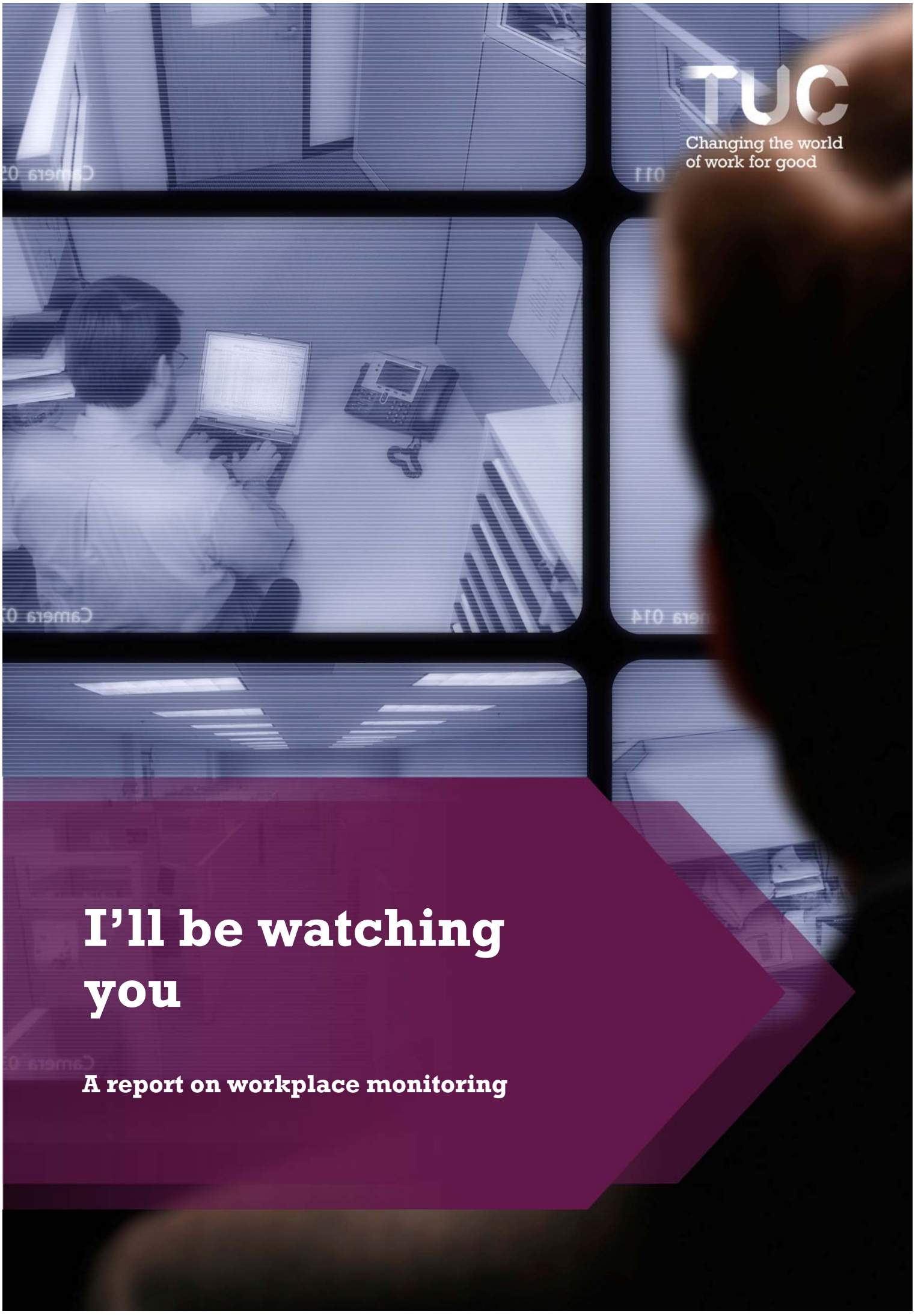


I'll be watching you

A report on workplace monitoring

Acknowledgements

Thanks to BritainThinks for conducting qualitative and quantitative research into workplace surveillance on our behalf.

Thanks also to all those who gave up their time to speak to us about their experiences, as well as the unions who provided advice and case studies.

Congress House, Great Russell Street, London WC1B 3LS
020 7636 4030 www.tuc.org.uk

For more copies call 020 7467 1294 or email publications@tuc.org.uk

Please ask if you need an accessible format.

Cover image by: J.R. Bale / Alamy Stock Photo

Contents

Key findings

- Over half of workers (56 per cent) think it's likely that they're being monitored at work.
- Workplace monitoring is more likely to be happening to younger workers and employees in large companies.
- Two-thirds of workers (66 per cent) are concerned that workplace surveillance could be used in a discriminatory way if left unregulated.
- 70 per cent think that surveillance is likely to become more common in the future.
- Trade unions should have a legal right to be consulted on and to agree in advance the use of electronic monitoring and surveillance at work.
- The government should ensure employers can only monitor their staff for legitimate reasons that protect the interests of workers.

Executive summary

Workplace monitoring is becoming increasingly prevalent.

We've recently heard about Amazon patenting wristbands to track warehouse workers, Uber keeping a bit-too-close of an eye on its drivers, and sci-fi sounding software that tracks the emotions and "intensity" of staff.

But these stories only offer a glimpse into the role of surveillance in the workplace. We wanted to know whether they were indicative of wider trends, or just extreme examples.

Our focus on surveillance at work also goes beyond recent news stories. In fact, the trade union movement has been fighting the changing face of workplace surveillance for years. To quote Michael Ford QC when he was writing about workplace monitoring twenty years ago:

> *Surveillance is almost as old as work itself, but new techniques represent a growing threat of a different kind of workers and unions.*[1]

When workplace monitoring is justified and used fairly, it can protect the health and safety of workers and improve business practices. When used badly or inappropriately, however, it becomes symptomatic of an employer's lack of trust in staff, which in turn demoralises workers and can make staff miserable.

We set out to establish the bigger picture so that we have the information needed to best tackle bad practice in workplace monitoring. To do this, we decided to look at:

- how widespread workplace surveillance is
- the impact of surveillance on working people
- how employees feel about being monitored.

We found that surveillance is happening now, and it's happening a lot. Working people also think it's likely to become more widespread in the future.

A majority of working people (56 per cent) think it's likely that they're already being monitored at work. Almost three-in-four (72 per cent) believe it's at least fairly likely that at least one form of workplace monitoring is happening in their workplace.

The most common forms of surveillance include:

- monitoring employees' work emails, files and browsing histories (49 per cent of people think it's fairly likely or very likely to be happening in their workplace)
- CCTV (45 per cent)

[1] Michael Ford (1998), Surveillance and Privacy at Work Institute of Employment Rights

- phone logs and calls, including the recording of calls (42 per cent).

However, even more advanced forms of surveillance (such as facial recognition and handheld/wearable location tracking devices) are more commonly used than might have been expected.

While workplace monitoring is already an issue for some workers, many people believe that it's going to become more widespread in the near future. While some people can see some benefits to this, there are clear concerns.

Working people are particularly worried about the impact of surveillance on relationships between workers and their employer, as well as the danger that an increase in unregulated surveillance could lead to a rise in discrimination.

Data protection law, recently strengthened by the General Data Protection Regulation (GDPR), places significant limits on when and how employers should use new technology to monitor their staff in and outside the workplace.

However, too few people know about these rights and how they might apply in their workplace. Many feel unable to challenge employers' use of surveillance.

Working people are clear about what they want to see happen next, which includes:

- a legal requirement for employers to consult with staff before introducing new forms of surveillance
- employers to fully justify the use of any new forms of workplace monitoring before they can be enforced
- a clear line between when surveillance is and isn't acceptable, with an understanding that it isn't acceptable outside working hours (including while on breaks)
- regulations to be put in place to stop monitoring being used in a discriminatory way.

In the report, we're going to go into more detail on the issues covered in this executive summary. There's four sections, covering:

- what workplace surveillance is
- where it's happening, how much it's happening and who's most affected by it
- how workers feel about surveillance
- what changes workers would like to see and what new policies are required to bring about that change.

Methodology

We commissioned BritainThinks to carry out qualitative and quantitative research into workplace surveillance.

The qualitative stage of research involved a range of focus groups and depth interviews held across four cities: London, Birmingham, Manchester and Bristol.

The results of these groups and interviews were used to create a quantitative survey. BritainThinks then carried out a nationally representative online survey between 18th and 21st May 2018 that received 2,100 responses from members of the UK public. The results were weighted to be representative of the adult UK population.

Questions relating to an individuals' specific workplace or current experiences of work were only asked to those currently in work (base size, 1,099, weighted to 1,210). The figures included in this report are based on the answers given by those in work.

What is workplace monitoring?

Workplace surveillance is any form of employee monitoring undertaken by an employer.

There's nothing new about workplace monitoring. It's been around for a long time, and it's something unions have worked on for just as long.

However, as technology has advanced, so have the ways employers can monitor their staff. While in the recent past employers relied on timesheets, bag checks, and keeping a close eye on their employees, they can now make use of a litany of new surveillance methods.

This means that workplace monitoring can now vary drastically, from fairly basic and rudimentary surveillance, to much more complex and technology-driven monitoring.

"I've taken jobs where we don't use a sign-in sheet. Instead, they take our fingerprint. It skips a process, but I feel like it's an invasion of privacy."

Barry, a construction worker

Here are some examples of common forms of monitoring, broken down into two groups:

Monitoring computer and phone use

- monitoring employee emails from their work account and browser history and/or files saved on work computers
- monitoring employee browser histories on personal devices that are on connected to the employer's Wi- Fi network
- monitoring employees using webcams on work computers
- using keystroke-logging software to monitors when and how much an employee is typing
- keeping records of employee telephone logs and calls, as well as recording their calls
- monitoring employee use of social media outside of working hours (such as monitoring the posts on an employee's personal Facebook or Twitter account).

Tracking the movement of employees

- CCTV
- tracking the location of company assets, e.g. location trackers on company vehicles, computers or phones
- using facial recognition software to monitor the expression and mood of staff while working

- security and bag checks when entering and leaving the workplace
- using access cards to monitor and record the location of employees in a building and how long they spend there
- using handheld or wearable devices to monitor and record the exact location and movements of employees within the workplace.

Union case study: the changing nature of surveillance in the energy sector

Unite the Union have noticed an increasing trend towards excessive surveillance in the energy sector. This includes the use of vehicle monitoring technology and dash cameras at a number of companies, and even real-time streaming video surveillance in some vehicles. Companies are now also pushing for body cameras to be worn. So far, however, unions have been able to successfully resist this.

Unite say that surveillance has caused widespread condemnation from members, especially as management have attempted to utilise the information obtained around less-than-perfect driving in disciplinary hearings. Unite has resisted this and managed to negotiate a situation where only a key manager has the right to view footage but only after they have consulted the lead union representative. The footage is now inadmissible in disciplinary hearings.

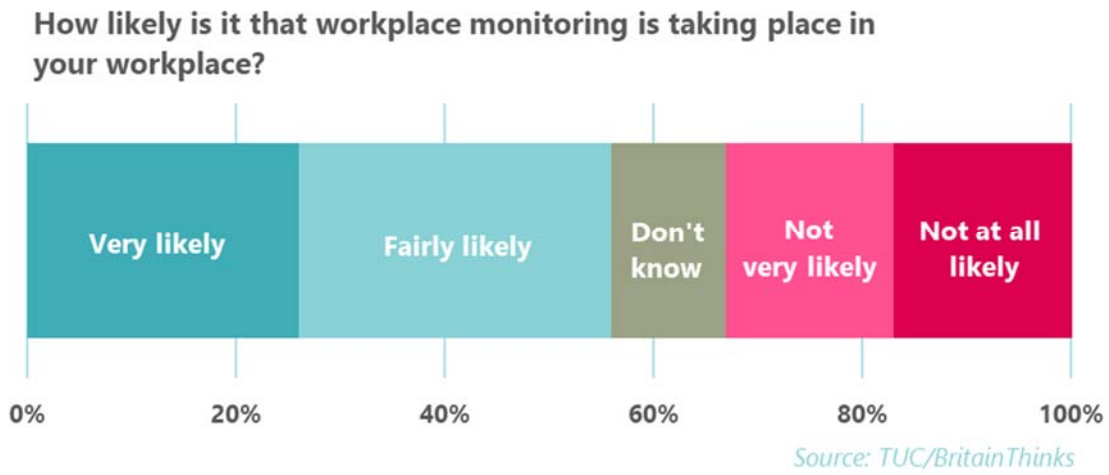
In other companies, especially those fitting smart meters, engineers have to use a web-based app to control their call outs and daily work programme. Employers have attempted to set a minimum number of jobs per individual per day but workers have reported that in many cases it is not possible to install this number in the normal working day, and mistakes are being made due to engineers rushing jobs.

Again, the union has intervened and agreed that no disciplinary can be based on the number of jobs completed in a day, provided that a report was submitted on the issues encountered by the worker.

Where it's happening and who's affected

How widespread is workplace surveillance?

It's clear that workplace surveillance isn't confined to a few big companies. Over half of workers (56 per cent) think it's likely to be taking place where they work.



When provided with a list of types of surveillance, over two-thirds thought it was likely that at least one of these was used in their workplace. 41 per cent considered it very likely that at least one type was happening where they work. 72 per cent felt that it was at least fairly likely that one form of monitoring was taking place at work.

Which groups are particularly affected?

Workplace surveillance is more common among:

- younger workers
- employees in large companies
- certain regions.

We were also interested to see if there are any differences in the perceived prevalence of surveillance among men and women and people of different ethnicities. However, we found that there's:

"Obviously they monitor you, everywhere does, doesn't it?"

Office-based worker, Manchester

- only a slight difference between the percentage of men and women who think monitoring is likely to be happening in their workplace (57 per cent and 55 per cent respectively)

- a similarly slight difference between the percentage of white workers and Black, Asian and minority ethnic (BAME) workers who think that monitoring is likely to be happening in their workplace (56 per cent and 57 per cent respectively).

Young workers

While 56 per cent of working people think that workplace monitoring is likely to be taking place where they work, this rises to 60 per cent among 25-to-34-year olds. It's even more common among 18- to 24-year-olds. Over two-thirds (68 per cent) think it's likely to be happening in their workplace.

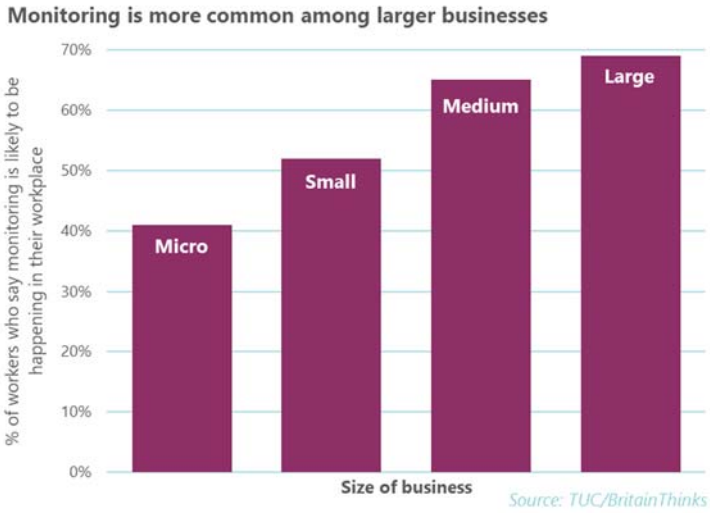
Large companies

People working for big companies are also more likely to think that their employer is keeping an eye on them. 69 per cent of those working for a large employer (250+ employees) consider it likely that their employer uses workplace monitoring.

The figure remains high among those working for medium employers (51-250 employees), with 65 per cent saying it's likely their employer uses workplace monitoring.

This drops to:

- 52 per cent among small employers (11-50 employees)

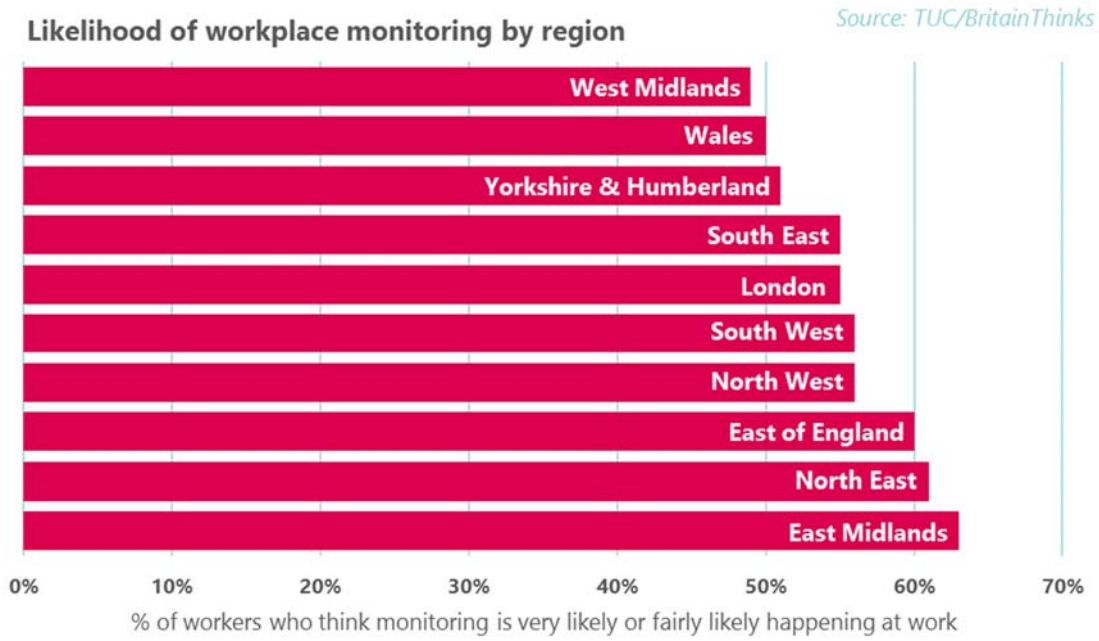


- 41 per cent among "micro" employers (1-10 employees)

Regional disparities

There are also clear regional differences when it comes to how common workplace monitoring is.

In the West Midlands, less than half (48 per cent) of workers think that monitoring is likely to be happening in their workplace. This rises to over 60 per cent of working people in the North East and the East Midlands.

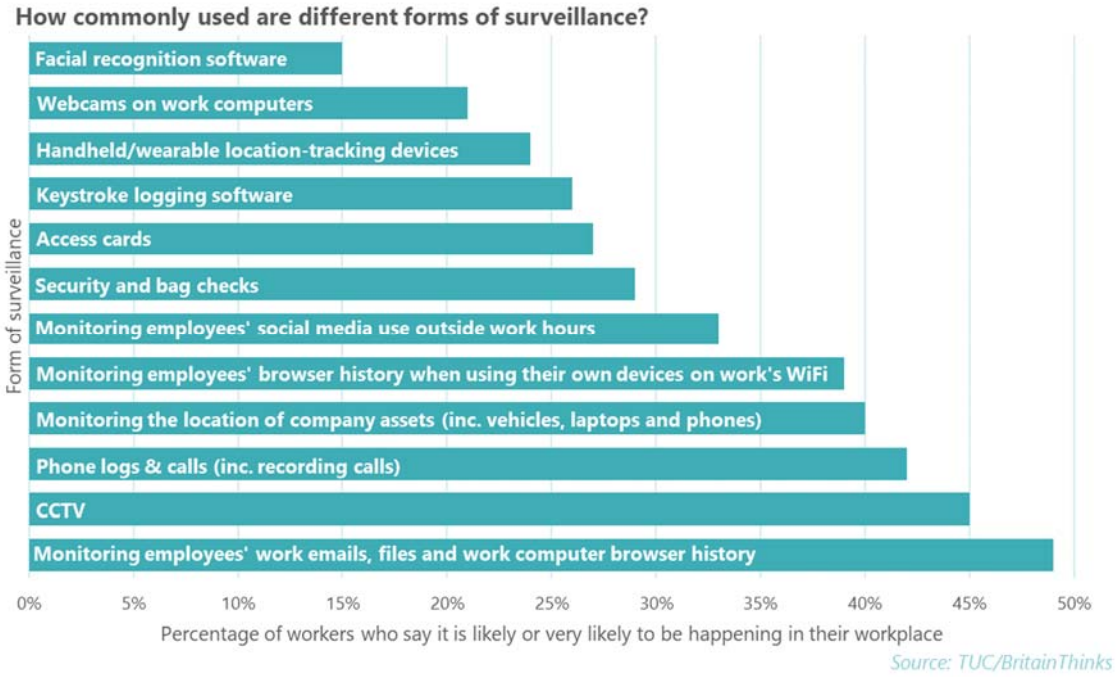


What are the most common types of surveillance?

The forms of surveillance that working people think are most likely to be happening in their workplace include:

- monitoring work emails, files and work computer browsing history (49 per cent of people think it's fairly likely or very likely to be happening in their workplace)
- CCTV (45 per cent)
- phone log and calls, including the recording of calls (42 per cent).

While not as widely used as other forms of surveillance, some more advanced forms of surveillance are more commonly used than some might expect. 23 per cent of workers think that handheld or wearable location-tracking devices are very or fairly likely to be being used in their workplace, while 15 per cent find it fairly likely or very likely that their employers are using facial recognition software.

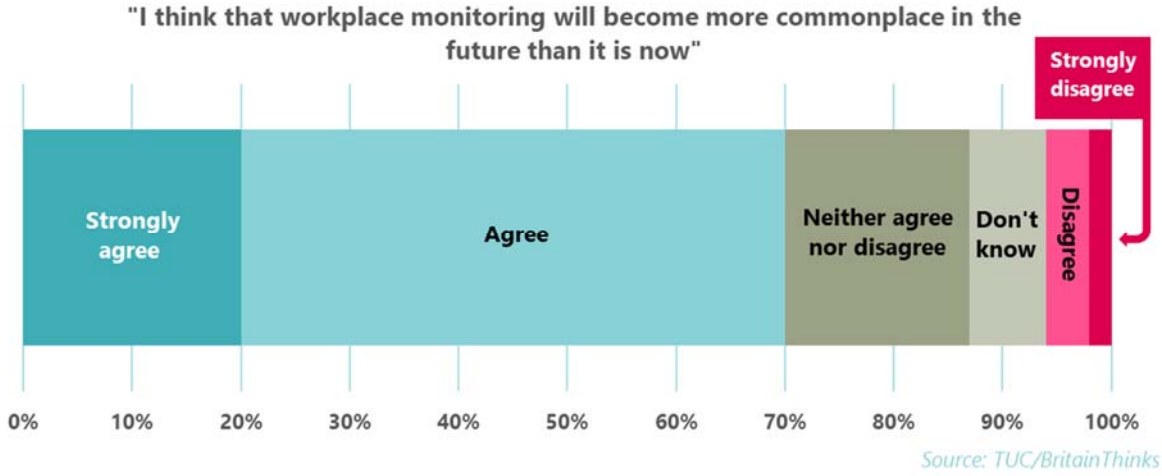


The types of surveillance that workers have experienced varies based on whether the person works in an office or a non-office job. Those in office jobs, for example, are more likely to have their emails checked, while those in non-office jobs are more likely to have worked for employers who track the location of company assets.

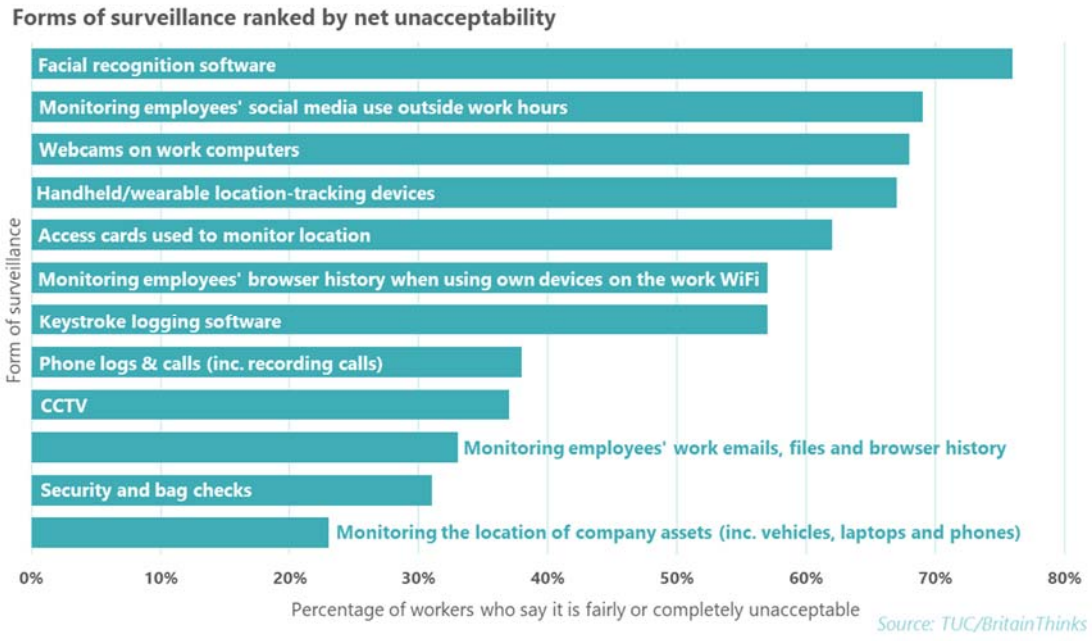
Workers' attitudes to surveillance

Workers expect surveillance to become more widespread

The majority of workers believe that surveillance is already likely to be taking place in their workplace. 70 per cent think surveillance will become more widespread in future, while only 6 per cent thought that it'll become less common.



Which types of surveillance are considered most unacceptable?



It's clear that some forms of workplace monitoring are considered even more unacceptable than others.

Monitoring company assets, for example, is thought of as unacceptable by less than a quarter of working people. In contrast, around three-quarters (76 per cent) believe that facial recognition software and the monitoring of employee's social media use outside of work hours is unacceptable.

Employees want justifications for monitoring

In our qualitative research, we found a clear dividing line for some workers is whether the monitoring is arbitrary or justified. Many people struggle to see the justification for facial recognition software or the monitoring of personal Facebook posts. By contrast, bag checks or monitoring calls and emails made sense to some.

Invasive or individualised monitoring

Anything that feels too invasive or overly-focused on one individual also tends to be widely seen as unacceptable. Those we spoke to wanted monitoring to be applied universally and not just against specific employees. It's considered unfair if some employees are monitored, but others aren't. For example, Bill, an engineer in the energy sector, told us how junior employees were unfairly monitored much more heavily than senior staff.

"I had a job where I had to handle lots of money and obviously they had bag searches then. I'd be annoyed if they introduced it where I work now though, there's no reason."

Donald, a call centre worker

There's also a clear dislike of any form of surveillance that films specific individuals. This was backed up in our quantitative findings. Around two-thirds of working people thought that the use of webcams on individual work computers was unacceptable, while only around a third thought the same of CCTV. Both involve filming employees, but the latter involves filming everyone from a distance rather than the expressions on an individual's face.

Monitoring toilet use

Another particularly invasive form of surveillance considered a step-too-far by many of the people we spoke to in focus groups was monitoring or limiting the amount of time staff could spend going to the toilet. Although not covered in the quantitative polling, it repeatedly came up in qualitative discussions.

"They try and make me monitor how long people go toilet for. I just hate that. It's not your business why someone is in there."

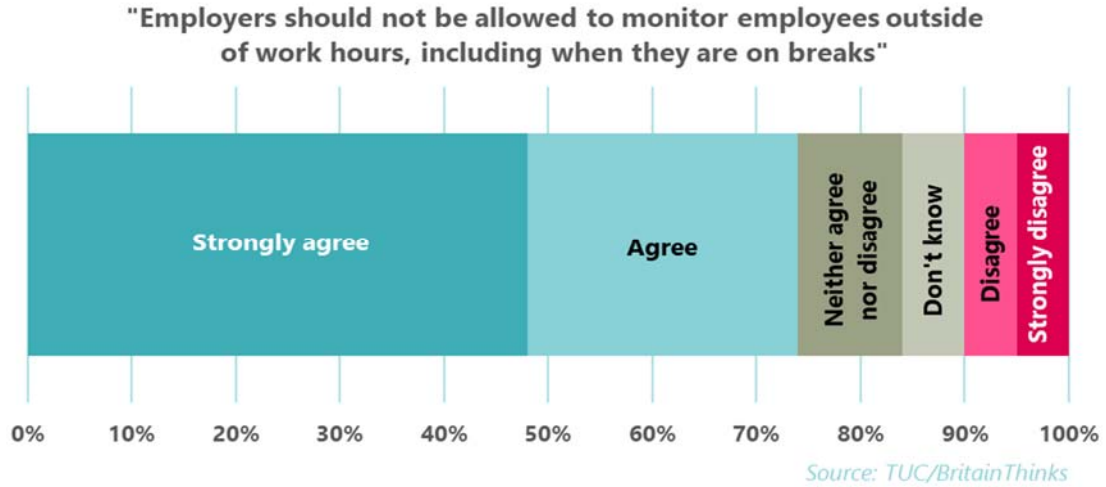
Angela, a team leader in a call centre

A team leader in a call centre told us that her manager would ask her to keep an eye on how long people were spending on the toilet. While she was happy to monitor staff in other ways, this felt over-the-top and unfair. A call centre worker who had experienced this type of monitoring told us how his boss would watch everything staff were doing, "you couldn't even go to the toilet without them wanting to know".

Monitoring or limiting toilet use is not only unpleasant for workers, it can also lead to issues around equality. There have been cases in Europe, for example, of female members of staff being made to wear certain items of clothing to make it clear when they're menstruating so that they are allowed more frequent trips to the toilet[2] [3].

Outside of work hours is off-bounds

Surveillance outside of working hours also crosses a line for many. There's strong support among workers for employers to be barred from monitoring staff at these times, including while on breaks.



74 per cent of working people think that employers should not be allowed to monitor staff outside of working hours, with only 10 per cent thinking they should be allowed.

When we spoke to workers about this, they strongly believed that what people did outside of work was off-bounds as long as they were doing their jobs while in work and unless it somehow impacted upon their ability to do the job.

---

[2] https://www.theguardian.com/world/2008/mar/27/germany.supermarkets

[3] https://ic.steadyhealth.com/red-bracelet-for-menstruating-employees

Social media

Checking a staff member's social media is widely unpopular. 69 per cent of working people think it's unacceptable to monitor an employee's use of social media outside of working hours.

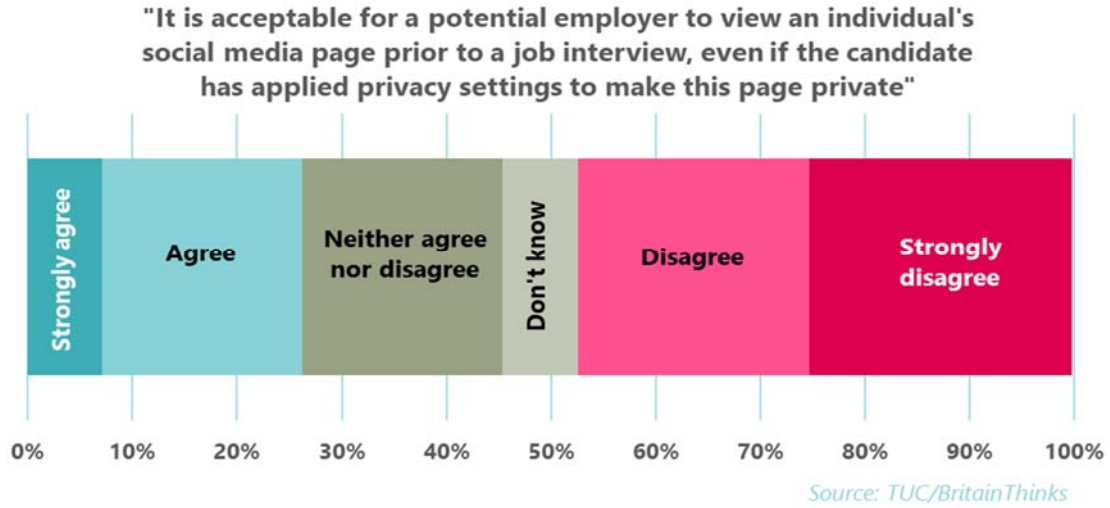
"People judge you, don't they? If you went to Magaluf 4 years ago, they might think you're not the right fit for this organisation."

Noel, an office-based worker

Social media offers a glimpse into a worker's life outside work. The risk for many people is that an employer might make sweeping judgements based on this glimpse. Being tagged in some Facebook photos from a night out years ago, or having a drinks-heavy Instagram, might be frowned upon by a snooping line manager who then unfairly carries these judgements into the workplace.

But it's not just judgements about a staff member's social life. Workers could express political views or opinions about their workplace on social media that lead them to being dismissed or victimised by their employer. This puts union members who want to take part in social media campaigns in a tough and risky position.

It's bad enough when your current boss has a look at your social media. But, employers might be doing this during the recruitment phase, and decide not to hire a candidate based on what they find. Just under half of working people (47 per cent) don't feel it's acceptable for an employer to even look at a candidate's social media presence before a job interview.

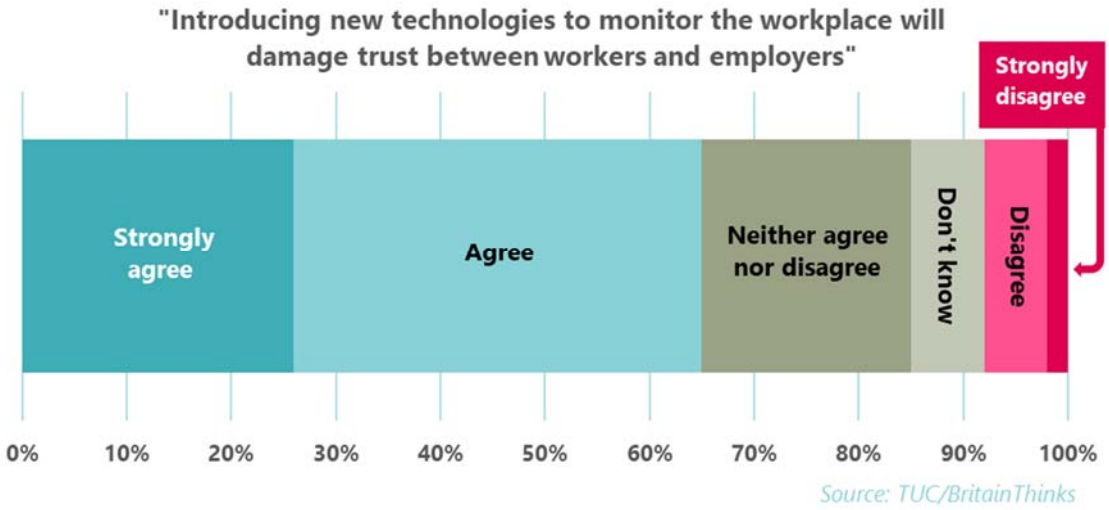


Trust

Surveillance can be a symptom of a bad relationship between an employer and employee. People should be trusted to do their job, and they should be judged by their output rather

than their input. We like to feel trusted by those they're working for, but surveillance implies the exact opposite. As a result, monitoring employees too closely can harm the relationship between them and their employer.

A strong majority of workers (65 per cent) believe that the introduction of a new type of surveillance would have a damaging impact on their relationship with their employer.



Trust works both ways. It's not just that workers worry about whether their employer trusts them, they're also worried about what an employer is going to do with the monitoring data being collected.

"Say if I don't like the look of you, say I don't like your glasses, can I just go trawling through until I find something?"

Call centre worker, Manchester

One of the risks when surveillance data is collected is that employers can build up a bank of data so they can sack someone that they take a disliking to.

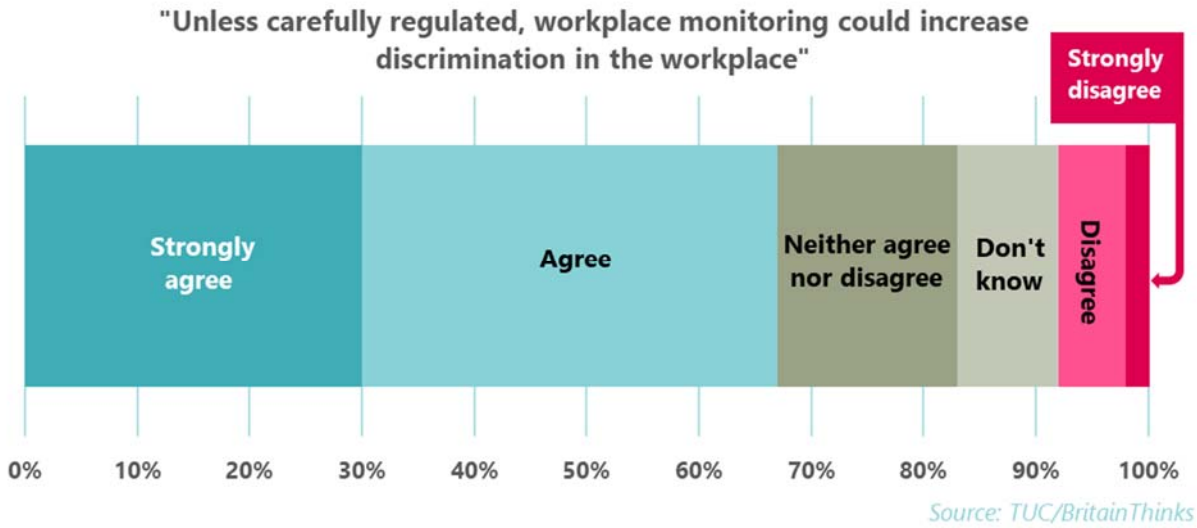
This is something we heard about during our qualitative research, with one worker telling us that a previous employer would "manage people out" of the company using surveillance. "They definitely used it to get rid of people," he said. "They could listen back through all your recordings to find the one mistake you made if they wanted."

Managing people out using surveillance isn't always an intentional act. Workplace monitoring can often be a blunt tool for measuring performance that leads to workers being penalised unfairly. For example, Simon, a gas technician for a large energy, told us that his performance is monitored by tracking how long he spends on each job. This isn't an accurate way of measuring performance and it doesn't take into account the realities of his job. He explained:

> *I get 18 minutes to fit a length of pipe. If I go over, the system tells my boss, who then asks why I'm taking too long. But sometimes, you have to move a sofa or lift a carpet to get to the pipe. There's no room for error.*

Another big concern is that "micro-management" via monitoring could lead to a rise in discrimination in the workplace. If an employer can use data to get rid of a staff member they dislike, it's not hard to imagine how this could be used in a discriminatory way.

Two-thirds of workers (66 per cent) think that unless workplace monitoring is carefully regulated, it could increase discrimination. Only a very small minority disagreed with this.



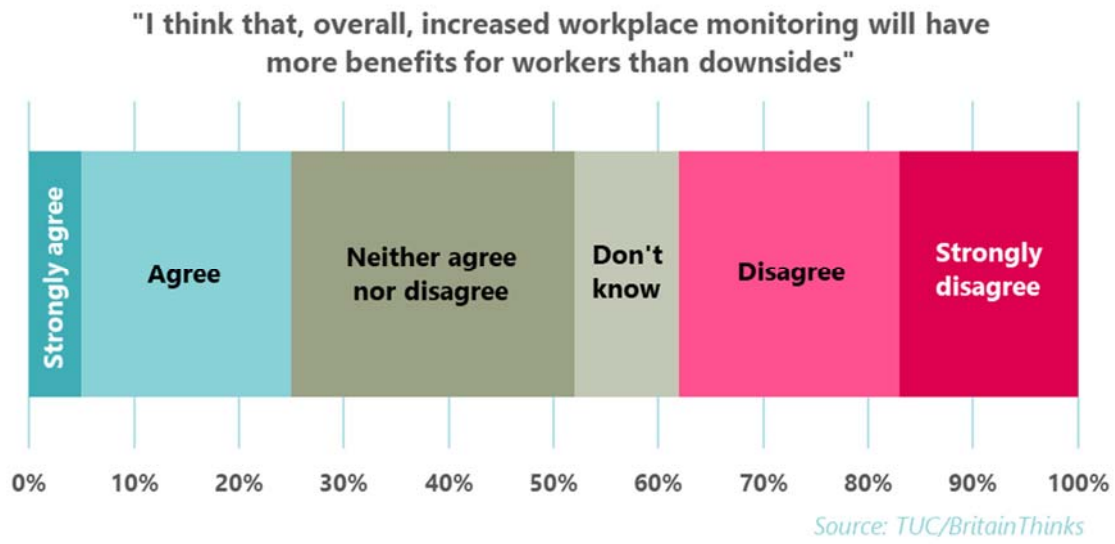
Mixed views on the benefits of surveillance

Workplace monitoring can have some benefits for workers. The most obvious are health and safety related. Wearable cameras, for example, can provide extra protection for security staff and parking attendants who face potential violence in their jobs. Tracking the location of staff within the building via access cards allows an employer to know where they are in case of a fire. Similarly, tracking the location of workers who travel or work alone as part of their job can give them much greater security.

There's also benefits unrelated to health and safety. Some workers in call centres, for example, thought an upside of calls being recorded is that the recordings could prove them right if a customer claimed that they had said something on the phone which they hadn't.

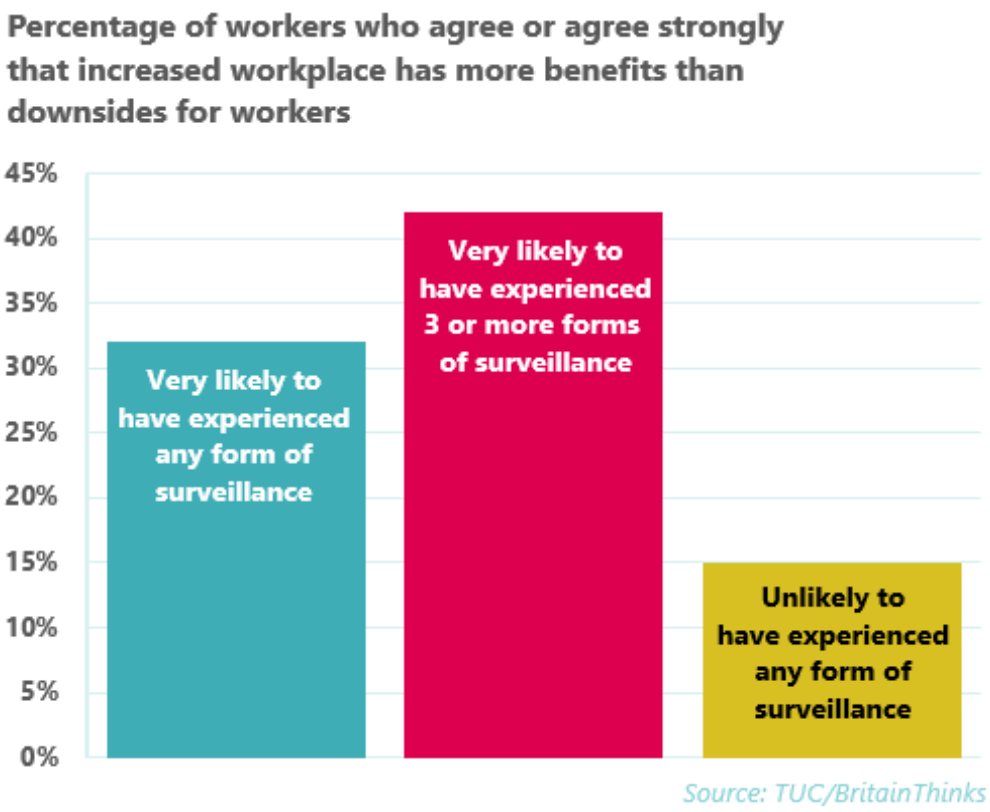
However, working people are sceptical about the potential benefits of workplace monitoring. For each of these positives, there's plenty of negatives, many of which have been set out above. Even in terms of health and safety, monitoring can provide extra security, but it can also cause added stress.

Only a quarter (25 per cent) feel that surveillance will have more benefits for workers than downsides, while 38 per cent disagree that surveillance has more positives than downsides. A sizeable proportion are uncertain or don't know.

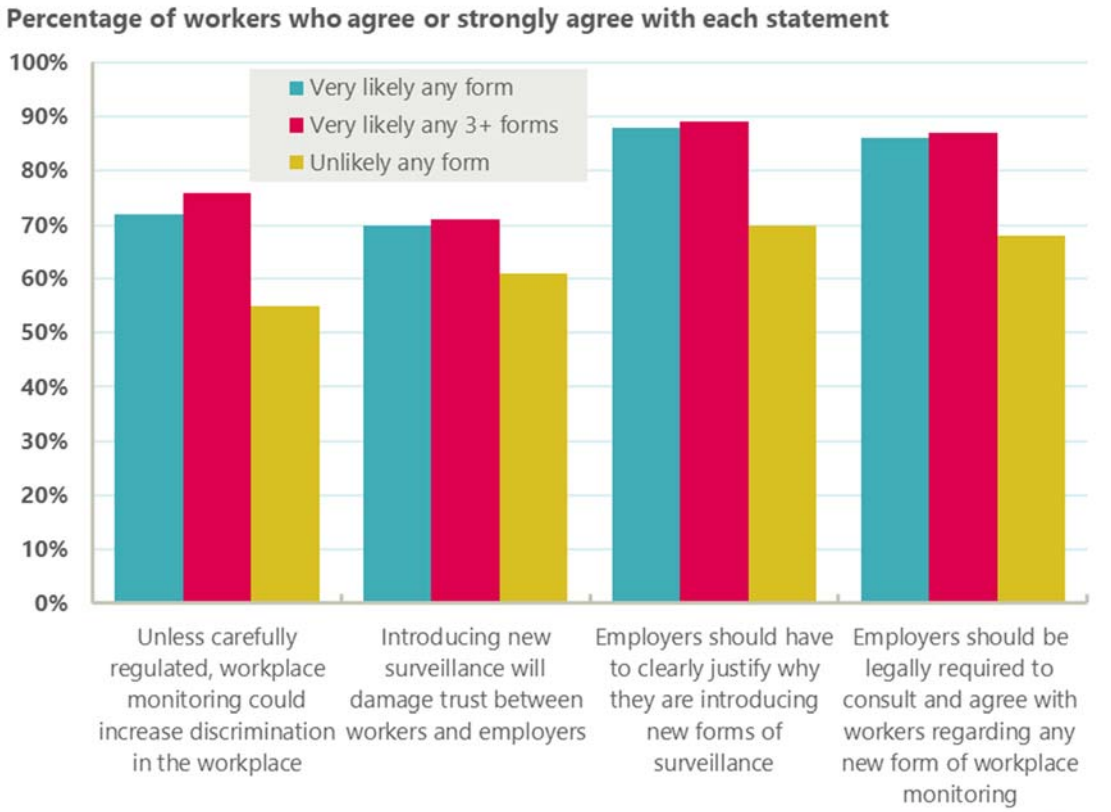


Those who have more experience of workplace monitoring are more likely to be aware of both the benefits and negatives of surveillance. Around a third (32 per cent) of people who told us that at least one type of surveillance was very likely to be happening in their workplace agreed or strongly agreed that surveillance had more benefits for workers than negatives.

This rose to 42 per cent among people who thought it very likely that three or more forms were very likely to be happening at their workplace, and dropped to just 15 per cent among those who felt it was unlikely any surveillance was being used by their employer.



Despite being more positive about the potential benefits of increased surveillance, those with experience of workplace monitoring were far more likely to think that it could damage trust or lead to discrimination if left unregulated. They're also more likely to support bringing in a legal requirement for employers to consult staff before introducing surveillance.



Source: TUC/BritainThinks

Fear of the future

Familiarity with a type of surveillance tends to be linked to how acceptable workers find it. In other words, workers are more likely to think that forms of workplace surveillance that are common are more acceptable.

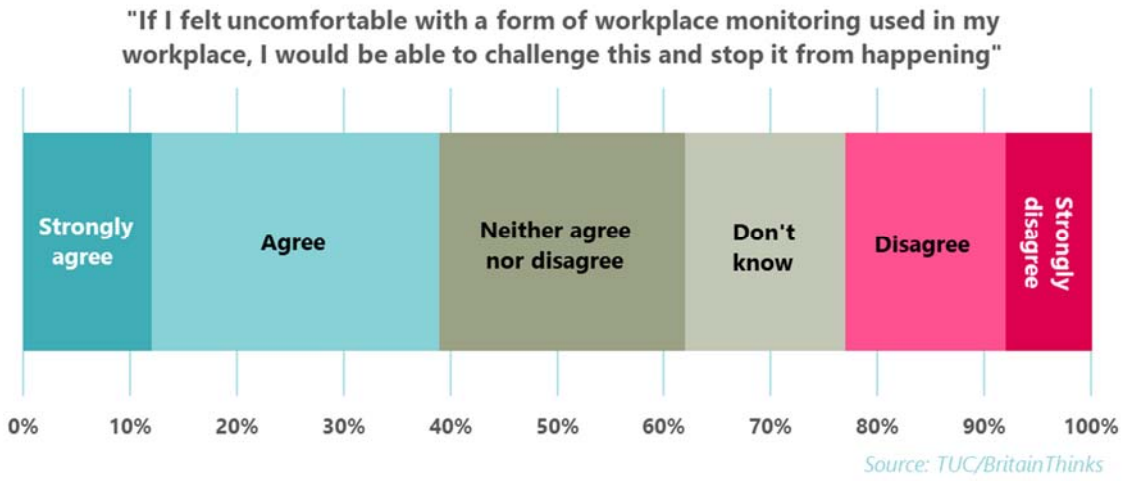
An exception to this trend is the monitoring of social media use outside work hours. It's one of the more common forms of surveillance, with around a third of working people (33 per cent) saying it's fairly or very likely to be happening in their workplace. However, only around one-in-five people consider it acceptable (22 per cent).

Source: TUC/BritainThinks. Labels for each specific form of surveillance have been removed to make the chart easier to read.

This link between how common a form of surveillance is and how widely accepted it is could mean one of two things. Either:

- workers have grown used to the surveillance they've experienced and have a sense of futility about changing it; or
- employers have introduced acceptable surveillance methods and avoided those that are unacceptable

We suspect that it might be the former due to the high number of workers who feel they would be unable to challenge workplace monitoring if they felt uncomfortable with it. According to our research, only 38 per cent of workers would feel able to do this.

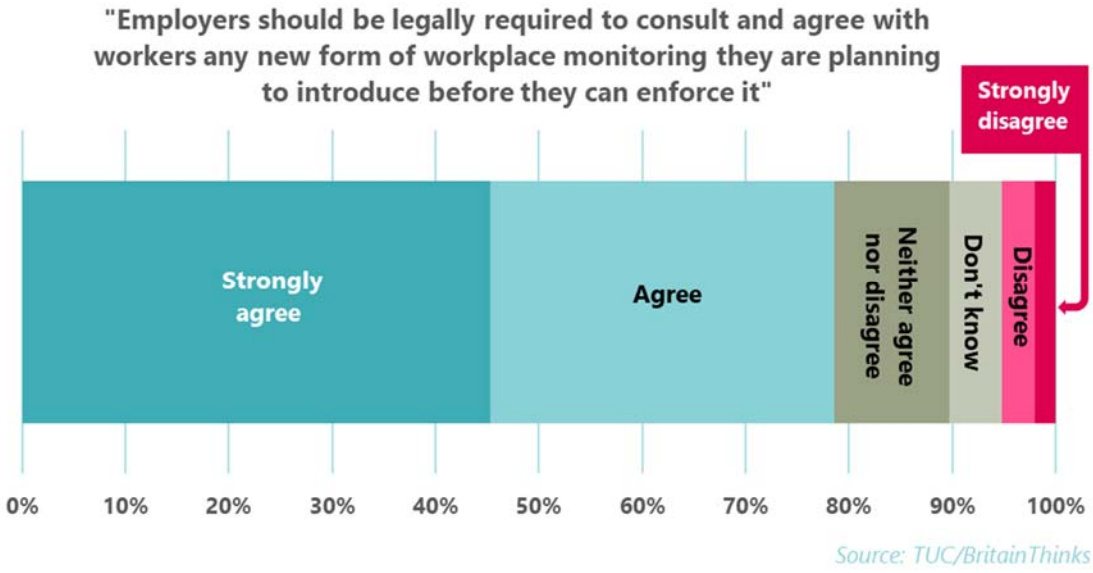


A lot of working people think that workplace monitoring is going to increase, yet have serious concerns about the risks of this. To make matters worse, they feel powerless to change it.

To avoid the risks of workplace monitoring, we need to shift some of the power away from employers who can use surveillance with little justification and with no consultation with staff. In the next section, we show that there's clear demand from workers for this power dynamic to change. Working people want some say over how they're monitored.

What do workers want to see change?

There's a clear will among workers to have some control and some say over how they are monitored at work. 79 per cent think that employers should be legally required to consult and agree with them before any new form of workplace monitoring is introduced and enforced.



Consultation alone is not enough for the majority of workers. In total, 81 per cent believe that employers should have to provide a clear and understandable justification to their workforce as to why they're introducing a new form of workplace monitoring before it is rolled out.

Being clear about the purpose of monitoring is also important. Staff want to know why they're being monitored and what it's used for. During our discussions with workers, we heard about cases where surveillance was introduced for business purposes (such as tracking vehicles for insurance purposes), but then used to measure performance.

Clarity and transparency apparent monitoring and what it's used for also allows workers to ensure they aren't caught out by monitoring they were unaware of. As one worker told us: "it you know what the rules are then you know not to break them".

Union case study: ensuring monitoring is used fairly and as agreed

As part of their Four Pillars agreement with the Royal Mail, CWU have negotiated a position that allows Royal Mail to use new technology to improve productivity, but without the threat of it being used to discipline or discriminate against workers.

The agreement includes a strong statement on how data will only be used in a way that respects workers' privacy:

> *Both parties recognise that new technology will improve Royal Mail's performance, and the service we provide to our customers. It is agreed that all individuals have a*

right to privacy at work, and it is accepted that there is a mutual obligation of confidence and trust applied to every contract of employment, and that all parties should act in a way so as not to break that relationship.

The use of data will be in the spirit of our agreements. It is recognised that the use of technology may increase levels of individual visibility and it is agreed that this new technology is not being deployed for, or will be used as, a disciplinary tool. As such it will not enhance the ability of managers, or the evidence available, to take disciplinary action.

The agreement includes details of a trial of a new hours-monitoring system, but there's a clear statement that this will not be used to track individuals or be used for individual performance management. There's also a commitment that a CWU rep will be involved in any evaluation of the trial.

What needs to change to protect workers from unfair monitoring?

Everyone has a right to a private life, even when they're at work. But, as we've shown, workplace monitoring is widespread and likely to become more so. New technology is making it easier than ever for employers to snoop on their workers.

Workplace monitoring puts rights at risk. In too many workplaces, workers' rights are being eroded with employers using excessive and intrusive forms of surveillance. As our research highlights, this creates stress and a loss of trust. It undermines staff morale and in some cases, can be demeaning for workers.

Data protection law, recently strengthened by the EU General Data Protection Regulation (GDPR), places significant limits on when and how employers should use new technology to monitor their staff in and outside the workplace.

But, too few people know about these rights and how they might apply in their workplace. Many feel unable to challenge employers' use of surveillance. This could be for fear that they will lose their job or be victimised at work. And employers have been able to get away with illegitimate snooping and relying on the data to dismiss employees.

In this section, we set out the legal protections that already exist. We then consider the policy changes needed to ensure that the right to a privacy in the workplace is respected and that workers are protected from excessive and intrusive surveillance and monitoring.

The policy recommendations include:

- Trade unions should have a legal right to be consulted on and to agree in advance the use of electronic monitoring and surveillance at work.
- It should be unlawful for employer to victimise or dismiss union members for using social media to build effective workplace campaigns.
- The government has a responsibility to introduce tougher regulation to prevent employers' use of excessive and intrusive surveillance and to protect people's right to privacy in the workplace. The government should ensure employers can only monitor their staff for legitimate reasons that protect the interests of workers.
- The government should also ask the Information Commissioner to update the Employment Practices Code to take account of new forms of technology, in consultation with the TUC and the CBI.
- The Code should have legal status and should be taken into account by courts and tribunals in employment cases.
- The Code should clearly state that employers can only use surveillance for legitimate reasons that protect the interests of workers and that employers must consult

recognised trade unions and reach agreement before introducing of electronic monitoring and surveillance in the workplace.

How does the law protect workers from excessive and intrusive monitoring?

This section considers how far the law protects workers from excessive and intrusive surveillance in the workplace.

Data protection law and workplace monitoring

Since 1998, the UK has had data protection rules that set out strict principles on how personal data can be used by organisations, including employers.

Personal data must be processed in a fair and lawful way. This includes data gathered through workplace surveillance such as:

- a person's image on a CCTV recording
- information about a person's use of a computer or use of emails or the internet at work.

Data protection law regulates when and how employers can carry out workplace monitoring.

Data protection law does not prevent employers from monitoring workers. There are legitimate reasons why employers may wish to monitor their workforce, for example, to prevent theft or make sure people work safely. But excessive or unjustified monitoring of staff can cause stress, a loss of trust and low morale.

If monitoring and surveillance involves collecting, storing or using personal data, it needs to be done in a way that complies with data protection principles and is fair to workers. Safeguards must be put in place before employers decide to introduce workplace monitoring. The ICO Employment Practices Code contains useful guidance.

Before deciding to introduce monitoring arrangements, the guidance recommends that employers should:

- be clear about the reason for monitoring staff
- carry out a risk assessment to identify any potential benefits for staff and identify any negative effects monitoring may have on staff. Any adverse impact of monitoring on individuals should be justified by the benefits to the employer and others
- consider whether there are less intrusive alternatives which could be used other than surveillance
- ensure that staff are aware of any monitoring or surveillance, the reasons for using it and how information can be used
- if information is gathered for one purpose, e.g. to protect health and safety, not use it for other reasons, for example, to discipline staff.

Data protection laws have recently been strengthened by the GDPR that came into effect on 25 May 2018.[4] The GDPR has the potential to provide increased protection for workers.

Key changes include far more stringent rules when organisations rely on consent to process personal data. Generally, employers will not be able to rely on workers' consent to process data – due to the imbalance of power in the employment relationship. Employers are required to carry out risk assessments before processing data.

Perhaps most significantly, the GDPR introduces far heavier penalties for employers that breach the regulations, including a maximum fine of 20 million Euros. The new rules on data protection have for the first time acquired teeth.

For a general summary of data protection law and how it affects the workplace in general, see the annex at the end of this report.

Privacy in the workplace is a human right

Everyone has the right to privacy and a family life, even in the workplace.

These rights are protected by Article 8 of the European Convention on Human Rights forms part of UK law, thanks to the Human Rights Act 1998.

According to the European Court of Human Rights, private life is a broad concept that does not stop at the door of the workplace. For example, under the Convention:

- Workers have a reasonable expectation of privacy when using the phone at work, especially if employees have not been warned them their telephone might be bugged[5]
- Monitoring of work emails can breach employees' rights to privacy, particularly where employers do not have a workplace policy[6]
- Employers must be able to justify surveillance of employee communications, especially if this involves reading employees' private emails or online messaging. They should also explore any less intrusive alternatives[7]
- Covert surveillance at work can only be justified in exceptional circumstances[8]

Monitoring email, internet and phone use

Employers have no legal obligation to allow staff to use the phone, email or internet at work for personal reasons. However, good employers trust staff with some private use during working hours, as long as it does not interfere with their work.

To comply with data protection rules, employers must tell staff of any plans to monitor email or internet use and the reasons for doing so. Employees should have a clear

---

[4] The EU General Data Protection Regulation was implemented in the UK through the Data Protection Act 2018.
[5] *Halford v United Kingdom* [1997] IRLR 471:
[6] *Copland v United Kingdom* (2007) 45 EHRR 37
[7] *Barbulescu v Romania* [2017] IRLR 1032
[8] *Lopez Ribalda v Spain* (App nos. 1874/13 and 8567/13, 9.1.18).

understanding of when monitoring will take place, why information is being gathered and how it will be used.

Employers should also adopt a workplace policy that:

- makes clear the extent and type of private use which is allowed
- clearly specifies any restriction on internet material which can use, view or copy, including for example materials which may be considered offensive as it contains racists language or nude or derogatory images
- spells out any restrictions on what materials can be sent, for example sending or receiving sexually explicit material and bans on offensive statements based on race, sex, sexuality, disability, age or religion.

CCTV and video surveillance

Employers may want to use CCTV or video surveillance for security reasons, such as theft, vandalism or threats to the safety of their staff.

Before introducing CCTV surveillance, employers should carefully consider whether this type of monitoring is justified, or whether the same results could be achieved by using other, less intrusive methods. Continuous CCTV monitoring of workers will rarely be justified.

If employers use CCTV surveillance that records the activities, staff should be told where and why it's being carried out.

CCTV surveillance should be targeted at areas only where particular risks have been identified and should not be used in areas where staff have a legitimate expectation of privacy. This includes, for example, toilets, changing rooms and private offices.

Covert monitoring

Covert monitoring should only be used in very exceptional circumstances. Employers must have genuine reasons to suspect that criminal activity is taking place and that telling staff about the monitoring would put the investigation at risk.

The Code of Practice published by the Information Commissioner's Office (ICO) says that it will be rare for covert monitoring of workers to be justified. It also makes clear:

- covert monitoring must only be used as part of a specific investigation and must stop once the investigation is complete
- if audio or video equipment is to be used, it must not be used in places such as toilets or private offices.

Surveillance at work and unfair dismissal protection

While the European Court decisions and data protection laws are welcome, UK courts have been far more reticent to recognise workers' right to privacy in the workplace. As a result,

employers have been able to get away with snooping on their workforces and using the information gathered to decide whether to sack people. [9]

For example, the Employment Appeal Tribunal (EAT) has decided:

- Covert surveillance of an employee's home who was suspect of fiddling time sheets, was not disproportionate[10].
- Filming of an employee in public did not breach his right to a private life[11]. The employee had been seen at a sports centre when he was supposed to be at work but had not clocked out. Because he had acted fraudulently he had no right to privacy.
- It was fair for an employer to dismiss an individual because of derogatory comments they had made about the employer on social media, even though the comments were posted two years before the dismissal took place. The employer had also found evidence on social media that the individual had consumed alcohol whilst on standby[12].

The reality in the workplace

And as our research suggests, most workers are not aware of the law, their rights, or the Information Commissioner's Code. The TUC is also concerned that the standards set out above are not complied with or are simply ignored in too many workplaces.

Workers' ability to rely on data protection rules in the workplace depends on their confidence to challenge management. We found that workers in higher paid positions (in occupational groups ABC1) were more likely to think they could challenge and stop forms of workplace monitoring that they were uncomfortable with than lower paid workers (in occupational groups C2DE) by some margin (42 per cent compared to 33 per cent). Again, trade union organisation is vital.

We are therefore calling for better regulation and enforcement to ensure that workers' rights to privacy and dignity at work are respected.

Key recommendations

Our research shows that vast majority of workers (79 per cent) say employers should be legally required to consult their workforces and reach agreement before using surveillance.

Trade unions are critical to ensuring workers have a voice and the power to speak up over how technology is used in their workplace. Where trade unions are organised, they regularly negotiate agreements on workplace monitoring to ensure that new technology is used to improve the quality of working life – and not lead to the exploitation of working people.

---

[9] Philippa Collins, 'The Inadequate Protection of Human Rights in Unfair Dismissal Law' (2017) *Industrial Law Journal*
[10] *McGowan v Scottish Water* [2005] IRLR 167
[11] *City and County of Swansea v Gayle UKEAT/0501/12*
[12] *BWB v Smith*_- UKEAT/0004/15

Trade unions should have a legal right to be consulted on and to agree in advance the use of electronic monitoring and surveillance at work.

Unions should also be able to take advantage of new technologies to recruit and organise working people and to campaign on workplace issues. **Union members should have a right not to suffer detriment including dismissal for using social media to build effective workplace campaigns.**

The TUC is campaigning for new rights to extend collective bargaining coverage so that more workers can have a genuine say over their working lives. But many working people cannot currently benefit from union representation. The government therefore has a responsibility to introduce tougher regulation to prevent employers' use of excessive and intrusive surveillance and to protect people's right to privacy in the workplace.

In summary, the government should:

- ensure employers can only monitor their staff for legitimate reasons that protect the interests of workers
- ask the Information Commissioner to update the Employment Practices Code to take account of new forms of technology:
  - Any revised Code should be the subject of detailed consultation with the TUC and the CBI.
  - The Code should have legal status and should be taken into account by courts and tribunals in employment cases.
  - The Code should clearly state:
    - Employers can only use surveillance for legitimate reasons which protect the interests of workers.
    - Employers must consult recognised trade unions and reach agreement before introducing of electronic monitoring and surveillance in the workplace.
- strengthen unfair dismissal rules to safeguard individuals' right to privacy at work, ensuring that courts and tribunal take data protection rules and the ICO's Code of Practice into account when deciding if a dismissal is lawful
- work with the ICO to ensure that workers' rights to privacy at work are properly enforced.

Annex: Data protection at work: the basics

Employers must ensure that personal data is processed in a fair and lawful way. For example, employers:

- can only gather and keep information for limited and stated purposes
- must tell workers what personal information is being recorded, how it was gathered, why it's being recorded and who is likely to have access to it and for what reason
- must ensure that information kept about individuals is accurate, relevant and up to date and that it is not kept for longer than necessary. they must also ensure that personal information is held securely
- must not reveal personal information to people who do not have a legitimate interest for seeing it, unless individuals have willingly given their employers permission to do so.

There are also stronger legal safeguards in place for special categories of data including information about a person's:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- mental or physical health
- sexual orientation or sexual life
- alleged or actual criminal offences.

Data protection law also gives workers important individual rights, including the right to:

- be informed about how any why their personal data is gathered and how it will be used
- request an easily accessible copy of the personal information that an employer holds about them. Thanks to the GDPR, the information must be provided free of charge and within 1 calendar month. In limited circumstances, employers can withhold information, for example where the disclosure of information may breach a duty of confidence to someone else, where providing the information would require 'disproportionate effort' or whether the information might undermine on-going negotiations between an individual and their employer
- ask employers to correct, delete or destroy any information held about them that is factually inaccurate. This could be particularly important in relation to disciplinary records or information held about health

The law also places limits on when employers can use **automated decision making** in the workplace. Under the GDPR, automated decision-making systems can only be used if it is necessary for the performance of or entering into a contract; if it is authorised by law; or an individual has explicitly consented to it.

Individuals must be told when a decision has been taken solely using automated decision making and have the right to ask for the decision to be reviewed by a person in authority. Organisations using automated decision making should also carry our regular reviews and use appropriate procedures to prevent errors.

These rights could provide important safeguards in the gig economy where employers use algorithms to allocate work and set pay rates. There's widespread concern these systems can be discriminatory and lead to unfair outcomes.

The Information Commissioner's Employment Practices Code sets out helpful guidance on how data protection rules affect the workplace.[13] This Code, however, does not have legal effect.

[13] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf