation membership, and genetic and biometric data.	Does not include a definition for sensitive personal data.

Figure1: Comparing India's PDP with EU's GDPR and Singapore's PDPA

5. Conclusion: Looking forward

Following the above outline of the specific risks associated with data collection and surveillance of workers, and the discussion of gaps in the existing legal protections for Indian workers, outlined below are the key issues that will need close attention as workplace monitoring practices unfold.

1. Strengthen PDP Bill 2019 and Labour Codes to address changing workplace dynamics

First, the proposed PDP Bill 2019 and Labour Codes should be strengthened to include issues around workplace surveillance. Currently, the proposed PDP Bill 2019 exempts employers from seeking informed consent prior to collecting, storing, or processing employee data. Additionally, regulatory capacity to enforce the PDP and hold companies accountable needs to be developed.

Second, the PDP Bill 2019 should recognise workers in non-standard employment. Only 22.8 per cent of the workforce in India is formally employed (Economic Survey, 2020). Non-standard employment relationships—including gig workers, the unorganised sector, and daily wage workers—should be included within the ambit of the PDP Bill 2019. Only the Code on Social Security recognises platform workers. However, the new Labour Codes make no mention of workers' data rights, nor do they address workplace surveillance.

The new Labour Codes make no mention of workers' data rights, nor does it address workplace surveillance.

2. Strengthen workers' ability to access data and information

Employers should be directed to ensure that workers are aware of data being collected and the purpose for which it is being collected. Transparency and the ability for workers to revoke consent need to be included. Conversely, employers make it extremely difficult for workers to access their personal data or company data that should be publicly available. Strategies to correct these information asymmetries and access need to be implemented. The PDP Bill 2019 and the IT (Amendment) Act 2008, should have provisions for workers to access their data. Directives from the Ministry of Corporate Affairs to make company data publicly available need to be strictly implemented. Processes should be simplified where possible. This information should be made available on online databases or be accessible through the Labour Department so that workers are able to easily access the data they require. Up until now, employers have been able to sidestep these requirements with severe implications for worker rights.

3. Strategise use of data

Extensive collection of worker data can have a detrimental impact on their agency and autonomy, but at the same time, access to data can be empowering for workers. There are several examples of workers using data to advocate for better working conditions.

The New York Taxi and Limousine Commission (TLC) commissioned a report based on administrative data submitted to them. Based on the report's findings, the New York City Council voted to put a cap on the number of app-based taxis on the road in 2018 (Parrot and Reich, 2018). This policy helped raise drivers' earnings and addressed road congestion too (Hawkins, 2019).

Workers should have access to crucial data like the company's financial records, as mandated by the Ministry for Corporate Affairs, so that they can advocate for better working conditions. Access should be complemented with the ability to strategically use the data to advocate for better working conditions. Workers should be supported with skills training initiatives that will help them access data and use it meaningfully. Workers' organisations and civil society organisations should aid with these initiatives.

Workers should be supported with skills training initiatives that will help them access data and use it meaningfully.

Endnotes

[1] Basudev Barman is a labour researcher around issues affecting platform workers in India. He recently authored a paper on the impact of COVID-19 on gig workers, including problematic data collection policies they are exposed to.

[2] Parvathi C.M is an expert on the garment industry and the experience of garment workers in Bangalore. She works as a programme officer at Cividep India, aiming to improve the working conditions of garment workers. (http://cividep.org/)

[3] Suhasini Singh is an expert on the garment industry in India. She is the India Country Representative at Fair Wear, which campaigns for a fairer way of producing clothing along global supply chains. (https://www.fairwear.org/)

[4] Rakhi Sehgal is the founder of Gurgaon Shramik Kendra (Gurgaon Workers' Centre) and Gurgaon Mahila Kaamgar Sangathan (Gurgaon Working Women's Collective). She is a consulting researcher with the International Labour Organisation (ILO) and has worked extensively as a labour activist in India.

[5] The Pinkerton National Detective Agency was a detective agency founded in 1850, and used to investigate and limit collectivisation in manufacturing industries in the United States.

Bibliography

1. Agrawal, Aditi (2020) Gig economy workers' collective questions use of Aarogya Setu, Medianama. Retrieved on 26 October 2020 from https://www.medianama.com/2020/06/223-ifat-aarogya-setu-gig-economy/

2. Aneja, Urvashi, Aishwarya Shridhar and Ria Singh (2019) Worker well-being on digital work platforms: A study of Olacabs and UrbanClap in New Delhi. Tandem Research. Available at https://tandemresearch.org/assets/Worker-Wellbeing-Tandem-Research-2019.pdf

3. Ajunwa, Ifeoma., Kate Crawford and Joel S. Ford. (2016) Health and big data: An ethical framework for health information collection by corporate wellness programs. The Journal of Law, Medicine and Ethics, vol. 44, issue 3 (September)

4. Ajunwa, Ifeoma., Kate Crawford and Jason Schultz. (2017) Limitless Worker Surveillance. California Law Review, vol. 5, issue, 3 (March)

5. Ajunwa, Ifeoma., and Daniel Greene. (2019) Platforms at work: Automated hiring platforms and other new intermediaries in the organization of work. Work and Labor in the Digital Age, vol. 33 (April)

6. Benjamin, Ruha. (2019) Race after technology. New Jersey: John Wiley and Sons.

7. Cardozo, Nate, Kurt Opsahl and Rainey Reitman (2016) Who Has Your Back? Protecting your data from government requests: Sharing Economy Edition. Electronic Frontier Foundation Report. Retrieved on 25 September 2020 from https://www.eff.org/files/2016/05/04/who-has-your-back-2016.pdf

8. Crawford, Kate (2013) The hidden biases in big data. Harvard Business Review. Retrieved on 25 September 2020 from https://hbr.org/2013/04/the-hidden-biases-in-big-data

9. Duggan, James, Ultan Sherman, Ronan Carebery and Anthony Mcdonnel (2019) Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM. Human Resource Management Journal, vol. 30, issue 1 (January 2020)

10. Government of India, Ministry of Finance (2020) Economic Survey 2019-2020. Available at https://www.indiabudget.gov.in/economicsurvey/

11. Hawkins, Andrew. J. (2019) New York City extends its cap on new Uber and Lyft vehicles. The Verge. Retrieved on 27 August 2020 from https://www.theverge.com/2019/8/7/20758796/nyc-uber-lyft-cap-extended-tlc-de-blasio

12. The Hindu (2012) 80 p.c garment workers come to Bangalore for sheer survival. The Hindu. Retrieved on 20 August 2020 from https://www.thehindu.com/news/national/karnataka/80-pc-garment-workers-come-to-bangalore-for-sheer-survival/article3898214.ece

13. Holder, Sarah. (2019) For Ride-Hailing Drivers, Data is Power. Bloomberg CityLab. Retrieved on 16 August 2020, from https://www.bloomberg.com/news/articles/2019-08-22/why-uber-drivers-are-fighting-for-their-data,

14. IFAT (2020) Covid-19 and Lockdowns: A Study About The Response to the Pandemic By the App-Based Companies,

The Unions and The Government. July 2020, on file with authors.

15. ILO (2018) Women and men in the informal economy: A statistical picture (Third edition) International Labour Office - Geneva. Available at: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_626831.pdf

16. India, Ministry of Electronics and Information Technology (2000) The Information Technology Act, 2000. Available at https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

17. India, Ministry of Electronics and Information Technology (2008) The Information Technology (Amendment) Act, 2008. Available at https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf

18. India, Ministry of Electronics and Information Technology (2011) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

19. India, Ministry of Electronics and Information Technology (2019) The Personal Data Protection Bill, 2019 (Bill no. 373 of 2019) Available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

20. ITUC (2020) 2020 ITUC Global Rights Index: The world's worst countries for workers. Available at https://www.ituc-csi.org/IMG/pdf/ituc_globalrightsindex_2020_en.pdf

21. Jodka, Sarah H. (2018) The GDPR Covers Employee/HR Data and It's Tricky, Tricky (Tricky) Tricky: What HR Needs to Know. Dickinson Wright. Accessed on 1 October 2020, from https://www.dickinson-wright.com/news-alerts/the-gdpr-covers-employee-hr-data-and-tricky

22. Jones, Sarah (2018) The Pinkertons Still Never Sleep. The New Republic, Retrieved on 25 September 2020 from https://newrepublic.com/article/147619/pinkertons-still-never-sleep

23. Kane, Gillian. (2014) Facts on India's Garment Industry. Clean Clothes Campaign. Available at: https://www.clean-clothes.org/resources/publications/factsheets/india-factsheet-february2015.pdf

24. Kar, Sanghamitra (2019) Women bag frontline roles in gig economy, but lag behind in wages. ET Tech, 30 July. Retrieved on 2 October 2020 from https://tech.economictimes.indiatimes.com/news/internet/women-bag-frontline-roles-in-gig-economy-but-lag-behind-in-wages/70439828

25. Kaur, Nehmat (2017) What Studying the Impact of Surveillance on Women Can Teach Us About Power. The Wire. Retrieved 26 September 2020 from https://thewire.in/culture/what-studying-the-impact-of-surveillance-on-women-can-teach-us-about-power

26. Lecher, Colin (2019) How Amazon automatically tracks and fires warehouse workers for 'productivity'. The Verge, 25 April. Retrieved on 29 September 2020 from https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

27. Lee, Min Kyun (2016) Algorithmic Bosses, Robotic Colleagues: Toward human-centered algorithmic workplaces. XRDS: Crossroads, The ACM Magazine for Students - The Future of Work, 23(2), 42-47

28. Lim, Ian., Li Wanchun and Nicholas Ngo. (2019) Employee data protection in Singapore. Retrieved 27 August 27 2020, from https://www.lexology.com/library/detail.aspx?g=4c9e6e94-5fad-4b66-afc3-db447e61c78a

29. Lyon, David (2001) Introduction, Surveillance Society: Monitoring everyday life, Open University Press: Buckingham. Pp 1-12.

30. Mateescu, Alexandra., and Aiha Nguyen (2019a) Explainer: Workplace Monitoring & Surveillance. Data and Society. Available at https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf

31. Mateescu, Alexandra., and Aiha Nguyen (2019b) Explainer: Algorithmic Management at the workplace. Data and Society. Available at https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf

32. Mukhopadhyay, Devdutta (2020) How does the Personal Data Protection Bill 2019 impact workers' rights? Retrieved 27 August 2020, from https://internetfreedom.in/workplace-surveillance-your-employer-could-be-watching-you/

33. Noble, Safiya (2018) Algorithms of oppression: How search engines reinforce racism. New York: New York University Press.

34. O'Neill, Cathy (2016) Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Crown Books.

35. Parrot, James. A., and Michael Reich. (2018) An earnings standard for New York City's app-based drivers: Economic analysis and policy assessment. Center for New York City Affairs

36. Peters, Jay. (2020) Whole Foods is reportedly using a heat map to track stores at risk of unionization. The Verge, 20 April. Retrieved 27 August 2020 from https://www.theverge.com/2020/4/20/21228324/amazon-whole-foods-unionization-heat-map-union

37. Phophalia, Zeenat (2016) Employee Data Protection In India: What Should Employers Be Aware Of? Retrieved 27 August 2020, from https://www.mondaq.com/india/data-protection/470538/employee-data-protection-in-india-what-should-employers-be-aware-of

38. Privacy International (2017) Case Study: The Gig Economy and Exploitation. available at: https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation,

39. PRS Legislative Research (2019) Overview of labour law reforms. Accessed on 1 October 2020, from https://www.prsindia.org/billtrack/overview-labour-law-reforms

40. Pundir, Pallavi (2020) Indian Employers are Using the Pandemic as an Excuse to Surveil Their Workers Even More. Vice. Retrieved 20 September 2020, from https://www.vice.com/en/article/y3zpag/india-surveillance-pandemic-data-rights

41. Ranganathan, Nayantara (2017) Caution! Women at Work: Surveillance in Garments Factories. Gendering Surveillance. Retrieved 01 August 2020, from https://genderingsurveillance.internetdemocracy.in/cctv/

42. Rao, Mohit M. (2019) The 'gig' economy is creating lakhs of jobs, but workers don't see a future. The Hindu, 30 August. Retrieved on 2 October 2020 from https://www.thehindu.com/business/Economy/the-gig-economy-is-creating-lakhs-of-jobs-but-workers-dont-see-a-future/article29299673.ece

43. Saleem, Shaikh Z. (2019) Your digital profile to affect credit score. Livemint, 21 March. Retrieved 27 August 2020, from https://www.livemint.com/money/personal-finance/your-digital-profile-to-affect-credit-score-1553090225093.html

44. Satariano, Adam (2020) How my boss monitors me while I work from home. The New York Times, 6 May. Retrieved on 29 September 2020 from https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html

45. Singh, Pooja (2020) Coronavirus: For many, work from home is never an option. Livemint, 18 March. Retrieved on 29 September 2020 from https://www.livemint.com/mint-lounge/business-of-life/for-many-work-from-home-is-never-an-option-11583769892323.html

46. Tandem Research (2020) Tracking Worker Surveillance: Covid-19 and Before: TANDEM RESEARCH PUBLIC. Retrieved on 30 September 2020 from https://docs.google.com/spreadsheets/d/1NNaz4Q3P8rf7gSG50SA4Ru4OlVqCGqnq_Y_f0_evrao/edit#gid=0

About the authors

Iona Eckstein is a Research Associate for the Future of Work & Learning initiative at Tandem Research. Her research focuses on the intersection between technology and labour. She is also interested in feminist perspectives on the future of work.

Zothan Mawii is a Research Fellow at Tandem Research. Her research interests lie at the intersection of technology, work, and gender in the global south. She is currently working on a project exploring Indian women's experiences of working in the digital economy.

Imprint

© 2020 Friedrich-Ebert-Stiftung India Office
K-70-B, Hauz Khas Enclave | New Delhi-110016 India

Responsible
Wulf Lapins | Resident Representative
Anup Srivastava | Program Adviser

+ 91 11 26561361-64
www.fes-india.org
FriedrichEbertStiftungIndia

To order publication:
info@fes-india.org

The Friedrich-Ebert-Stiftung is the oldest political foundation in Germany. Founded in 1925, it is named after Friedrich Ebert, the first democratically elected president of Germany. FES is committed to the advancement of both socio-political and economic development in the spirit of social democracy, through civic education, research, and international cooperation.

This publication is part of the research paper series Shaping the Future of Workers in Asia, a regional project coordinated by the FES Office for regional cooperation in Asia. This publication is published by the FES Office India

www.fes-asia.org

EFQM Committed to excellence