Institute for Public Policy Research

WATCHING ME, WATCHING YOU

WORKER SURVEILLANCE IN THE UK AFTER THE PANDEMIC

Henry Parkes

March 2023

ABOUT IPPR

IPPR, the Institute for Public Policy Research, is the UK's leading progressive think tank. We are an independent charitable organisation with our main offices in London. IPPR North, IPPR's dedicated think tank for the North of England, operates out of offices in Manchester and Newcastle, and IPPR Scotland, our dedicated think tank for Scotland, is based in Edinburgh.

Our purpose is to conduct and promote research into, and the education of the public in, the economic, social and political sciences, science and technology, the voluntary sector and social enterprise, public services, and industry and commerce.

IPPR
14 Buckingham Street
London
WC2N 6DF
T: +44 (0)20 7470 6100
E: info@ippr.org
www.ippr.org
Registered charity no: 800065 (England and Wales),
SC046557 (Scotland)

The contents and opinions expressed in this paper are those of the authors only.

The progressive policy think tank

CONTENTS

ABOUT THE AUTHORS

Henry Parkes is a senior economist at IPPR.

ACKNOWLEDGEMENTS

The author would like to thank Kirstie Ball, Eliot Bendinelli, Reid Blackman, John Chadfield, Katherine Holden and Mary Towers for their insight into the subject matter. At IPPR, the author would like to thank George Dibb, Richard Maclean and Rachel Statham.

Further, thanks to our focus group participants for sharing their thoughts and experiences.

The report was financially supported by the Alex Ferry Foundation, but the views expressed in the report are those of IPPR only.

Download
This document is available to download as a free PDF and in other formats at:
http://www.ippr.org/research/publications/worker-surveillance-after-the-pandemic

Citation
If you are using this document in your own writing, our preferred citation is:
Parkes H (2023) *Watching me, watching you: Worker surveillance in the UK after the pandemic*, IPPR.
http://www.ippr.org/research/publications/worker-surveillance-after-the-pandemic

SUMMARY

Worker surveillance is as old as work itself, but new technology is making it easier and cheaper than ever. This includes both the ability of employers to collect employee data, and for that data to be interpreted by machines to inform decisions in the workplace or for decisions to be made entirely by machine, referred to as 'automated decision making' (ADM). In some cases, these practices go beyond a reasonable expectation towards something more intrusive and potentially harmful, for example minute-by-minute tracking of workers' physical movements through to facial recognition technology, assessing whether a worker is concentrating on the task at hand.

Data suggests that workplace surveillance practices have hugely expanded during the pandemic and are here to stay – though there are prominent data gaps around who, and to what extent, people are affected. Unaddressed, the spread of these practices could leave workers permanently worse off, with the most adverse outcomes likely to impact those with the least power in the labour market, such as the young and certain ethnic groups. There is a tangible risk of normalisation: policies and practices which would have been seen as extraordinary before the pandemic could become acceptable.

Workers' protection against excessive surveillance is governed by a strong legal framework in the form of the UK's General Data Protection Regulations. Its implementation, however, relies on employers having sound judgement, and good faith that they understand and act on complex guidance prior to the decision to monitor. There are also rules governing the use of ADM which rely on good faith that workers will be told when it is being used, with a right to human intervention for significant decisions.

Evidence shows that excessive surveillance can harm workers' wellbeing, increase staff turnover and lead to counter-productive work behaviours, such as company sabotage. This can be mitigated by being transparent on monitoring purpose and using less invasive monitoring techniques. There are, however, legitimate use cases around ensuring health and safety and training, alongside fulfilling some regulatory requirements.

We find that worker surveillance has the potential to increase power imbalances between workers and employers. It can undermine unionisation efforts in the present, and the threat of future surveillance can be used to exert control over employees. When employees don't have access to the data collected through monitoring, it gives employers an unfair advantage in negotiations and performance conversations.

Further automated decision-making creates a higher risk of 'algorithmic bias'. Decisions made by algorithms are complex, lack transparency and are at risk of favouring certain groups. The 'black box' nature of such technology requires managers to make a leap of faith that such systems are not discriminatory, but there are currently limited obligations for those who develop or deploy this technology to ensure this is the case.

We make a number of recommendations for policymakers that seek to prevent a damaging power shift from workers to employers, reduce the risks of algorithmic bias, and increase the collection of data on this new technology.

- **Employers should be more transparent in their monitoring decisions, and employees empowered to challenge where appropriate –** including through an easier right of redress through a single workers' rights enforcement body.
- **Employers should give workers access to the data which is collected on their activities –** to empower workers and their representatives in negotiations.
- **Government should consider whether some monitoring practices should be outlawed –** for example keystroke monitoring which is unlikely to ever be acceptable.
- **Give unions access to workplaces –** to ensure fair monitoring practices on the ground and provide direct challenge as required to those responsible for data protection.
- **Government should champion algorithmic accreditation –** to incentivise firms to develop algorithms which do not discriminate, and help employers do the right thing by only using algorithms which do not perpetuate bias.
- **Government should strengthen protections against automated decision-making** – including the right to a personalised explanation of how an algorithm reached a decision where the impact is significant, such as in pay or promotion decisions.
- **We need better data collection from government to understand the scale and scope of worker surveillance –** collected through the Labour Force Survey.

Taken together these policy recommendations would help redress the balance of power between workers and employers. They would ensure that when surveillance is happening it is fair and proportionate as the law intended, respecting worker's fundamental rights.

1. INTRODUCING WORKER SURVEILLANCE AND THE LEGAL CONTEXT

Workers have always been monitored by their bosses in some form, and to some extent this is expected and necessary; employers need to know that their employees are working when they say they are.

But new and emerging technology is making this easier and cheaper than ever before, both in terms of the ability of employers to collect data on employees but also for that data to be interpreted by software to develop measures of 'performance' which can be used to make decisions in the workplace.

There can be benefits, for instance around training and protecting workers' health and safety. But in some cases, this can go beyond reasonable expectations towards something more intrusive and detrimental. This includes a wide range of technologies from automated e-mail monitoring and webcam technology which can assess your mood, through to physical technology which monitors your every move – which has controversially been deployed in some warehouse settings.

Surveillance has hugely expanded during the pandemic and is here to stay. It has the potential to creep further in terms of the *depth* in which people are monitored and the *breadth* of workers affected. This is a concerning trend that needs more attention from policymakers and the public more widely. Unaddressed, it could leave workers permanently worse off financially, physically or mentally with outcomes likely to be worse among groups with the least power in the labour market. There is a risk of 'normalisation'; policies and practices which would have been seen as extraordinary before the pandemic could become acceptable post-pandemic.

This paper seeks to shine a light on the issue of workplace surveillance and related automated decision making in a post-pandemic context. Supported by expert interviews, desk research and a series of focus groups with affected workers, we seek to understand where we are now, and why policymakers and the public should pay attention to this subject.

Crucially we consider the policy implications: we make eight core policy recommendations which, if implemented, could help shift workers away from a future of disempowerment and towards something much fairer, harnessing technology – where appropriate – for the benefit of all.

DEFINING EXCESSIVE SURVEILLANCE INVOLVES VALUE JUDGEMENTS

One definition provided by the United Tech and Allied Workers Union, adapted from Lyon (2001), defines employee surveillance as 'the monitoring of employees and collection of employee data, identifiable or not, for the purpose of influencing and managing the behaviour of those being monitored' (UTAW no date).

By this definition, surveillance may not be inherently harmful – though we focus on surveillance which could be seen as excessive or disproportionate, recognising such terms include value judgements. This is more challenging to define, but excessive surveillance could be thought of as 'surveillance which involves the collection of more data than is justifiable to meaningfully monitor performance or compliance, whilst respecting the fundamental rights of the worker'.

SURVEILLANCE CAN TAKE BOTH DIGITAL AND PHYSICAL FORMS

Surveillance exists in both digital and physical domains as outlined in table 1.1.

TABLE 1.1: FORMS OF WORKPLACE SURVEILLANCE

Digital monitoring	Physical monitoring
• Keylogging and mouse tracking. • Recording and screenshotting screens. • Webcam monitoring and checking physical presence and facial expressions. • Application usage recording. • Reading and 'analysing' instant message and email usage. • Recording telephone calls • Monitoring social media usage (including outside of working hours). • Calendar monitoring	• Key cards and fingerprint access. • Vehicle monitoring and dash cameras. • Body-worn cameras. • Using handheld or wearable devices to monitor and record the exact location and movements of employees within the workplace. • GPS and mobile device tracking. • Physiological tracking (eg heart rate monitors). • Drug testing. • Bag checks.

Source: Author's analysis

Some forms of workplace monitoring may be mandatory, for example to fulfil regulatory requirements, such as identifying insider trading in the financial sector, or key card access to restrict access to an office space. Most monitoring is restricted to working hours, although there is a trend towards monitoring outside of these (Thompson et al 2020).

However, most monitoring is an active choice for employers because it is perceived as advantageous in some way to the organisation. Examples of more controversial worker surveillance are found among the boxes in this chapter.

BOX 1.1: TRACKING WAREHOUSE WORKERS BY THE MINUTE

Leaked documents filed with the US National Labor Relations Board have exposed Amazon's monitoring practices in one warehouse in Staten Island, New York. The papers reveal that workers are tightly monitored, with every minute of 'time off task' (TOT) recorded with radio-frequency handheld scanners used to track customer packages.

Examples and sample spreadsheets show Amazon tracking, down to the minute, the amount of time individual workers spent in the bathroom and infractions such as 'talking to another Amazon associate,' going to the wrong floor of a warehouse, and, as an example, an 11-minute period where a worker 'does not remember' what they were doing.

Managers were asked to identify 'top offenders' within each team with the greatest TOT, who would be expected to account for their whereabouts in every period of inactivity or face disciplinary action. The documents indicate Amazon used video surveillance footage to corroborate and/or disprove claims made by workers for these time periods.

Workers can be fired for breaching certain TOT thresholds, for example accumulating 30 minutes time off task on three separate days in a one-year period. (Gurley 2022)

In the digital realm, worker monitoring is often available in software packages

In an office environment, surveillance is enabled in practice for many employers through 'productivity suites'. Such suites typically offer to employers a package of monitoring tools and a streamlined approach to capturing a variety of data on employees and their computer use. In some cases these software suites seek to synthesise the data collected to provide some sort of assessment of how the employee is performing.

TABLE 1.2: WORKER MONITORING SUITES AND THEIR FEATURES

Brand	Software monitoring	Remote control takeover	Keystroke logging	Screen monitoring	Internet monitoring/ filtering	Call tapping	Location tracking	Webcam surveillance	Audio recording	Email monitoring	IM monitoring	Mobile device access	User action alerts	Time-tracking
ActivTrak	✓			✓	✓			✓					✓	✓
Aware	✓													
CleverControl	✓		✓	✓	✓	✓		✓	✓	✓	✓			✓
Crossover	✓		✓	✓				✓						✓
Desktime	✓			✓	✓									✓
Digitalendpoint	✓		✓		✓			✓	✓			✓	✓	
Efficientlab	✓		✓	✓	✓					✓	✓		✓	✓
FlexiSPY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Hubstaff	✓		✓	✓	✓		✓					✓		✓
iMonitorSoft	✓	✓	✓	✓	✓			✓	✓	✓	✓		✓	✓
InterGuard	✓		✓	✓	✓		✓			✓	✓	✓	✓	✓
Kickidler	✓	✓	✓	✓	✓									✓
NetVizor	✓	✓	✓	✓	✓				✓	✓	✓		✓	✓

Source: Migliano (2022)

The development of such packages offer greater convenience for employers, enabling multiple monitoring methods through one piece of software, and could lead to creeping surveillance practices - that is, a package could be primarily purchased for one sort of monitoring could then be used to introduce other means of monitoring.

BOX 1.2: AN ALWAYS-ON VIDEO SERVICE WHICH PHOTOGRAPHS WORKERS UP TO EVERY MINUTE

Sneek is group video conference software which is 'always on' by default. The software gives workers and managers access to a 'wall of faces', which stays on throughout the work day and features constantly-updating photos of workers taken through their laptop camera every one to five minutes, with the frequency set by managers. Managers and workers can click on photos from the 'wall' to start an instant video conversation with the person clicked on, although this can be turned off. (Holmes 2020) Although marketed as a collaboration tool to help bring together remote teams, it is easy to imagine how it could be misused by unscrupulous firms to exert worker control and violate worker privacy.

SURVEILLANCE PRACTICES HAVE HUGELY EXPANDED DURING THE PANDEMIC

As millions were forced to work from home during the pandemic, there was a rapid expansion of monitoring practices as anxious employers sought to keep a closer eye on their staff as they were forced to work from home (Blum 2022). Although no data are systematically collected to understand the prevalence of the practice and how it has changed, there are numerous ways to glimpse at the issue and understand the scale of the increase.

Analysis of search terms

Considering the growth in search behaviour since the pandemic as one way of understanding the growth in workplace surveillance.

TABLE 1.3: GROWTH IN RELEVANT SEARCHES RELATING TO WORKER SURVEILLANCE

Search term	Increase in March 2020 from pre-pandemic baseline	Increase up to September 2022 from pre-pandemic baseline
Employee monitoring software	102%	71%
Employee tracking	45%	42%
How to monitor employees working from home	1,689%	383%
Monitoring employees in the workplace	-5%	26%
Best employee monitoring software	140%	201%

Source: Adapted from Migliano (2022)
Note: Analysis is of English-speaking world and so is skewed towards US-based workplaces.

When the pandemic began there was a huge surge in relevant searches relating to workplace surveillance, for instance for 'how to monitor employees from home' and 'employee monitoring software' – but 18 months later we still see significantly higher levels of search than before the pandemic. For instance, between the first quarter of 2020 and September 2022, searches for 'employee monitoring software' remain 71 per cent higher and ‘employee tracking’ remain 42 per cent higher (Migliano 2022).

Polling

Polling from the Trades Union Congress (TUC 2022) shows that in the UK:

- Almost three in 10 (28 per cent) agree monitoring and surveillance at work has increased since the pandemic – and young workers are particularly likely to agree (36 per cent of 18–34-year-olds).
- There has been a notable increase in workers reporting surveillance and monitoring in the past year alone (60 per cent in 2021 compared to 53 per cent 2020).
- More workers are reporting monitoring of staff devices (24 per cent to 20 per cent) and monitoring of phone calls (14 per cent to 11 per cent) in 2021 compared to 2020.

However, we know that more systematic data collection is needed. This polling is the most recent data available at time of writing, and can only provide a snapshot. To understand trends and who is most affected, data on workplace surveillance should be collected more systematically. We would argue this data collection is key to understanding how this area is developing and to be better understand the need for action.

BOX 1.3: FACIAL RECOGNITION TECHNOLOGY WHICH ASSESSES CONCENTRATION

Japanese tech firm Fujitsu has developed an AI model which detects small changes in muscle movements in a person’s facial expressions, for example a tense mouth or how intently somebody is staring, to assess whether they are concentrating. The technology has a claimed accuracy rate of 85 per cent based on testing in the US and Asia, and the company plans to deploy the technology in settings such as classes, meetings and in sales (Keane 2021).

The pace of adoption into new areas creates risks

This seemingly rapid adoption of surveillance technology is a cause for concern, as the circumstances under which this expansion occurred were suboptimal due to the pandemic. Interviewers highlighted there was limited time for employers to think through any legal and privacy implications of monitoring, with limited opportunity for consulting the workforce in line with best practice. At the same time workers, who were also living through the pandemic, were not well placed to resist such practices as many had concerns about job security, as well as limited information to understand whether what was being imposed was legal.

Our focus group found instances where surveillance had been introduced overnight during the pandemic with little support on offer for workers, and very little consultation.

> ***“During the pandemic when we were working from home and it was implemented from the get go. There was no HR to speak to and there was no one to take your issue to… You just had to get on and do it”***
> Focus group participant

Beyond surveillance, there is a growing risk of employees’ time being encroached

The growth of home and hybrid working has blurred the lines between the workplace and home, and similarly blurred the boundaries between working and non-working time. As such, there is a growing risk of workers being expected to be ‘on-call’ and are increasingly responding to emails out of hours (CIPD 2021).

Research has shown that just the *anticipation* of potential emails which could require a response is a stressor which prevents workers from 'switching off' with associated negative impact on worker wellbeing (Sanfilippo 2023).

WORKER MONITORING IS LAWFUL, BUT DEPENDS ON SUBJECTIVE JUDGEMENTS

The basis on which worker surveillance is legal is largely determined by the UK's General Data Protection Regulations (GDPR), incorporated directly from EU law. The rules are complex and include considerable scope for judgement by employers. Although there are six 'legal bases' for processing personal data in the workplace, new guidance from the Information Commissioner's Office (from which this section heavily draws) show some routes are more applicable than others (ICO 2022).

1. **Consent: If the worker freely gives consent to have their data collected.** The word 'freely' matters here; the ICO advise that in an employment context, it is unlikely to be an appropriate route because of the imbalance of power between workers and employers, meaning that 'workers are likely to feel that they have no choice but to give [the employer] consent.' They note consent could be appropriate if 'workers have a genuine choice and control over monitoring'. This is different from GDPR's predecessors where consent alone was often relied upon by employers through generic contractual or policy statements (Woods 2019).
2. **Contract: If the monitoring is necessary for a contract an employer has with the worker.** The word 'necessary' is important here, and implies there should be no other way to achieve this aim. The ICO surmise 'whilst scenarios may exist where [monitoring] it is the only way for the employer to fulfil their side of a contract, it is hard to envisage'.
3. **Legal obligation: If the monitoring is necessary for you to comply with the law in some way.** For instance if a logistics company needs to monitor driving time, speed and distance to comply with the rules on drivers' hours.
4. **Vital interests: If the monitoring is necessary to protect someone's life, for use in emergencies.**
5. **Public task: If the monitoring is necessary to perform a task in the public interest, mostly relevant to public authorities.** As with the 'contract' basis, it must be necessary, ie there should not be 'a less intrusive way to achieve the same purpose'.
6. **Legitimate Interests: If monitoring is necessary for the employers 'legitimate interests'.** This lawful basis is the most flexible and can apply in a range of circumstances. The ICO advises employers that they must 'balance [their] legitimate interests and the necessity of the monitoring' with the 'interests, rights and freedoms of workers, considering the particular circumstances', noting that this is different to other lawful bases because it does not assume the interests of the workers and the employer are balanced.

   The 'legitimate interests' question can be broken down into three tests.

   - Purpose test – is there a legitimate interest behind the processing?
   - Necessity test – is the processing necessary for that purpose?
   - Balancing test – is the legitimate interest over-ridden by the person's interest, rights or freedoms?

   Employers are required by law to assess each test prior to monitoring and to document this decision internally.

There are some grey areas as to whether monitoring is lawful, particularly through the 'legitimate interests' basis, in particular when considering the 'balancing test' and the relative weight attached to the workers' 'interests, rights and freedoms'. These require an unbiased assessment of the impact surveillance practices have on workers wellbeing and their wider rights to privacy, against the benefits of monitoring.

Further, in instances where monitoring is likely to cause 'high risk to workers' and other people's interests' then a data protection impact assessment (DPIA) must be undertaken, and other lower risk circumstances they should be 'considered'. A DPIA is a detailed document which outlines the nature, scope, context and purposes of any processing – which shows it is proportionate and in line with data protection principals, with mitigations in place where there is a risk of inappropriate disclosure.

It is worth noting that although the circumstances under which a DPIA is necessary are wide (see table 4 below), and they demand a lot of detail and consideration – there is no requirement for these to be published or even shared amongst workers although workers should always be consulted. The requirements depend on employer's being compliant, and there are limited routes for non-compliance to be identified beyond legal challenge.

TABLE 4: CIRCUMSTANCES IN WHEN A DATA PROTECTION IMPACT ASSESSMENT SHOULD BE COMPLETED OR CONSIDERED

Compulsory	Should consider
• Using systematic and extensive profiling or automated decision-making to make significant decisions about people. • Processing special-category data or criminal-offence data on a large scale. • Systematically monitoring a publicly accessible place on a large scale. • Using innovative technology in ombination with any of the criteria in the European guidelines. • Using profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit. • Carrying out profiling on a large scale. • Processing biometric or genetic data in combination with any of the criteria in the European guidelines. • Combining, comparing or matching data from multiple sources • Processing personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines. • Processing personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines. • Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them. • Processing personal data that could result in a risk of physical harm in the event of a security breach.	• Conducting evaluation or scoring. • Automated decision making has been used with significant effects. • Systematic monitoring. • Processing of sensitive data or data of a highly personal nature. • Processing data on a large scale. • Processing of data concerning vulnerable data subjects. • Innovative technological or organisational solutions. • Processing that involves preventing data subjects from exercising a right or using a service or contract.

Source: ICO (2022a)

AUTOMATED DECISION MAKING AND EMPLOYERS' RESPONSIBILITIES

Increasingly sophisticated artificial intelligence and machine learning techniques mean that more complex decisions are being made by machines affecting everything from task allocation and work scheduling, to pay and progression. This goes beyond worker monitoring and towards a greater role for automated decision-making and 'algorithmic control'. We discuss in the next chapter the potential implications of this for workers.

GDPR offers specific protection around the use of such automated decision-making (ADM) where the decision-making has a 'legal or similarly significant effect'. In these cases employers should (ICO 2022):

- give workers information about the processing
- introduce simple ways for them to request human intervention or challenge a decision
- carry out regular checks to make sure their systems are working as intended.

The guidance emphasises that human reviewers must be willing to challenge the recommendation made by ADM and involvement should not be tokenistic, and they should have the 'authority and confidence' to challenge the decision, and should take account of 'additional factors' which may be relevant to the decision. As with the guidance around monitoring, it requires sound judgements by employers to be used legally and transparently.

There are other relevant legislation which can provide protection around algorithmic processing, for example the Equality Act 2010, which provides protection against discrimination on the basis of protected characteristics (which includes discrimination facilitated by algorithm), or the Health & Safety Act 1974 which states employers have to reduce or remove stress 'as far as is reasonably practicable'.

The next chapter considers the effects of surveillance for workers, employers and the relationship between them.

2.
WHY SHOULD WE CARE?

Given the presence and growth of worker surveillance, we seek to understand its potential effects for workers, employers and the power dynamics between them.

WORKER SURVEILLANCE CAN DRIVE POOR OUTCOMES

There is substantive evidence collected since the 1980s which suggests that worker surveillance can have a negative effect on workers.

- **Decreased job satisfaction and increased workplace stress.** Excessive monitoring is stressful for employees and can reduce enjoyment of work. A recent meta-analysis examining the relationship between worker surveillance and other worker variables found that surveillance decreased job satisfaction and increased workplace stress controlling for other characteristics (Siegel et al 2022).
- **Increased risk of physical health conditions.** Other evidence has suggested a link between worker monitoring and development of physical health conditions: namely repetitive strain injury (Nahgrang et al 2011) and musculoskeletal discomfort in the context of call-centre workers (Sprigg et al 2007).
- **Decreased organisational trust.** A recent survey found that three-quarters of workers thought that trust would decline if monitoring was introduced in their workplace (CIPD 2020)

Focus group participants told us they were left with feelings of paranoia from constant monitoring, or the threat of it.

> ***"You feel guilty for the smallest things, like going to the toilet…just taking a breather for like five minutes. You just feel like someone's watching you…someone probably thinks you're doing something else even though that's not what you're doing. So I find myself, when I'm working from home, I don't stand up and I just stay in my seat the whole time, and yes you're just really paranoid with it even though you're not doing anything bad, you are getting things done – but it sort of puts the fear inside you and I don't like that."***
>
> Focus group participant

Others highlighted that whether monitoring contributed to stress depended on the management style of the employer

> ***"Some [managers] are very relaxed but some really like to micromanage you, and those more …draconian micromanagers can cause extreme stress and make you feel quite paranoid. And that is a very serious issue when that starts to happen"***
>
> Focus group participant

IMPACTS ON WORKER TURNOVER AND PRODUCTIVITY

Given the established relationship between job satisfaction and turnover (Reukauf 2018), we would expect that worker surveillance would lead to higher turnover through the channel of decreased job satisfaction and lower commitment, with all the associated costs of recruitment and training.

A global survey of 7,600 businesses found between the start of the pandemic and August 2021, firms with ‘plans to monitor employee productivity’ were more than 80 per cent more likely to report increased turnover compared to those businesses with no such plans (VMWare 2021).

Focus group participants highlighted the self-defeating role which monitoring could have on morale.

> ***“I understand about the cost implications. I understand about … the competitive edge and all that. But I think that if you treat people like robots, treat them like machines, I don’t think it’s ultimately a good thing for any business.” “They’re using this [monitoring] to compensate for management’s own failings … I think a lot of it’s unnecessary and it will damage morale.”***
>
> Focus group participants

For industries where recruitment and training are easier, we would expect retention to be a less significant consideration for employers. In industries where surveillance is already widespread (such as call centres), our focus groups found there may be more acceptance from workers themselves and so these effects may be minimised.

> ***“I don’t mind it, I accept it … what choice do you have? Like I say, you get on with it.”***
>
> ***“I kind of understand why they need to, it’s a big organisation and unfortunately you get colleagues who work really hard and then colleagues who maybe try and push the boundaries.”***
>
> Focus group participants

RESISTANCE AND ‘COUNTER-PRODUCTIVE WORK BEHAVIOURS’

Given what workplace surveillance sets out to achieve, it is perhaps surprising to find evidence that excessive surveillance can give rise to greater deliberate negative employee behaviour such as company sabotage and deliberate waste, so-called ‘counter-productive work behaviours’.

A recent study summarises a range of ‘resistant’ behaviours which can arise through worker monitoring (Ball 2021).

- Utilising monitoring processes and outcomes to create their own, informal social orders within the workplace which ran counter to the version put forward by management.
- Deliberately subverting managerial values.
- Sabotaging customer interactions.
- Developing their own ‘workarounds’ to improve monitoring statistics.
- Exploiting the system’s weaknesses.
- Turning the tables on management by using ‘reverse surveillance’.

Two recent studies in the US found that employees who were more closely monitored were more likely to break employee rules, including: cheating in a test, stealing equipment, and deliberately working at a slower pace – despite these things being directly observable by managers (Thiel et al 2022). This could be attributed to the desire for employees to ‘retaliate’ against employers for not trusting them in the first place. Other studies have found that those in higher autonomy more professional roles are more likely to respond to surveillance with counter-productive work behaviours, as they have more scope to sabotage (Holland et al 2015). Correspondingly, our focus groups highlighted that in more tightly monitored work settings scope for sabotage or avoidance felt very limited.

Interviewees highlighted that worker efforts around counter-surveillance can lead to a game of 'cat and mouse' between those doing the surveillance and those seeking to avoid surveillance – work activity which would contribute very little to worker productivity.

The effects of monitoring depend on its purpose, transparency and invasiveness, and workers identify some benefits

The extent to which surveillance will be perceived negatively by employers, affecting job satisfaction, turnover and leads to counter-productive work behaviours, depends on a number of factors, the most critical of which identified by Ball (2021) in the literature are the following.

- **Monitoring purpose:** For example, worker monitoring for the purposes of genuine training and development is very different from if monitoring appears to be for punitive purposes . Data collection where there is no explicit purpose can also result in negative attitudes from employers.
- **Invasiveness:** Monitoring of data on whole teams rather than individuals are preferred by workers, as is task-based monitoring as opposed to location or person-based monitoring. Employees perceive monitoring as less intrusive if they can control when it happens, and giving employees ability to turn off monitoring can result in better performance.
- **Transparency:** There are strong positive relationships between the transparency of electronic monitoring and perceptions of fairness and task satisfaction.

A further related factor identified by interviewees is *how* the technology is introduced. Whether it is in meaningful consultation with workers or if imposed from above can affect both perceived monitoring purpose and transparency. As such, monitoring which is less invasive, is transparent and has a purpose which is clear to employees and management could reduce the risks identified above.

Our focus groups mirrored this emphasis on purpose in particular, with some participants identifying perceived benefits around safety and training.

> ***"The benefits for my company are those calls are monitored, we speak to a lot of vulnerable customers, it's really important we're giving the right advice to these customers. From a training point of view it's really important that if there are any training needs they get fixed quickly so we're not impacting any more customers than we need to"***
>
> ***"Any hard breaking, speed, it's all logged, monitored. And I mean some lads have had to go on a driving test, they have a league each week of drivers who are speeding or whatever. They send you out with a driving instructor to put you right, it's a good thing I suppose"***
>
> **Focus group participants**

However transparency was not always there, with some workers saying they didn't know precisely what was monitored in their workplaces.

> ***"I don't know how much they monitor, that's a real concern to me. I haven't always worked in retail, it's very fast paced there's not a lot of time for anything really. I'm assuming that they're not monitoring as much as they would like to, but I really don't know, and they can spring something on you … so you know it's very disconcerting."***
>
> ***"If you ask me I don't think that conversation [about monitoring] has actually been had. Like, literally ever since I have joined work I don't think, even with HR, or even if I've done any training, it has never actually been brought up, your rights in terms of surveillance. I don't think that's something that's been talked about and it's something which should be talked about actually."***
>
> **Focus group participants**

ACCESS TO INFORMATION AND POWER IMBALANCES

In most the cases, the reams of data collected during workplace monitoring can only be accessed by the employer and not the employee. This creates an inherent imbalance, as employers are able to use this data selectively to penalise the employee, for example to justify disciplinary action, or otherwise make decisions which affect them. But employees are not always able to use that same data to support their own goals or make their own arguments, for example in negotiation or in making the case for a promotion.

This one-way flow of data leaves workers in a weaker position and is likely to exacerbate existing inequalities if those at the lower end of the labour market are more likely to have their work activities recorded and encoded into digitally stored data, or 'datafied'. If workers had access to this information, it could be empowering.

WORKER SURVEILLANCE CAN HELP EMPLOYERS EXERT CONTROL OVER WORKFORCES

Workplace surveillance has fuelled demand for unionisation in some contexts (Greene 2021) but surveillance practices can undermine worker organising. Surveillance means those seeking to unionise can be more easily identified, and organising networks potentially broken up as has been alleged in some Amazon warehouse settings in the US (Palmer 2021).

Further, in our focus groups we heard of *threats* of increased surveillance being used as a stick by managers.

> ***"I've recently had a particularly draconian manager, who liked to refer to the technology, but when she has been saying "we'll get the cameras on you" and that sort of thing, it does affect the way you work."***
>
> Focus group participant

We also heard from interviewees that surveillance can be applied selectively 'as a form of retribution' to intimidate or otherwise seek to discipline staff who were perceived to be causing issues in the workplace.

AUTOMATED DECISION MAKING AND RISKS OF ALGORITHMIC BIAS

Data collected through workplace monitoring are 'the fuel to fill the tank of algorithmic management tools, which can make automated or semi-automated decisions affecting the workforce' (Gaudio 2021). Increasingly sophisticated artificial intelligence and machine learning techniques mean that more complex decisions are being made, or considerably assisted by, machines affecting everything from task allocation and work scheduling, to pay and progression. This goes beyond worker surveillance and towards a greater role for 'profiling' (the automated processing of data to make individual judgements or predictions), automated decision-making and 'algorithmic control'.

Although such automated decision-making and profiling could have clear efficiency benefits, it also raises the risk of 'algorithmic bias'. Previous IPPR research has highlighted the risk that decisions made by algorithms are by their nature complex and lack transparency, and are at risk of favouring certain groups (Roberts et al 2019). The 'black box' nature of such technology requires managers to simply trust that such systems are not discriminatory; but there are currently limited obligations for those who develop or deploy this technology to ensure this is the case. Use of algorithms may therefore facilitate discrimination under the Equality Act (CDEI 2020). Further, interviewees highlighted the risk that employers can 'hide behind' algorithms, with their use as a defence for discriminatory practices.

Proponents argue that algorithms, if well designed, should be neutral and their use will actually eliminate the bias which is common in human decision-making, but recent history has highlighted, where algorithms are not achieving this goal. (See box 2.1).

BOX 2.1: ALGORITHMIC BIAS IN ACTION

In summer 2020, the Department for Education employed an algorithm to estimate student grades in the absence of exams due to the pandemic. The algorithm looked at the recent historical grade distribution of each school and then decided a student's grade on the basis of their ranking within the school (Kolkman 2020). However, less weight was placed on past performance in schools with smaller classes, which disproportionately benefitted those at private schools (ibid), a form of algorithmic bias. The resulting outrage forced the government to change tack, resulting in the use of teacher assessment grades rather than those determined by the algorithm.

As such, to realise the benefits of algorithmic decision-making it is essential to understand how bias can be identified and prevented.

SOME WORKERS MAY BE MORE EXPOSED TO SURVEILLANCE PRACTICES THAN OTHERS

At present there are no data available to systematically understand the likelihood of surveillance, however we can identify a number of 'risk factors' which may make invasive surveillance more likely.

- For lower-skilled roles, worker retention may be perceived as less critical for employers, making surveillance relatively more attractive an option.
- For roles with lower levels of employee trust, surveillance may be more likely to be employed. Although there are limited available data on employer trust, we consider low worker autonomy as a proxy for this[1]
- If a workplace is non-unionised, the likelihood of worker consultation or the ability for employers to resist excessive surveillance are lower. According to research by Prospect, union members are twice as likely as non-union members to be consulted on the introduction of workplace monitoring software. (Prospect, 2021)

Our analysis of these risk factors using available survey data (Understanding Society) shows a complex picture.

[1] We measure this as workers self-reporting having little or no autonomy in three or more of the following aspects of work: job tasks, work manner, pace and task order.

TABLE 2.1: PREVALENCE OF WORKER SURVEILLANCE ‘RISK FACTORS’ AMONG DEMOGRAPHIC GROUPS

	Gender		Ethnicity					Age				
	Men	Women	White	Mixed	Asian	Black	Other	16-29	30-39	40-49	50-59	60+
Low autonomy	16%	19%	18%	22%	14%	21%	22%	25%	14%	14%	17%	18%
Low skilled	33%	38%	35%	36%	36%	43%	32%	49%	28%	28%	33%	39%
No union representation	60%	52%	56%	58%	58%	52%	67%	69%	54%	52%	52%	55%

Source: IPPR analysis of ISER (2022)

Table 2.1 shows the following.

- Overall, young people are the most exposed across all the risk factors: they are far more likely to be in lower-skilled work, not have union representation in the workplace and to experience low levels of autonomy in the workplace. This chimes with polling conducted by Prospect which found young people were at much greater risk of monitoring (Prospect 2021).
- Women are more likely to be in lower-skilled work and slightly more likely to report low autonomy, but have overall slightly higher rates of union representation, which is driven by a greater likelihood to be in the public sector. Among those in the private sector, women are at higher risk across all three measures.
- Overall Black workers have high rates of low autonomy and lower-skilled, but this is balanced somewhat by being more likely to benefit from union representation than other ethnic groups.

Interviewees highlighted that the rise of surveillance practices can fuel insecurity particularly for those in more precarious work, given they are less empowered to ‘argue back’ with technology and have lower barriers to dismissal by algorithm. Previous research has shown that such work is disproportionately taken up by minority ethnic workers (Living Wage Foundation 2022) and the young (Posch et al 2020).

FUNDAMENTAL RISKS TO HUMAN RIGHTS

Workers have a fundamental right to privacy in most cases as outlined in article 8 of the European Convention on Human Rights (EHRC 2021).

Article 8: Right to Privacy

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is easy to see how some forms of surveillance would not meet this standard – and any gains for employers, perceived or real, should not come at the expense of worker's fundamental rights. The key point of interpretation is the extent to which surveillance could be deemed 'necessary' given the provisos set out in the second clause which could create a legal grey area. The ICO notes that workers' expectations of privacy are likely to be greater at home than the workplace, and that the risks of capturing family and private life information are higher (ICO 2022).

SUMMARY

Surveillance when poorly implemented can have a negative impact on worker wellbeing – with the potential to cause higher worker turnover and counter-productive worker behaviour such as deliberate sabotage. It makes a difference for workers whether surveillance has a clear purpose, whether it is considered invasive and whether employers are transparent, with some positive use cases for example in training and safety. Our preliminary analysis suggest that young and black workers may be particularly exposed, but more data collection is needed.

Surveillance can lead to an imbalance in power between employers and employees, as employers hold more information on their employees which can be used against them. It can also undermine worker unionisation efforts and be used as a threat to exert control.

Increased data collection through monitoring gives rise to greater use of automated decision-making, which could lead to more widespread 'algorithmic bias'. Well-designed algorithms could reduce the bias inherent in human decision-making, whilst poorly designed ones can exacerbate existing societal prejudice.

Unchecked, worker surveillance practices could violate our fundamental right to privacy, particularly given the shift to home working, and this must be balanced against any benefits. The table below summarises the key pros and cons.

TABLE 2.2: POTENTIAL COSTS AND BENEFITS OF WORKER MONITORING

Potential benefits	Potential costs
• Can lead to improved health and safety outcomes • Can be used to identify training needs and support training • Can boost efficiency through greater automated decision-making • Can empower workers with data on their performance and time use, when shared and employees can interpret the data	• Can have negative effects on worker wellbeing, trust and turnover • Can lead to "counter-productive work behaviours" • Can be used to undermine unionisation efforts • Can be used as threat for management to exert control • Can lead to unequal access to data on workers, when not shared • Can violate fundamental right to privacy • Can fuel 'algorithmic bias' • Can lead to over-emphasis on 'being seen to work' rather than quality of work

Source: Author's analysis

3.
WHAT SHOULD WE DO ABOUT IT?

ADDRESSING WORKER POWER

Considering the potential effects of surveillance outlined in the previous chapters, there is a real risk of a shift in power away from workers facilitated by the ever-increasing adoption of these new technologies. We need a set of proposals aimed at shifting this power imbalance arising from the rise of worker surveillance.

Employers must be more transparent in their monitoring decisions and employees empowered to challenge where appropriate

Protection of workers' rights is largely covered by data protection regulations so strengthening this and ensuring that the current law is enforced is critical for protecting workers from unnecessary or otherwise intrusive surveillance. Much of the law around monitoring and GDPR relies on employer compliance, placing very little obligation on employers to 'show their working' when making decisions around whether monitoring employers has a legal basis (as outlined in chapter 2). In effect, it is difficult from the outside or for workers (or their representatives) to understand the basis on which decisions have been made, and if they have been well thought through. Although the ICO encourages the publication of data privacy impact assessments, there is no requirement for this, with the exception of public bodies for which they can be requested under the Freedom of Information Act.

We recommend that employers should demonstrate their compliance with GDPR through a publicly available 'worker monitoring statement' which should outline in plain English:

1. the nature of any monitoring in the organisation
2. the 'legal basis' on which the data is collected, processed and disseminated, including any justification that the balancing test applies
3. an explanation of how data collected is minimised only to the purposes set out
4. if and how automated-decision-making or profiling are used.

This should not place an additional burden on businesses because they are obliged by law to make these considerations anyway, however there would be a number of benefits.

1. It would incentivise businesses to seriously grapple with the relevant GDPR questions for monitoring, given the potential for public scrutiny, and compelling them to ensure they have followed the appropriate steps including workplace consultation.
2. It allows prospective workers to understand the monitoring they will be subject to should they take employment, and empower current workers to understand and potentially challenge practices.
3. It would provide assurance to the ICO, who should do 'spot checks' to ensure compliance.

If firms do not carry out monitoring, they should also set this out, providing much needed clarity in situations where monitoring policies may be ambiguous.

Employees' induction processes should address the monitoring policy document and where it can be accessed, give the employer opportunity to ask questions, and outline the complaints process including routes to escalation within the organisation.

Although the Information Commissioner's Office may investigate large-scale employer breaches and can fine employers for breach of the law as well as an issue advice, it is *not* an ombudsman and they are clear that their role is not 'to investigate or adjudicate on every complaint' (ICO 2022). But there is a role for an organisation to do so, providing workers have already tried to escalate internally, and this need will likely grow as these practices become more common and if transparency is increased.

As such, we recommend the UK government should press ahead with establishing a single enforcement body for employment rights as outlined in the Conservative Party manifesto (Conservative Party 2019). This body must enable routes to redress against unlawful surveillance practices in line with GDPR.

Employers should give workers access to the data which is collected on their work activities

As outlined in chapter 2, worker surveillance gives rise to 'datafication' which becomes an issue if only one side, the employer, has access to the data collected, which can be used against the employee.

This has given rise to demands for 'data reciprocity', that is a legal right for workers to have access to the exact same data as their employers, offered by default. Such data could be analysed by workers and their representatives such as trade unions to support campaigning for better terms and conditions at work (TUC 2021). This right could also assist workers in exposing discriminatory, unethical or inaccurate AI or automated decision making (ibid), and serve as a mechanism to keep employers in check.

Government should consider whether certain surveillance practices should be outlawed

There are certain monitoring practices which are very unlikely to be compatible with the fundamental principal in GDPR that only essential data should be collected. Keystroke monitoring and screenshot capture may be difficult to justify, or the need for always-on webcams, particularly in a working-from-home context where expectations of privacy are likely to be greater (ICO 2022).

The government should consider outlawing digital monitoring techniques and software where legitimate use cases are likely to be limited, or actively regulate their use - for instance through licensing requirements for the small number of cases where there could be legitimate uses.

Workers should have the 'right to disconnect'

To counter the blurring boundaries between work and home life, and in line with other European countries (WEF 2023), the UK should introduce a statutory 'right to disconnect' for workers. This right would mean that every employee has the right to 'switch off' from work contact outside of contracted working hours and enjoy their free time away from work without being disturbed, unless there is an emergency or prior agreement to do so, for example while being 'on call' (CIPD 2021).

Give unions access to workplaces to ensure fair monitoring practices

As outlined above, we know that the presence of a union increases the likelihood of workplace consultation in the introduction of surveillance, and policies geared at increasing union membership would strengthen the hands of workers against excessive surveillance. In the short-term however we need policies which can enable existing unionised workplaces to understand what is happening on the ground and challenge unlawful practices. As such, we recommend a statutory right for unions to access the workplace which could be used to examine monitoring practices, and to speak to the organisational data protection leads. Unions would need to give sufficient notice and there should be limitations on how often they could visit to ensure this would be manageable for employers.

Taken together these policy changes would address issues of worker power in the context of rising surveillance.

RESPONDING TO THE RISE OF ALGORITHMIC CONTROL

We also need policies in response to the growing use of algorithmic decision-making arising from an expansion of worker monitoring.

UK government should champion algorithmic accreditation

We know that wider use of algorithms by businesses creates more opportunities for algorithmic bias. Currently, there is no way for employers to distinguish between those algorithms which have been thoroughly examined in line with best practice, and those where a more relaxed approach has been taken – and it would be difficult if not impossible for businesses to determine this independently.

As such, algorithm accreditation could be a useful mechanism, both to help employers make better choices and to drive up standards amongst industry. To achieve accreditation, businesses developing such software would need to demonstrate at each stage in the development chain that the data inputs and underlying code made by their products do not lead to biased outcomes on the basis of protected characteristics.

This accreditation could be coordinated by UK government but led by industry experts with the British Standards Institute, with the suitable tests devised by the Centre for Data Ethics and Innovation. Financial support should be available for small and medium businesses to jump over the necessary hurdles and to ensure a level playing field with larger companies in achieving accreditation.

Enhancing protections against algorithmic control

As outlined in chapter 1, GDPR offers specific protection when automated decision making technology has a 'legal or similarly significant' impact. This requires employers to give workers information about the processing and introduce simple ways to request human intervention, as well as carry out regular checks to make sure the systems are working as intended.

However, we recommend this is taken further by doing the following.

- Lowering the threshold of protections to *all* automated decision making which meaningfully affect the worker, as opposed to relying on subjective judgements of impact. This would broaden the instances where further information is provided, alongside a much broader obligation to provide simple ways to request human intervention when automated decision making is applied.
- In higher-risk applications, introducing a right for a personalised explanation for how any decisions were reached using automated decision making, setting out the logic in an understandable way. GDPR currently only requires a 'generic' explanation to be provided, such as which data sources are fed into the algorithms.

Finally, we need to increase our understanding of what surveillance is happening and for whom to inform future policymaking.

Collecting better data

From sporadic surveys and analysis of web search data we know that worker monitoring and digital surveillance are a growing phenomenon, but by how much and for whom is much less clear. Given this is issue likely to remain important, it is essential that the ONS begin to collect relevant data through nationally representative surveys – a prime candidate being the Labour Force Survey (LFS). The LFS already collects detailed information around other aspects of worker conditions such as flexible working practices, overtime and job satisfaction (ONS 2022) – and monitoring practices are a natural extension to this data collection.

In doing this, we can begin to understand more concretely the scale of the problem, and who is most affected – identifying demographic and industry trends. The survey would need to enable participants to identify the nature of any such surveillance, giving clear examples of what is meant and allowing them to select particular options. In addition, workers should be able to identify how far the worker feels the monitoring is invasive. Closing this evidence gap will be crucial to developing future policy in this area and understanding the equality implications of any developments.

CONCLUSION

Taken together these policy recommendations would help redress the balance of power between workers and employers, and ensure that when monitoring is happening it is fair and proportionate, as the law intends. We should champion the use of algorithms which can reduce bias and boost productivity through accreditation, and we should close prominent data gaps to inform future policymaking.

REFERENCES

Ball K (2021) *Electronic Monitoring and Surveillance in the workplace*, Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC125716

Blum S (2022) *Employee surveillance is exploding with remote work – and could be the new norm*, HR Brew, news article. https://www.hr-brew.com/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm

Centre for Data Ethics and Innovation [CDEI] (2020) *Review into bias in algorithmic decision-making*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

Chartered Institute of Personnel Development [CIPD] (2020) *Workplace technology: The employee experience*. https://www.cipd.co.uk/Images/workplace-technology-2_tcm18-80853.pdf

Chartered Institute of Personnel Development [CIPD] (2021) 'What is the right to disconnect?', news article. https://www.hr-inform.co.uk/news-article/what-is-the-right-to-disconnect

Conservative Party (2019) *The Conservative and Unionist Party Manifesto 2019.* https://www.conservatives.com/our-plan/conservative-party-manifesto-2019

Equality and Human Rights Commission [EHRC] (2022) *Article 8: Respect for your private and family life*. https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

Gaudio G (2021) 'Algorithmic bosses can't lie! How to foster transparency and limit abuses of the new algorithmic managers', *Comparative Labor Law and Policy Journal*. https://ssrn.com/abstract=3927954

Greene J (2020) 'Amazon's employee surveillance fuels unionization effort: 'It's not prison it's work'', *Washington Post*, news article. https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions/

Gurley L (2022) Internal documents show Amazon's dystopian system for tracking workers every minute of their shifts', *Vice*, news article. https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts

Holmes A (2020) 'Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working — and the service is seeing a rapid expansion since the Coronavirus outbreak', *Insider*, article. https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3?r=US&IR=T

Information Commissioner's Office [ICO] (2022a) *Employment practices: monitoring at work draft guidance*. https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf

Information Commissioner's Office [ICO] (no date) 'Data protection impact assessments, guidance', webpage. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Information Commissioner's Office [ICO] (2022b) 'Our service standards, guidance', webpage. https://ico.org.uk/about-the-ico/our-information/our-service-standards/

Institute for Social and Economic Research, University of Essex [ISER] (2022) 'Understanding Society Wave 12', dataset, accessible via UK Data Service

Kolkman D (2020) '"F**k the algorithm?" What the world can learn from the UK's A-level grading fiasco?', London School of Economics, blog. https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/

Living Wage Foundation (2022) 'Minority ethnic workers disproportionately employed in UK's most precarious jobs', press release. https://www.livingwage.org.uk/news/minority-ethnic-workers-disproportionately-employed-uks-most-precarious-jobs

Lyon D (2001) *The Surveilanec Society: Monitoring Everyday Life*, Simon and Schuster

Migliano S (2022) 'Employee surveillance software demand up 58% since pandemic started', blog. https://www.top10vpn.com/research/covid-employee-surveillance/

Nahrgang J, Morgeson F and Hofmann (2011) 'Safety at work: A meta-analytic investigation of the link between job demands, job resources, burnout, engagement, and safety outcomes', *Journal of Applied Psychology*. https://pubmed.ncbi.nlm.nih.gov/21171732/

Office for National Statistics [ONS] (2022) Labour Force Survey User Guide: Volume 2 - LFS Questionnaire 2022. https://www.ons.gov.uk/file?uri=/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/methodologies/labourforcesurveyuserguidance/volume2combined.pdf

Palmer A (2021) 'How Amazon keeps a close eye on employee activism to head off unions', CNBC, article. https://www.cnbc.com/2020/10/24/how-amazon-prevents-unions-by-surveilling-employee-activism.html

Prospect (2021) 'New protections needed to stop employee surveillance of remote workers', press release. https://prospect.org.uk/news/new-protections-needed-to-stop-employer-surveillance-of-remote-workers

Reukauf J A (2018) 'The correlation between job satisfaction and turnover intentions in small business', Walden University. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=5425&context=dissertations&httpsredir=1&referer=

Roberts C, Parkes H, Statham R and Rankin L (2019) *The future is ours: Women, automation, and equality in the digital age*, IPPR. https://www.ippr.org/research/publications/women-automation-and-equality

Sanfillipo M (2023) 'What after hours emails really do to your employees', *Business News Weekly*. news article. https://www.businessnewsdaily.com/9241-check-email-after-work.html

Siegel R, König C and Lazar K (2022) 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counter-productive work behaviour: a meta-analysis', *Computers in Human Behaviour reports*. https://doi.org/10.1016/j.chbr.2022.100227

Simonite T (2018) 'This call may be monitored for tone and emotion', *Wired*, news article. https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/

Sprigg C, Stride C, Wall T, Holman D and Smith P (2007) 'Work characteristics, musculoskeletal disorders, and the mediating role of psychological strain: A study of call center employees', *Journal of Applied Psychology*. https://psycnet.apa.org/doiLanding?doi=10.1037%2F0021-9010.92.5.1456

Thiel C, Bonner J, Bush J, Welsh D and Garud N (2022) 'Monitoring employees makes them more likely to break rules', *Harvard Business Review*, news article. https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules

Thompson P, McDonald P and O'Connor P (2020) *Employee dissent on social media and organizational discipline*, *Human Relations,* 73(5) pp 631– 652

United Tech and Allied Workers [UTAW] (no date) 'What is employee surveillance?', webpage. https://utaw.tech/surveillance/what-is-employee-surveillance/

VMWare (2021) *The virtual floorplan: New rules for a new era of work*, report. https://www.vmware.com/content/dam/learn/en/amer/fy22/pdf/vmw-virtual-floorplan-exec-summary_r3v2-1162603.pdf

World Economic Forum [WEF] (2023) 'Right to disconnect: The countries passing laws to stop employees working out of hours', news article. https://www.weforum.org/agenda/2023/02/belgium-right-to-disconnect-from-work/

Trades Union Congress [TUC] (2021) *Dignity at work and the AI revolution: A manifesto*. https://www.tuc.org.uk/sites/default/files/2021-03/The_AI_Revolution_20121_Manifesto_AW.pdf

Trades Union Congress [TUC] (2022) 'Intrusive worker surveillance tech risks "spiralling out of control" without regulation, TUC warns', press release. https://www.tuc.org.uk/news/intrusive-worker-surveillance-tech-risks-spiralling-out-control-without-stronger-regulation

Woods A (2019) 'The GDPR implications of monitoring your workforce', *People Management*, news article. https://www.peoplemanagement.co.uk/article/1741588/gdpr-implications-monitoring-your-workforce

APPENDIX

ORGANISATIONS AND INDIVIDUALS INTERVIEWED OR ENGAGED FOR THE PROJECT

- Privacy International
- Tech UK
- Reid Blackman, Ethical AI consultant
- Communication & Workers Union
- Chartered Institute of Personnel and Development
- Trades Union Congress
- Kirstie Ball, professor of Management, University of St Andrews

The report does not represent the views of the interviewees or organisations identified.

DETAILS OF FOCUS GROUPS

IPPR ran two 90-minute online focus groups in week commencing 6 February 2023. Participants were recruited by DJS Research, with participants identified by whether they responded positively to the question: ‘Does your employer use technology in some way to closely track your movements or computer use when at work?’. Participants were drawn from across the UK and included a range of ages, ethnicities and industries.

Institute for Public Policy Research

GET IN TOUCH

For more information about the Institute for Public Policy Research, please go to www.ippr.org

You can also call us on +44 (0)20 7470 6100, e-mail info@ippr.org or tweet us @ippr

Institute for Public Policy Research
Registered Charity no. 800065 (England & Wales),
SC046557 (Scotland), Company no, 2292601 (England & Wales)

The progressive policy think tank