No. 297/26

30th October 2026

To: All CWU Branches

Dear Colleagues,

CWU response to government consultation on workplace monitoring technologies

The CWU has made the attached submission to the government's Make Work Pay consultation on workplace monitoring technologies (WMT).[1]

The CWU's response highlights examples of WMT used in the postal, telecoms, tech and financial services sectors. It argues that our members are at the sharp end of monitoring technologies that undermine trust, damage physical and mental wellbeing, increase stress and sickness absence, and contribute to lower job satisfaction and staff retention. These outcomes carry significant costs for employers. Workers who feel trusted and empowered are generally more motivated and productive than those subjected to continuous electronic surveillance.

The consultation seeks views on proposals to support the fair, transparent and responsible use of WMT. It asks whether there should be:

- **A statutory code** of practice on employers' use of WMT **(Option A**);
- **Primary legislation** to impose a duty to consult with trade unions or elected representatives where monitoring is introduced or significantly changed (**Option B**); or
- **A non-statutory code** of practice on employers' use of WMT (**Option C**).

The CWU's response strongly supports Option B which would place a legal duty on employers to consult trade unions before introducing or significantly changing workplace monitoring technologies. We argue that consultation should take place before procurement or deployment decisions are finalised and employers should be required to

[1] Make Work Pay: workplace monitoring technologies - GOV.UK

provide relevant information including Data Protection Impact Assessment (DPIAs), equality impact assessments and details of any automated decision making.

The response argues that a statutory code as set out in Option A would help, but only as a supplement to the legal rights established through primary legislation. Option C, based on non-statutory guidance alone, would not provide sufficient safeguards to support responsible adoption.

Beyond making the case for primary legislation under Option B, the CWU's response calls for:

- **Workers to have a clear legal right to information about what data is collected from WMT**, why it is collected, whether automated decisions are involved and how decisions are made, among other requirements.

- **Workers to have meaningful rights and ownership interests in the data collected about them at work.** This would allow workers and their representatives to understand how systems affect them and would support informed collective bargaining on pay, working time, privacy, workload and reasonable productivity expectations. Greater worker access to data would help identify emerging risks, prevent stress and burnout and create more balanced employment relationships.

- **Workers to benefit from productivity gains arising from new technology**, for example through better pay and conditions of employment and shorter working hours.

- **Safeguards to apply where WMT is used**, including mandatory impact assessments, equality and discrimination testing, human oversight of significant decisions and clear routes for challenge and redress.

The CWU recognises that WMT can deliver genuine benefits in areas such as health and safety, security, training, quality assurance and fraud prevention. However, positive examples such as location-based alerts warning of workplace hazards are the exception, not the norm. Our experience of workplace surveillance has been overwhelmingly negative. WMT is frequently deployed primarily to intensify work, scrutinise performance and increase managerial control. The claimed productivity benefits often fail to materialise, while the harmful impacts on workforce wellbeing, trust and morale are substantial.

Workplace monitoring and surveillance is an issue the CWU raised at the Labour National Policy Forum ahead of the 2024 general election, and Labour committed to consulting on this in its Next Steps to Make Work Pay policy paper in November 2024.[2]

The government's proposals offer an important opportunity to secure a new legal right for workers and trade unions to be consulted and negotiated with over the introduction of workplace monitoring technologies. However, the government has yet to indicate its preferred approach, and there is no guarantee it will proceed with Option B in the face of

[2] Next Steps to Make Work Pay (web accessible version) - GOV.UK

likely business opposition. Continued pressure from the trade union movement will therefore be essential to secure a legal right to consultation and negotiation, along with stronger regulation of WMT more broadly.

If you have any questions or comments on the above, please email btaylor@cwu.org.

Yours sincerely



Bill Taylor
Head of Research



CWU workplace monitoring consulta

CWU 150 The Broadway | Wimbledon | London | SW19 1RX
E: info@cwu.org | T: 020 8971 7200 | F: 020 8971 7300
General Secretary: Dave Ward | @DaveWardGS | Dave Ward CWU

30th September 2026

Make Work Pay Consultation - Workplace Monitoring Technologies

Communication Workers Union Response

Introduction

The Communication Workers Union (CWU) is the largest union in the communications sector in the UK, representing approximately 160,000 members in the postal, telecoms, tech, financial services and related industries. We are the recognised trade union for all non-managerial employee grades in Royal Mail, BT Group and Post Office Limited (POL), and we also represent members in many other companies. We welcome the opportunity to respond to the government's consultation on workplace monitoring technologies (WMT).[1]

There has been a significant increase in workplace digital surveillance and AI-driven monitoring across all the CWU's industrial sectors in recent years. Employers often justify these tools on productivity grounds, but in our experience workplace monitoring is frequently excessive and its effects are overwhelmingly negative. From location and movement tracking at Royal Mail to digital activity monitoring in fintech companies and voice analytics in BT and Santander contact centres, CWU members are at the sharp end of technologies that undermine trust, harm physical and mental wellbeing, increase stress and anxiety, and contribute to lower job satisfaction and staff retention.

The current regulatory framework provides insufficient protection against intrusive monitoring practices. Nor does it provide adequate transparency regarding how surveillance systems operate or their impact on workers, even at the most basic level. In particular, employers can too easily invoke commercial confidentiality to avoid meaningful scrutiny and withhold data protection impact assessments from workers and trade unions.

We believe workers should have meaningful rights over the data collected about them in the workplace, including visibility of how WMT affect issues such as pay, working time, health and safety. Workers and their representatives should also have a voice in decisions about the use of these technologies and their workplace impacts.

We recognise that new technologies will continue to be introduced in workplaces. The key challenge is ensuring their deployment is subject to meaningful safeguards that protect

[1] Make Work Pay: Workplace Monitoring Technologies Consultation

workers' rights and interests. Trade unions have an important role in securing these protections through collective bargaining, and our experience demonstrates that negotiated agreements can improve transparency, accountability and fairness. Government action is also essential to establish clear rules, strengthen workers' rights and ensure effective enforcement.

The CWU strongly supports the Government's Option B: introducing a legal requirement for employers to consult and negotiate with recognised trade unions before workplace monitoring technologies are introduced. This approach would help to deliver significant benefits, including stronger worker engagement and acceptance of new technologies, better-designed systems, and increased trust and confidence in their operation.

Experience of WMT

Question 06. Which of the following activities takes place in your workplace or organisation?

Selected:

- Location and movement tracking
- Digital activity monitoring
- Biometric access or verification
- Health and physiological monitoring
- Individual video monitoring
- Automated performance evaluation
- Telemetrics and front facing dashcams
- Other: Voice analytics, emotion recognition technologies, algorithmic management systems, screen recording, productivity scoring and AI-enabled customer interaction monitoring.

Our members report widespread use of workplace monitoring technologies across the tech, telecoms, postal and financial services sectors. Examples include handheld devices tracking postal and engineering workers' location and pace of work, call-centre systems monitoring conversations and productivity, vehicle telematics, driver monitoring technologies, screen recording software, keystroke logging and algorithmic performance management systems. In addition, some of our members are simply unaware that any monitoring is taking place and

therefore it is essential that there is greater transparency of surveillance technologies and their intended use.

Personal tracking devices in the postal sector

Workers in Royal Mail carry personal digital assistants (PDAs) that they use to sign in and out of work and that constantly track their location, collecting data on their pace of work, including walking speeds and time standing still. PDAs are capable of gathering huge amounts of data about how delivery workers go about their shifts and this data is accessible to supervisors with few barriers.

The CWU has agreements with Royal Mail to ensure the data is used in a supportive rather than a punitive way. However, Royal Mail managers have sometimes been found to be using the data to reprimand postal workers or challenge their performance. There is no doubt that these new technologies have led to a culture where the fastest time on a delivery round becomes the target norm and a postal worker could be reproached or penalised for legitimate interruptions to their work, like spending time answering customer questions on the doorstep, helping an elderly person across the road or navigating their delivery route in poor weather.

There are legitimate uses of tracking technology for safety purposes. However, as there are no concrete legal protections against the unbalanced application of the data gathered from surveillance devices, employers are free to use this data to unduly pressure workers. The use of technology itself and the use and/or application of the data garnered from that technology therefore must both be subject to regulation.

Artificial Intelligence-Powered recording systems in contact centres

Contact centre workers in BT, EE, Santander, VM02 and Capita are monitored from the moment they log in each day. They are required to use AI-powered applications to guide customer conversations and meet call handling targets. Many telecoms and financial services call centres use speech analytics technology that automatically evaluates every recorded customer conversation. The system analyses the language used by both the customer and advisor and generates a score for each interaction, as well as overall score over time. Employers claim that it is primarily a customer experience and coaching tool and it does not assess tone, pitch and silence. The CWU has had some consultation and trials for some of these systems before roll-out. There has been a mixed reception from members since implementation. Some have welcomed the technology as it has generated a better bonus for them, but other members have had a negative experience with the application scoring them lower than previously. A particular concern is that managers are often unable

to explain why the machine has generated a particular score, but they nevertheless rely on the technology in relation to performance.

Another example of workplace monitoring is the introduction of task mining. This tracks workers on their computer, analyses how work is carried out, identifies efficiencies and duplication and looks for opportunities for automation. We have been informed that the technology operates at employee level with data aggregated and anonymised and is not used for individual performance management. The CWU has concerns about the lack of consultation and protections for workers and we are concerned that workers have not been given sufficient information about what data is being collected, who can access it and whether it could be repurposed in the future. Our members have concerns over the potential for the machine to learn their jobs and eventual job cuts.

Attempts to install webcams for home based contact centre workers

During the pandemic, business process outsourcing firm Teleperformance issued webcams to monitor thousands of contact centre staff in Scotland which would have live-recorded footage of their home workstation and would have included mandatory random visual checks of workers.[2] They attempted to justify the move by saying that the cameras would tackle loneliness and create a '*highly collaborative and engaged workforce*'.[3]

The CWU's Scottish Region publicly intervened and condemned the plans as an unnecessary invasion of privacy and Teleperformance subsequently dropped the idea amidst mounting criticism[4]. However, Teleperformance's initial confidence in putting forward this webcam proposal is reflective of the lack of legal safeguards against these technologies and the importance of trade unions in creating protections for workers.

Vehicle tracking technology in post and telecoms

Vehicle telemetry systems have been used for over a decade in Royal Mail and Openreach to record metrics such as fuel efficiency, vehicle speed, braking and acceleration and GPS location. They also evaluate driver behaviour, including harsh braking, sharp turns and idling time. Openreach and other employers argue that these systems promote safer and more efficient driving practices, but they can also be used to penalise workers. The CWU has

[2] *'Big Brother' fears over call centre's webcam plan to snoop on Scots staff at home - Daily Record*

[3] *Union fears over call centre firm's 'home webcam plan' - BBC News*

[4] *(1) Call Centre Collective on X: "🚨 VICTORY FOR TELEPERFORMANCE WORKERS 📞 Workers at Teleperformance have won in the fight against the mandatory installation of webcams in their homes. Teleperformance has backed down and webcams will now be completely voluntary. The collective strength of workers wins again!" / X*

reached agreements with Openreach to ensure that the data from these will only be used to coach workers in a supportive rather than a punitive way.

For example, the Openreach Driver Safety app is a phone-based application that allows drivers to "*learn more about their driving style and how to become a 'greener' driver*". No data is collected by the phone and use of the app remains entirely voluntary for staff. BT and CWU have agreed that "*the data and information gathered will not be used punitively or discussed at line management level, including at 121s, and in team meetings. It will not be used in disciplinary action*."

However, Openreach is looking to expand the use of these systems and has previously proposed to introduce inward facing dashboard cameras to monitor driver behaviour, which the CWU successfully opposed.

Employee monitoring and analytics in the tech sector

Tech sector workers are increasingly being subjected to 'bossware' surveillance technologies such as mouse tracking and screen recording systems, which scrutinise every detail of their behaviour and performance.

The CWU's United Tech and Allied Workers Branch (UTAW) has a campaign to tackle workplace surveillance, which alerts members to the surveillance applications used by employers. This includes software such as "Kickidler", "Work Examiner" and "Staff Cop", all of which are capable of tracking workers on a continuous basis throughout the day and monitoring their activity and output in forensic detail. These programmes often also offer automated analysis of workers' 'productivity' based on this surveillance.

Kickidler says that its software can record videos of employees' screens, and it can run in '*stealth mode*' so that workers are unaware they are being monitored. Kickidler acknowledges in its guidance that secret monitoring is rarely legal[5] but advises that stealth mode can be used in certain situations, including when a company is looking for baseline data prior to announcing employee monitoring, or when they are confident there are "*chronic procrastinators*" amongst their staff.[6]

BT's development of continuous authentication software

BT is currently developing new software to continuously monitor workers at their computers with the aim of improving cybersecurity and ensuring that only authorised workers have access to a company's IT systems. Known as continuous authentication software, these

[5] *Legal Opinion: Employee Monitoring Software and Privacy Laws (kickidler.com)*
[6] *Employee Monitoring Software | Kickidler*

systems would constantly film workers with a webcam or front-facing camera and identify if their face lines up with the expected dimensions. They can also track the user's emotions in real time, which would send out alerts if someone appears, according to the software, tired or stressed.

The software is at 'proof of concept' stage and there is no current proposal to roll it out in BT or any other employer where the CWU is active, but we are concerned about the risks posed by this new technology. The emotion recognition aspect of this technology is a particular concern, with the Information Commissioner's Office warning that this could lead to discrimination, and other experts cautioning that it could breach workers' data rights and create a culture of fear in the workplace.[7]

Question 07. What is the stated purpose of this WMT?

Selected:

- Work allocation or scheduling
- Health and safety compliance
- Performance evaluation, discipline or appraisal
- Security or fraud prevention
- Improve productivity or efficiency
- Supporting employee training or wellbeing

Employers typically justify WMT on the grounds of productivity, efficiency, operational management, security and health and safety. Some technologies can deliver clear benefits. For example, location-based alerts warning postal workers about dangerous dogs can improve worker safety, while monitoring technologies can support security, quality assurance, training and fraud prevention.

However, our experience is that WMT is frequently deployed primarily to intensify work, scrutinise performance and increase managerial control. The claimed benefits often fail to materialise, while the harmful impacts on workforce wellbeing, trust and morale are significant.

[7] *Why office workers could soon be filmed all day at their desks | Tech News | Metro News* and Innovation in action: continuous biometric authentication

Some of the harmful effects of surveillance are illustrated in the following case studies from the CWU's UTAW branch which highlight stress from constant micromanagement, the use of AI assessments in high-risk decision making on issues such as performance and pay, and concerns about the security of personal information being captured by monitoring systems.

More generally, we are concerned about employers using Large Language Models (LLMs) such as chatGPT to input and aggregate employee data for workplace monitoring purposes - including Personally Identifiable Information (PII) - sometimes in ways that are not clear to the employee.

Fintech case study

The CWU's UTAW branch recently conducted a stress survey in a major British fintech company. Surveillance and workplace monitoring came up as a key issue of concern for respondents. The company's employees are subject to almost constant surveillance (through mouse/click tracking) which manifests most obviously as pop ups that appear throughout the day based on their activity. If they are active during a designated break, such as finishing a task before going for lunch, the pop up will ask why they have not gone for their break. If their mouse does not move for 10 minutes, a pop up will ask them if they are still there. If they are late returning from lunch, it will ask why they are late. This constant monitoring makes employees feel that they cannot step away from their screen or manage their time effectively. This has had a huge impact on the health and wellbeing of employees, with survey respondents reporting concerns including:

"I often feel like i'm constantly being watched and measured on everything I do… I feel like they want us to sprint in a marathon all the time."

" it's stressful juggling work and childcare…and having to compress screen breaks to do school runs."

"it has affected my stress level personally and disrupted a lot of my personal life."

"I have been off ill for 2 weeks due to stress in the workplace."

"the fact that we are constantly monitored.. is really stressing me out."

"we were told if you don't like it, leave."

"The way we are monitored to every single minute of our shift is really stressful and then being questioned on each thing adds to that stress because I feel we're made to feel like we have done something wrong constantly and there is no trust."

These systems do not actually track if employees are meaningfully working and little to no consideration seems to be given to time needed to think, research, read or make written notes. These systems do however severely increase workplace stress because they leave workers feeling they are under constant micromanagement rather than trusted to do their jobs.

Multiverse case study

At digital skills company Multiverse, coaches have raised the alarm about surveillance and monitoring, with huge impacts to stress and mental health. One member reported the following:

“Previously, we were observed by our managers roughly once a month as part of the usual quality and performance process. That is now changing so that all of our live teaching sessions are observed and analysed by AI.

“On some days we can deliver up to six hours of live sessions, so this means nearly all of my working day is continuously monitored and assessed. That AI-generated information is then considered alongside learner LSAT feedback and feeds into our progress reviews, which in turn affect progression and pay.

“The policy is that a manager will ultimately make a human judgement rather than decisions being made automatically by AI. However, our concern is that this still represents a huge increase in the amount of monitoring taking place. AI-generated assessments are now part of the evidence used to make decisions about our performance and remuneration. Further to our worries is that this data is being used to train AI models looking to replace us. Its having a massive impact on my mental health."

Another member reported:

"They say ‘it's not for performance monitoring’ but then proceed to show us slides with performance rankings. It's so intrusive and so idiotic. Morale is at an all time low. We were never consulted.

"Our own learners are being recorded too. If they don't want to be recorded they have to turn their cameras off and not speak.

"We were recently given an FAQ document from the company that reads 'we think AI will do things a human coach can't do today.. like adapting to a learners context in real time by assessing their entire work history or watching every apprentices screen to help them unlock the answer to their specific problem'. The ethics and security concerns around some of this are wild."

Meta case study

Meta has attempted to enact draconian surveillance without employee consent or consultation. It transpired the monitoring was more invasive than first disclosed. For instance, they said that it was filtered per-app, but the leaked data came from a Video Learning Model which captures the full screen, interprets what it sees, and writes a summary in a table, explicitly identifying and extracting Personally Identifiable Information (PII) for storage in fields. Employees could not and can not be sure that the data was safely/securely stored and one huge and invasive leak of identifiable data happened within weeks of the tool being implemented in the US. Nearly 100 people globally were confirmed to have accessed this data.

The company said the data would be disassociated from employees, yet it was organised into one table per employee, with employee ID included in the table.

Workers explicitly asked for the privacy review information when the monitoring was started and it was announced, but those questions were dismissed by the company's leadership.

Although the tool has not been implemented in the UK/EU, emails and chats between UK/EU employees and their US colleagues were captured.

Software company case study

One software company where we have members uses Persona for every multi-factor authentication, which is mandatory.[8] This involves every employee taking a picture of their government ID and scanning their face at 3 angles into the software. This data is stored on a back end for an unspecified amount of time. Even our members working in cybersecurity for this company have told us they weren't able to see if or when the data is deleted. The un-

[8] Secure Identity Verification Solutions | Persona

redacted images are available to employees within certain teams who work on security at the company.

Interestingly, the policy is mostly global but not in place in Germany where there are much better protections for workers regarding this kind of surveillance/ID tracking. In India they redact the written information on the ID, such as the ID number. This is not the case in the UK where the full images are stored on the back end.

Question 08. To the best of your knowledge, how are decisions made using this technology?

Selected:

Combination of automated and human input – although human oversight and intervention is limited in practice due to system complexity that disempowers managers and makes it difficult to override system decision making.

In most workplaces decisions made using algorithmic management systems and surveillance technologies are presented as involving human oversight. However, in the vast majority of cases managers have no understanding of how AI systems work or why they reach certain decisions. This disempowers managers and makes it more difficult for them to override or adjust algorithmic decision making processes. Algorithmic scores, productivity metrics and automated recommendations often have a decisive influence over management decisions relating to performance, work allocation and attendance. In practice, human review can become little more than a rubber-stamping exercise, particularly where managers are under pressure to meet productivity targets.

Question 10. What information was provided in your workplace before the introduction of WMT?

Our experience is that workers and unions are often given limited information about the purpose, operation and impacts of new monitoring technologies.

In particular, employers have repeatedly refused requests to share Data Protection Impact Assessments (DPIAs), frequently citing commercial confidentiality. For example, Openreach have refused to share DPIAs relating to vehicle monitoring technologies and Royal Mail have refused to share DPIAs relating to Personal Digital Assistants. This creates a significant imbalance of power because workers and their representatives have little visibility of the

likely impact of surveillance, algorithmic management or automated decision-making systems before deployment.

Meaningful transparency should include access to DPIAs and wider impact assessments regarding new technologies, procurement information, data sources, purposes, retention periods and details of any automated decision-making.

Question 11. Were workers or their representatives consulted before the introduction of WMT?

In the CWU's major recognised employers including Royal Mail and BT, the union has generally been consulted in the introduction of workplace monitoring technologies, and in many cases we have reached agreements on their reasonable use.

This demonstrates that union consultation and collective bargaining can lead to better outcomes and stronger protections. Examples include agreements with Royal Mail and Openreach limiting the use of monitoring data for disciplinary purposes and ensuring technology is used in a supportive way. CWU campaigning also recently led to the withdrawal of proposals for inward-facing vehicle cameras and webcam monitoring in Openreach.

However, consultation is inconsistent and often inadequate. Many employers introduce technologies unilaterally or present workers with a fait accompli after key decisions have already been made.

Question 12. What impact has WMT had on workers?

Our experience is that the overall impact has been overwhelmingly negative.

Workers frequently report:

- Work intensification.
- Increased stress and anxiety.
- Loss of autonomy and professional judgement.
- A feeling of constant surveillance and scrutiny.
- Increased sickness absence.
- Lower morale and engagement.

- Higher staff turnover and attrition.
- Reduced trust in management.

Research and workplace experience both suggest that excessive surveillance can be counterproductive for workers, reducing motivation and commitment rather than improving performance.

Question 13. What impact has WMT had on employers or businesses?

Many employers believe WMT will improve productivity and efficiency.

While there can be genuine benefits in specific circumstances, excessive monitoring often undermines these objectives. The resulting stress, disengagement, sickness absence, disputes and employee turnover create significant costs for businesses. Workers who feel trusted and empowered are generally more motivated and productive than workers subjected to continuous electronic surveillance.

Question 14. Are existing legal protections sufficient?

No.

Existing protections are fragmented, difficult for workers to enforce and heavily dependent on individual data protection rights. In practice, employers enjoy broad discretion to introduce monitoring technologies provided workers are notified.

Current legislation does not adequately address power imbalances in the employment relationship, nor does it guarantee meaningful worker involvement before surveillance technologies are introduced.

Question 15. Should workers be provided with more information about WMT?

Yes.

Workers should have a clear legal right to information about:

- What data is collected.
- Why it is collected.
- How long it is retained.
- Who has access to it.

- Whether AI or automated systems are involved.
- How decisions are made.
- The results of DPIAs and relevant risk assessments.

Transparency is an essential precondition for trust, accountability and informed consent.

Question 16. Should workers have greater rights regarding workplace data?

Yes.

Workers should have meaningful rights and ownership interests in the data collected about them at work.

This would allow workers and their representatives to understand how systems affect them and would support informed collective bargaining on pay, working time, privacy, workload and reasonable productivity expectations. Greater worker access to data would help identify emerging risks, prevent stress and burnout and create more balanced employment relationships.

At present, employers possess almost all of the information and control relating to workplace data, creating a significant imbalance of power.

Question 17. What safeguards should apply where WMT is used?

The following safeguards should apply:

- Necessity and proportionality requirements.
- Mandatory DPIAs and AI impact assessments.
- Publication and disclosure of assessments to workers and recognised trade unions.
- Human oversight of significant decisions.
- Restrictions on covert monitoring.
- Limits on the use of monitoring data for disciplinary purposes.
- Equality and discrimination testing.
- Independent auditing of high-risk systems.
- Clear routes for challenge and redress.

Monitoring should be used only where justified and where less intrusive alternatives are not available.

Question 18. Which policy option do you support?

We strongly support Option B: a legislative requirement to consult and negotiate with trade unions, or elected worker representatives where no union is recognised, before workplace monitoring technologies are introduced.

This approach would:

- Improve worker engagement and acceptance.
- Lead to better-designed systems.
- Increase trust and confidence.
- Improve transparency and accountability.
- Identify risks before deployment.
- Reduce disputes, grievances and legal challenges.
- Improve compliance with data protection and equality law.
- Encourage responsible innovation.
- Ensure technology delivers benefits for workers and employers alike.

Our experience shows that where unions are involved early, employers achieve better outcomes and avoid many of the problems associated with poorly designed surveillance systems.

Question 19. What should consultation and negotiation involve?

Consultation should occur before procurement or deployment decisions are finalised.

Employers should be required to provide:

- DPIAs and AI impact assessments.
- Business cases and stated objectives.
- Information on data collection and processing.
- Equality impact assessments.

- Details of any automated decision-making.
- Independent audit results where applicable.

Trade unions should have sufficient time, information and resources to engage meaningfully in the process.

Question 20. Are there any additional comments?

Technology can and should play a positive role in the workplace. We recognise the potential benefits of WMT in areas such as safety alerts, security, fraud prevention, quality assurance, training and operational efficiency.

However, our experience across the tech, telecoms, postal and financial services sectors is that workplace monitoring technologies have too often been used in ways that intensify work, undermine autonomy and damage physical and mental health.

The Government should adopt a framework based on transparency, worker voice, collective bargaining and accountability. The introduction of a statutory duty to consult and negotiate with trade unions before deploying workplace monitoring technologies would be the single most effective step towards ensuring that technological innovation supports both productive businesses and healthy, sustainable working lives.

Principles for responsible use of WMT which supports good industrial relations

Question 21. To what extent are the 8 principles demonstrated in your workplace?

Our overall experience across the tech, telecoms, postal and financial services sectors is that implementation is inconsistent and often poor. The 8 principles listed are sometimes demonstrated in the CWU's major recognised employers where we have constructive industrial relations and strong collective agreements. But even under those positive circumstances, the CWU has to work consistently hard to ensure that the union is consulted appropriately on new technologies and that agreements are properly followed. Worker engagement and transparency are especially weak, with employers frequently withholding key information about monitoring systems and refusing to share DPIAs.

In many areas where we do not have a recognition agreement in place or we have less influence due to low membership levels, the 8 principles are never demonstrated.

8 principles:

1. Purpose and rationale
2. Transparency and understanding
3. Worker engagement and voice
4. Fairness and equality
5. Necessity, proportionality and privacy
6. Human oversight and accountability
7. Dignity and wellbeing
8. Accuracy, reliability and review

Question 22. Which 2 principles are most important?

1. Worker engagement and voice
2. Transparency and understanding

Without meaningful consultation and transparency, workers cannot understand, challenge or influence systems that may affect their pay, working lives, privacy, health and wellbeing.

Question 23. Please explain your answer.

These principles underpin all the others. Meaningful worker involvement leads to better system design, improved trust, earlier identification of risks and fewer disputes. Transparency is necessary for accountability and informed decision-making.

Question 24. Would these principles support responsible adoption and use of WMT?

Yes

The principles provide a useful foundation. However, voluntary principles alone will not change behaviour in any meaningful way without statutory requirements and enforceable rights.

Question 25. Please explain your answer.

Many employers already claim to follow similar principles while introducing highly intrusive monitoring systems. The key issue is not the existence of principles but ensuring compliance through regulation, consultation and enforcement.

Question 26. Are any important elements missing?

Yes.

Additional principles should include:

- Collective bargaining and consultation rights.
- Worker access to and control over workplace data.
- Publication of DPIAs and AI impact assessments.
- Rights to challenge algorithmic decisions.
- Limits on the use of monitoring data for disciplinary purposes.
- Benefit-sharing where productivity gains arise from technology, for example through better pay and conditions of employment and shorter working hours.

Question 27. What challenges exist in applying these principles?

Select all that apply:

- Lack of clarity around legal requirements.
- Difficulty applying principles consistently.
- Rapid evolution of technology.
- Lack of worker trust/confidence.
- Data protection/privacy concerns.
- Limited worker or representative capacity.

Comments

A major challenge is the information imbalance between employers and workers. Employers routinely possess extensive information regarding WMT while workers and unions have limited access to the evidence used to justify deployment.

The role and value of worker engagement

Question 28. Importance of engagement?

Strongly agree

Meaningful engagement is fundamental to responsible deployment of WMT and successful industrial relations.

Question 29. What does meaningful engagement look like?

Engagement should:

- Begin before procurement and deployment.
- Include provision of DPIAs and risk assessments.
- Allow unions sufficient time and information to respond.
- Include negotiation with a view to agreement.
- Continue throughout the life of the system through joint governance and review processes.

Question 30. Examples of engagement working well or badly.

The CWU can report some positive examples of early and meaningful engagement by employers regarding WMT. This includes agreements reached between the CWU and employers such as Royal Mail and Openreach which restrict punitive use of monitoring data and establish safeguards around technology use.

The CWU negotiated with Openreach regarding a Peoplesafe Lone Worker App, which is designed to strengthen the safety of field and lone workers. This is a good example of how a trade union can ensure better outcomes on WMT. A trial period identified some issues, around welfare checks creating additional tasks for employees and contributing to feelings of

being monitored and surveilled. The final agreement reached in January 2026, included important safeguards, including limits on manager access, no continuous location tracking and voluntary use of personal phones. Location data is only accessed when a safety alert, missed welfare check or failure to sign off occurs. Workers can also choose additional welfare checks voluntarily. The case demonstrates how early worker and union involvement can help shape the use of workplace technology, establish clear safeguards around monitoring and data, and ensure that technology introduced for safety purposes does not become a general performance monitoring tool.

Another good example of early worker and union involvement is a trial running on Geotab forward facing dashcams and associated telematics in Openreach. The technology is designed to help protect engineers and drivers, reduce road risk, provide objective evidence following incidents and support compliance. The agreement for the trial ensures GeoTab will not provide live video viewing, inward facing video or record in-cab audio. Line Managers will not have access to individual driver scores, dashboards, app data, or footage except where information is formally disclosed through the agreed governance process.

Poor examples include attempts to introduce inward-facing vehicle monitoring and home-working webcams without meaningful consultation, as well as repeated employer refusals to share DPIAs.

Options for intervention

Option A: Statutory Code of Practice

Question 31. Would a statutory code help?

Yes

But only as a supplement to legislative consultation rights.

Question 32. Impact on industrial relations?

Somewhat positive

Question 33. Explain.

A code would improve clarity and expectations but would not guarantee worker involvement or prevent unilateral employer action.

Question 34. Impact on adoption of WMT?

No impact

Responsible employers already adopting WMT should experience little impact.

Question 35. Explain.

A code would encourage more responsible use rather than prevent adoption.

Question 36. Benefits, costs, risks or challenges?

Benefits

- Greater clarity.
- Better consistency.
- Improved awareness of obligations.

Risks

- Becoming a box-ticking exercise.
- Insufficient enforcement.
- Limited influence on poor employers.

Question 37. Main purpose of a code?

Select all:

- Improving transparency.
- Reducing disputes.
- Clarifying expectations under existing law.

- Supporting responsible technology adoption.

Question 38. Should the code qualify for TULRCA compensation adjustments?

Yes

Failure to follow the code should have legal consequences.

Question 39. Should guidance supplement the code?

Yes

Practical guidance should accompany any statutory code.

Option B: Legislative Duty to Consult and Negotiate

Question 40. Would a legislative consultation requirement better support responsible WMT?

Yes

Strongly.

Question 41. Explain.

This is the option we most strongly support.

It would:

- Improve worker voice.
- Improve design and implementation.
- Increase trust.
- Reduce disputes.
- Improve legal compliance.
- Produce better outcomes for employers and workers.

Question 42. Impact on industrial relations?

Very positive

Question 43. Explain.

Most disputes arise because workers discover systems after decisions have already been taken. Consultation encourages cooperation rather than conflict.

Question 44. Impact on adoption of WMT?

Somewhat increased adoption

Question 45. Benefits, costs, risks or challenges?

Benefits

- Better systems.
- Improved trust.
- Reduced legal challenge.
- Better health and wellbeing outcomes.
- Increased workforce engagement.

Costs

- Additional consultation time.

Challenges

- Ensuring meaningful consultation rather than token engagement.

Overall benefits greatly outweigh costs.

Question 46. Preferred model?

Duty to consult and negotiate with a view to agreement before WMT is introduced or changed.

Question 47. Explain.

This best reflects the commitment in the Make Work Pay Plan and addresses the power imbalance between employers and workers. It is also the approach most likely to produce genuinely informed decisions.

Question 48. What should trigger consultation?

Select all:

- Introduction of any new WMT system.
- High-risk WMT, including systems that affect recruitment, disciplinary issues and performance management processes.
- Significant changes to existing WMT.
- Use of WMT for performance, discipline, pay or dismissal.
- Request from workers or representatives.

Question 49. Should consultation be time limited?

Up to 6 months would balance meaningful consultation with business flexibility for the introduction of new WMTs. However, we believe that employers should be required to consult with unions and worker representatives at regular intervals throughout the adoption and ongoing use of WMTs.

Question 50. Further consultation for significant changes?

Yes

Changes in purpose or functionality can substantially alter risks and impacts.

Question 51. What if representatives object?

Select:

- Employer should pause implementation and propose alternatives.

- Employer should seek external mediation.
- Employer should not proceed without agreement in specified high-risk cases.

High-risk systems, such as those that affect recruitment, disciplinary issues and performance management processes should require stronger protections.

Question 52. Who should be covered?

All individuals exposed to WMT, regardless of employment status. This should include workers who are classed as self-employed but who have all the characteristics of workers or employees, which includes many delivery drivers and couriers in the platform economy.

Question 53. Explain.

The risks arise from exposure to monitoring, not employment status. Platform workers and other atypical workers can be heavily affected by algorithmic management systems.

Question 54. When should enforcement apply?

Select all.

Consultation duties should be enforceable where:

- No consultation occurred.
- Consultation was procedurally inadequate.
- Workers had no genuine opportunity to influence outcomes.

Question 55. What remedies should be available?

Select all.

- Suspend deployment until compliance.
- Disclosure of required information.
- Financial penalties or compensation.

- Regulatory referral.

Question 56. How should consultation be enforced?

Enforcement should include employment tribunal remedies, access to Acas mediation, regulatory enforcement powers and financial sanctions for repeated non-compliance.

Option C: Non-Statutory Guidance

Question 57. Would guidance alone support responsible adoption?

No

Question 58. Explain.

Guidance may help responsible employers but will have limited impact on employers who choose not to engage workers.

Question 59. Impact on industrial relations?

Selected:

No impact or possibly somewhat positive

Question 60. Explain.

Guidance may improve awareness and understanding but is unlikely to change behaviour significantly without legal obligations.

Question 61. Impact on adoption of WMT?

No impact

Question 62. Explain.

Most employers will continue their existing practices whether guidance exists or not.

Question 63. Benefits, costs, risks or challenges from this option?

Benefits for employers

- Low cost.
- Flexible.
- Easy to update.

Risks for workers

- Lack of compliance.
- Inconsistent application.
- No meaningful worker voice.
- No enforcement.

Question 64. What should guidance include?

Select all.

- Sector-specific guidance.
- Case studies.
- Regular updates.
- Legal compliance checklists.

Additional content:

- Worker consultation templates.
- DPIA disclosure guidance.
- Algorithmic management examples.
- Health and wellbeing impact assessments.

Question 65. Who should guidance be aimed at?

Select all.

- Employers.
- Workers.
- Trade unions and representatives.
- HR professionals.
- WMT providers and vendors.

Question 66. What would increase use of guidance?

Select all.

- Regulatory endorsement.
- Practical examples.
- Sector-specific material.
- SME toolkits.
- Worker-facing summaries.

Final Questions

Question 67. Should government consider any other options?

Yes.

Government should consider:

- A legal duty to publish and share DPIAs and AI impact assessments with workers and unions.
- Stronger rights to human review of automated decisions.
- Worker rights to access workplace data collected about them.
- Independent auditing of high-risk AI and monitoring systems.
- Enhanced ICO powers and resources to enforce workplace protections.

Question 68. Any other comments?

We recognise that WMT can deliver genuine benefits, particularly in health and safety, security, training, quality assurance and fraud prevention. Examples such as dangerous dog alerts for postal workers demonstrate that technology can improve working conditions when used responsibly. CWU members of the dog attack working group in Royal Mail first alerted Royal Mail to technology back in 2018 that was used by the US postal service. Our call for 'real time' dog attack risk management mapping technology was supported by academic experts at Liverpool University. This technology is now being used in Royal Mail and although it is still in a phase of development and improvement, it is already having a positive impact and protecting delivery workers from the risk of harm from dangerous dogs.

However, positive examples such as this are the exception, not the norm. Our experience across the tech, telecoms, postal and financial services sectors has been overwhelmingly negative. Too often WMT is used to intensify work and monitor workers continuously, which undermines autonomy and increases stress, anxiety, sickness absence and attrition.

The central issue is the imbalance of power in the employment relationship. Employers currently control the design, deployment and interpretation of monitoring systems, while workers and unions are frequently denied access to information, including DPIAs, on grounds of supposed commercial confidentiality. This leaves workers unable to assess the likely impacts of technologies that shape their working lives.

The Government should rebalance this relationship through legally enforceable consultation and negotiation rights, greater transparency, stronger worker data rights and robust safeguards for algorithmic management and AI systems. Option B is therefore the most effective and proportionate route to achieving responsible innovation, improved productivity and fair work.

For further information on the view of the CWU contact:

Dave Ward
General Secretary
Communication Workers Union
150 The Broadway
London
SW19 1RX

email: dlynch@cwu.org
Telephone: (+44) 020 8971 7251

30th September 2026