BOSS WARE

The dangers of high-tech worker surveillance & how to stop them

BIG BROTHER WATCH
BigBrotherWatch.org.uk

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact
Silkie Carlo
Director
Email: silkie.carlo@bigbrotherwatch.org.uk

Jake Hurfurt
Head of Research and Investigations
Email: jake.hurfurt@bigbrotherwatch.org.uk

Susannah Copson
Legal and Policy Officer
Email: susannah.copson@bigbrotherwatch.org.uk

Acknowledgements
Thank you to our investigation volunteers, Maria Lira Moran and Jacqueline Holo, for their important help in researching this report.

Bossware: The dangers of high-tech worker surveillance, and how to stop them

Published: September 19 2024

CONTENTS

INTRODUCTION

Workers in the UK are under increasingly heavy surveillance from their bosses and their employers. Significant advances in the sophistication of technology, falling costs, and the shift to home working during the pandemic have all been key driving factors in the rise of worker surveillance. Britain Thinks found that the majority of workers (60%) believe they have been subject to some form of surveillance at their current or most recent job, and in 2021 1 in 4 workers reported device monitoring.[1]

Justifications for the growing monitoring of workers range from employee and public safety to counter fraud, whilst the importance of privacy, dignity and data protection for workers is effectively sidelined. Just because a person is a company's employee does not negate their data rights and give employers a carte blanche to surveil them.

Unlike some growing forms of extreme surveillance, some workplace monitoring can be justified when the circumstances allow. Even basic workplace monitoring rightly requires that all data processing is necessary, proportionate and transparent. Some technologies can never be justified, including mandatory biometric sign-ins to office jobs or emotion recognition of people's facial expressions to analyse their performance. Employers must be aware of their legal obligations and the degrading effects of excessive surveillance, and unions and privacy advocates must advocate against unjustifiable technologies in the workplace. However, this report also finds that there are gaps in the law and enforcement of existing laws that keep workers at risk of unfair, intrusive and harmful surveillance.

Big Brother Watch's research draws on open-source and publicly available information as well as interviews with workers impacted by monitoring and the unions representing them. We found that too often a 'surveillance first, questions later' approach is taken by companies, with productivity being prioritised over workers' autonomy and dignity to justify intrusive monitoring.

Workers told us that over-surveillance by bosses left them feeling uncomfortable, mistrusted and at times misled by their bosses. A 2022 Trade Union Congress poll suggested that at least 3 in 5 workers had been monitored by an employer, with this often having negative impacts on workers.[2] UNISON Scotland research found that, even before the boom in workplace surveillance technologies, members

1 Intrusive Worker Surveillance Tech Risks "Spiralling Out Of Control" Without Stronger Regulation, TUC warns, TUC, 28th February 2022: https://www.tuc.org.uk/news/intrusive-worker-surveillance-tech-risks-spiralling-out-control-without-stronger-regulation

2 Intrusive Worker Surveillance Tech Risks "Spiralling Out Of Control" Without Stronger Regulation, TUC Warns, TUC, 28th February 2022, https://www.tuc.org.uk/news/intrusive-worker-surveillance-tech-risks-spiralling-out-control-without-stronger-regulation

in jobs with electronic monitoring overwhelmingly described the experience as "demeaning" and more than half reported stress and anxiety as a result, with 17% suffering depression. Some staff members reported suffering lost sleep and extended sickness as a result of monitoring, and 52% considered resigning as a result.[3] Meanwhile, more recent polling of employees in the US found that employer surveillance had specific negative impacts on workers, from pressure around working more hours and presenteeism to anxiety linked to not knowing if they were being watched at that moment.[4] UK news coverage of the rise of workplace surveillance has often featured workers saying that the feeling of being watched constantly makes work feel much more stressful, and excessive monitoring has been linked to higher staff turnover.[5][6]

This lack of transparency could also lead to employees feeling that decisions about them are unfair, as they are not aware of the levels of surveillance they are subject to, the data that feeds into decisions, or how software tools influence them. The TUC has warned of a "huge lack of transparency over the use of AI at work, with many staff left in the dark over how surveillance tech is being used to make decisions that directly affect them"; and yet that automated decision making is increasingly being used in recruitment, line management, performance ratings, shift allocation and deciding who is disciplined or made redundant.[7] Surveillance at work is often linked to greater levels of algorithmic rather than human management, which can lead to an increased perception of isolation and less autonomy among workers as their day-to-day becomes directed increasingly by machines.[8]

Excessive workplace surveillance can breach individuals' data and privacy rights, but it also directly undermines the democratic health of the country. Oppressively surveilled workplaces can obstruct unionisation and suppress workers' voices, directly harming democracy. The power balance between workers and employers, unions and corporations, reflects the power the public has in a society – the right balance is essential in a healthy democracy.

---

3 UNISON Scotland Privacy Survey 2004: https://www.unison-scotland.org.uk/briefings/privacysurvey.html

4 78% Of Employers Engage In Remote Work Surveillance, ExpressVPN Survey Finds, ExpressVPN, 3rd November 2023, https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/#mental

5 How Worker Surveillance Is Backfiring On Employers, BBC Work: In Progress, 30th January 2023, https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers

6 One In Five Uk Adults Believe They Have Been Monitored By An Employer, the Guardian, 2nd October 2023, https://www.theguardian.com/world/2023/oct/02/uk-adults-monitored-by-employer-workplace-surveillance

7 Intrusive worker surveillance tech risks "spiralling out of control" without stronger regulation, TUC warns – TUC, 28 February 2022: https://www.tuc.org.uk/news/intrusive-worker-surveillance-tech-risks-spiralling-out-control-without-stronger-regulation

8 Monitoring And Surveillance Of Workers In The Digital Age, Sara Riso, Eurofound, accessed 2nd September 2024, https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age

“

The power balance between workers and employers, unions and corporations, reflects the power the public has in a society – the right balance is essential in a healthy democracy.

”

We found that the forms workplace surveillance can take vary widely, and are impacting workers in many different industries, such as:

- Construction workers, forced to use biometric sign-ins and GPS tracking apps while on site
- National Express coach drivers subject to AI-powered "fatigue monitoring" while they're at the wheel
- Office workers' attendance monitored using Wi-Fi connection records
- Supermarket workers' 'pick rates' and performance assessed by handheld computers
- Spyware from the company Teramind's recording every click and keystroke of office workers, often on work from home devices in sectors including insurance and recruitment.

Other forms of monitoring may appear at first to be less invasive, such as the data collection underpinning Microsoft Teams, but many still have the potential to cause harm with the 'shallow' level of surveillance allowing it to be used more widely.

The weak justifications for some forms of intrusive workplace surveillance are best illustrated by the victories unions have had in resisting them. The Communications Workers Union secured a major win in stopping BT introducing driver-facing cameras earlier in 2024, while the Independent Workers of Great Britain pressured Addison Lee to make sure that their in-cab cameras were only operational when drivers were working and not driving on personal trips.[9][10]

Victories for workers' data rights show that there is plenty of scope in this area to hold employers to account and push back against intrusive and inappropriate workplace surveillance, and demonstrates that constant monitoring is not inevitable. All workers, whether unionised or not, must be empowered to challenge excessive monitoring practices.

Throughout this report, Big Brother Watch draws on workers' experiences, trade union views and analysis of the surveillance products on the market in the UK to illustrate a broad cross-section of employer surveillance in the digital age. From this, we make a number of recommendations about what policy and legislative changes should be made to defend workers' rights going forward.

Power imbalances in the workplace leave workers particularly vulnerable to having their data rights infringed upon. In this report, the word 'worker' is used to refer

9 Union Achieves 'No Inward-Facing Cameras' Pledge From Openreach, CWU Southeast Central, 1st March 2024, https://cwusec.org.uk/union-achieves-no-inward-facingcameras-pledge-from-openreach/

10 IWGB Private Hire Drivers, Twitter, 23rd July 2024, https://x.com/UPHD_IWGB/status/1815737205219791115

to anyone exchanging labour for money, regardless of whether they are employed, freelancers/contractors or technically self-employed. These recommendations outline how we can push back, and ensure that everyone is empowered to protect their privacy and dignity at work.

RECOMMENDATIONS

In this report, we make policy recommendations that seek to address the current gaps in workers' rights protections and data protection that leave them at risk of excessive surveillance in the workplace.

1. **Although employers deploying biometric technologies, systematic monitoring, automated decisions and other high risk data processing in the workplace must produce Data Protection Impact Assessments, there is no current requirement for them to publish them. There should be a legal obligation for organisations to make DPIAs available to workers and unions upon request, enabling increased awareness and scrutiny from employees and unions.**

2. **The ICO should open a biometric data processing register which all companies processing employees' biometric data must register with.**

3. **Create a legal requirement for employers to perform algorithmic impact assessments prior to any implementation of AI or algorithmic-based technologies that are likely to be high-risk to workers' rights and freedoms. The assessment should be provided to workers or their representatives upon request. The legal requirement should be accompanied by a framework issued by the Secretary of State for organisations conducting an AIA to follow, including a requirement for mandatory bias testing to proactively ensure any such system is compliant with the Equality Act 2010, even if the system is procured from a third party.**

4. **Amend Article 22 of the UK GDPR to clarify that human involvement in a decision involving automation must be meaningful, if the decision is not to be considered 'solely automated'.**

5. **Restrict the use of surveillance for behaviour-shaping by preventing the use of location, audio, and video data in enforcing arbitrary performance metrics.**

6. **Prohibit the use of intrusive location data in disciplinary proceedings unless there is suspicion of gross misconduct.**

7. **Create a legal requirement to consult staff, their representatives, and trade unions on the introduction of new high-risk or other potentially intrusive AI monitoring and automated decision-making technologies in the workplace.**

8. **The ICO should issue further examples of what constitutes a 'legitimate interest' in the workplace surveillance context.**

9. **The ICO should issue further examples of necessity and proportionality tests applied in the workplace surveillance context.**

10. **The Government should issue guidance that clarifies the Equality Act responsibilities of organisations using AI and automated decision-making systems, including guidance on the lawfulness of bias mitigation and testing techniques.**

11. **The ICO should issue further workplace-specific guidance of what constitutes a 'similarly significant effect' in relation to Article 22 rights.**

12. **Parliament should prohibit the use of emotion recognition technology.**

BIOMETRICS IN THE WORKPLACE

Biometrics are slowly creeping into more and more workers' day-to-day routines. Fingerprints and face scans are now unfortunately common as a means of access to buildings, as well as being in frequent use to check-in on workers during the working day.[11]

Simply defined, "biometric recognition" is the automated recognition of a person based on their behavioural or biological characteristics. This might be a fingerprint, a vein pattern or even more novel tools such as behavioural biometrics, which identify people from their unique ways of acting - such as how they type.[12] In the context of employment the use of biometrics tends to centre on more mature technologies, such as fingerprints.

As biometrics are primarily used as a tool to identify people, the most common way biometric technology is used in the workplace is to grant access to buildings, rooms and devices in contexts including the military, construction, hospitals, retail and transportation.[13] This has quickly escalated from biometric data being taken for sign-in systems to register staff attendance and other purposes, such as tracking the whereabouts of staff.[14][15]Further, claimed advances in the tech mean that there is a growing trend for biometric tools not just to identify someone, but analyse their behaviour too.

Biometric data is personal data relating to the physical, physiological or behavioural characteristics of a person, which allow or confirm their unique identification, as defined by Article 4 of the UK GDPR. It is a form of "special category data", as outlined in Article 9(1) of the UK GDPR.[16] Special category data is a type of personal data that is afforded additional protection in data law, because collecting and using it has a higher risk of undermining people's rights or resulting in discrimination. Other examples include information on a person's race, trade union membership

11 Managed By Bots, Worker Info Exchange, December 2021, https://www.workerinfoexchange.org/wie-report-managed-by-bots

12 Biometric Recognition, Information Commissioner's Office, accessed 21st June 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition

13 Electronic Monitoring And Surveillance In The Workplace, Kirstie Ball, 2021, https://publications.jrc.ec.europa.eu/repository/handle/JRC125716 23.

14 I'll Be Watching You: A Report On Workplace Monitoring, Trades Union Congress, 2018, https://www.tuc.org.uk/sites/default/files/surveillancereport.pdf 8; Monitoring and surveillance workplace policies, UNISON, 2020, https://www.unison.org.uk/content/uploads/2020/07/Monitoring-and-surveillance-at-work-1.pdf 29-30;

15 The Connected Workplace: Characteristics And Social Consequences Of Work Surveillance In The Age Of Datafication, Sensorization, And Artificial Intelligence, Tobias Mettler, September 2023, https://journals.sagepub.com/doi/full/10.1177/02683962231202535 5.

16 What Is Special Category Data, Information Commissioner's Office, accessed 21st June 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data

or genetic data. Article 9 prohibits the processing of special category data unless certain conditions apply.

Not all of the conditions are relevant to the context of workplace surveillance. However, those that are include[17]:

- Explicit Consent – this must be freely given, specific to the data processing, clear and revocable.
    - The choice must be real and power relationships should be taken into account
- Employment social security and social protection law – the processing must be necessary for an organisation to meet its obligations and exercise its rights
    - Examples include ensuring health, safety and welfare of staff, or deducting trade union subs from payroll (if the data relates to union membership)
- Substantial public interest – processing of biometric data must be necessary for a reason of substantial public interest that has a basis in law
    - Substantial public interest has 23 sub-conditions, one of which must apply. The most relevant in this context are protecting the public, preventing or detecting unlawful acts, regulatory requirements and protection from fraud.

It is important for employees to know the legal justification relied on by bosses to subject them to biometric data processing. For example, if workers are compelled to use a fingerprint door access system, with no alternative offered, consent could not be the lawful basis – as there is effectively no free choice in that circumstance. The ICO cites an example of a gym compelling customers to use biometrics to access the building, with no alternative means of access, as a case of consent being invalid, underlining that the choice must be free.[18] No choice may be offered in very limited circumstances, but the company would then have to rely on one of the other relevant conditions and for this to be lawful the bar to be cleared can be high.

17 What Are The Conditions For Processing, Information Commissioner's Office, accessed 21st June 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/#conditions2

18 Ibid.

Biometrics as Physical Access

Fingerprint or facial scanners are now a common security feature on doors and gates in workplaces across the country. Several workers who responded to our call-out to get in touch about surveillance at work mentioned that their employers had installed fingerprint, or even facial recognition, scanners to grant their staff access. Businesses as diverse as large kitchen retailers, construction sites, window fitters and food manufacturers all use biometric scans to grant their staff access to their premises, or certain areas according to workers who we spoke to.

Generally, biometric access systems replace keycard, fob or pin-based systems which require no special category data to be processed, and often little personal data dependent on the wider system in use. Companies claim that biometrics offer benefits over physical access devices because they are more accurate, and cannot be lost or copied – and if used for clocking in systems, cannot be falsified[19]. However, as outlined in the Serco case study later in this chapter, the Information Commissioner takes a dim view of this argument when companies attempt to argue that those benefits tally up to meeting the threshold for an Article 9 condition.[20]

19 Serco Leisure Operating Limited Enforcement Notice, Information Commissioner, 23rd February 2024, https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts

20 Serco Leisure Operating Limited Enforcement Notice, Information Commissioner, 23rd February 2024, https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts

The ICO also expects that alternative options are offered to workers who seek to opt out of biometric systems, except in very rare cases when an Article 9 condition other than explicit consent can be demonstrated to apply. This effectively means that in the vast majority of cases an alternative such as a RFID keycard should be offered.

The use of biometrics carries an inherent privacy risk – as recognised implicitly by the placing of biometric data in the special category of personal information. It can lead to companies processing and/or holding significant quantities of sensitive data. Biometric data necessarily exists to identify individuals, and poor security may allow malign actors to steal identity data in the event of a data breach, or reverse engineer the biometric identifier, potentially granting them access to other systems secured using the same biometric.

Certain forms of biometrics also come with significant risks of bias against certain groups, such as ethnic minorities, which has repeatedly been shown to misidentify people from ethnic minority backgrounds and women at a higher rate than white people and men.[21] In the context of the workplace this may mean that individuals suffer discrimination by struggling to access buildings using facial recognition entry systems. These systems should not be deployed lightly, or out of convenience, and there remain questions in all but the rarest of circumstances if biometric access requirements can be justified at all.

Biometrics in the Construction Industry

Construction sites were repeatedly flagged to Big Brother Watch as an employment setting where biometrics are increasingly being used on entrances to authorise access and verify workers' identities. Suppliers of biometric access systems for building sites tout administrative and safety benefits as reasons to install fingerprint scanners.[22]

A promotional case study from Ace Tech, a security firm which provided access gates to a building project in Battersea, south London, claimed that "as well as controlling access to site [fingerprint recognition] would provide time and attendance records for contractors and personnel".[23] In addition to controlling access, it appears that biometric turnstiles are used to automatically track who is on site when – and these records can be integrated into other systems, such as

21 Facial Recognition Fails On Race, Government Study Says, BBC News, 20th December 2019, https://www.bbc.co.uk/news/technology-50865437
22 Vinci Battersea Place Case Study, Ace Tech Security, accessed 25th June 2024, https://acetechsecurity.co.uk/case-studies/access-control,cctv/vinci-battersea-place/
23 Ibid

payroll.[24] Facial recognition turnstiles are offered by Ace Tech in combination with other potentially intrusive monitoring, such as temperature checks or face mask verification, underlining a ratcheting effect where one surveillance tool can lead to others being introduced.[25]

One construction worker Big Brother Watch spoke to said that alternatives to biometrics, such as a RFID keycard, were generally offered to them - but on some sites another worker said that the biometrics were mandatory. However, a repeated theme was that workers on these sites were given little to no information about privacy policies relating to fingerprint or facial recognition access. Data rights surrounding biometric data were not explained, and policies around the retention, processing and deletion were not offered to workers enrolling onto the systems. The lack of understanding on behalf of companies was shockingly underlined by

24 Vinci Battersea Place Case Study, Ace Tech Security, accessed 25th June 2024, https://acetechsecurity.co.uk/case-studies/access-control,cctv/vinci-battersea-place/

25 Construction Security Turnstiles, Envision, accessed 25th June 2024, https://envision-is.co.uk/construction-security-turnstiles

one electrician who told us that the company contracting him said that it owned the rights to his fingerprints and could even sell them on. Although it is unlikely that data sales actually occurred, as it would be a flagrant breach of GDPR, it suggests that data rights are not always a priority and a lack of understanding could easily result in breach of those rights.

The case study of the construction industry raises unique questions as it is also a common requirement for construction workers to hold a CSCS (Construction Skills Certification Scheme) card to access building sites.[26] These cards are smartcards which can integrate with access systems sold to construction companies by third parties.[27] Even in the case of a construction company relying on non-consent based conditions under Article 9 to justify biometric access, the existence of a widely used certification card to verify qualified personnel raises questions about whether biometrics would be "necessary" vis-a-vis Article 9.

Power Imbalances & Consent In Cleaner Case Study

European data regulators applying GDPR have found that power imbalances should be taken into account when considering if consent is genuinely free and fair, as the ability of someone to refuse in reality, as well as on paper, should be accounted for when relying on consent as a grounds for processing biometric data.[28]

In 2020 Big Brother Watch supported 'John'[29] in his fight against compulsory facial recognition to clock in for his job as a cleaner at a school, which was introduced when an outsourcing company took on the cleaning contract.[30] John was told that as part of his new contract, he had to consent to clocking in via facial recognition on an app on his own phone, or he would not get paid. John did not own or want a personal phone with facial recognition enabled. He described the new requirements as "controlling and dehumanising", and he and his colleagues were also worried about losing pay for their work due to errors, poor signal, or technical issues with the new app. John and his colleagues refused to sign the contract and he contacted Big Brother Watch.

Big Brother Watch wrote to the new cleaning company and the school asking them

26 About, CSCS, accessed 25th June 2024, https://www.cscs.uk.com/about
27 Construction Site Access Control, Millenium Security Services, accessed 25th June 2024, https://www.millenniumsecurity.co.uk/service/construction-site-access-control-systems-biometric-access-control
28 Facial Recognition: School ID Checks Lead To GDPR Fine, BBC News, 27th August 2019. https://www.bbc.co.uk/news/technology-49489154
29 A pseudonym
30 Workers Fighting Compulsory Facial Recognition With Big Brother Watch – And Winning, Big Brother Watch, 22nd December 2020, https://bigbrotherwatch.org.uk/blog/workers-fighting-compulsory-facial-recognition-with-big-brother-watch-and-winning

to scrap the compulsory facial recognition, reminding them of their data protection obligations and the requirements for consent to be free, which had not been met. Shortly after, John's manager admitted his employers "crossed a line" and facial recognition clocking in was no longer required.

John's situation is a clear example of where the lawful basis of consent did not apply, as seeking consent via an ultimatum in a contract is not freely given or withdrawable without penalisation – the employers demanded that workers sign the contract in order to keep their jobs. However, the case study also demonstrates how a robust defence of existing biometric data rights can lead to a positive outcome.

Serco Gyms & ICO Intervention

In February 2024, the Information Commissioner issued a landmark ruling, ordering leisure centres run by outsourcing giant Serco and several associated community leisure trusts to stop using facial recognition and fingerprint scans for staff access and to check staff attendance.[31] 2,000 employees across 38 leisure centres were impacted by the biometric access policy – with 7 million biometric scans taking place.

31 Serco Leisure Operating Limited Enforcement Notice, Information Commissioner, 23rd February 2024, https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts

Serco claimed: "Biometrics is the sole technology capable of eliminating buddy punching and falsified time cards" and that biometric solutions are "more accurate and secure than cards or keys, because a fingerprint or face scan cannot be lost, stolen or (easily) replicated."[32] It relied on the employment condition under Article 9 of the GDPR to justify its use of special category data, and belatedly claimed that alternatives were offered although its initial assessment found that opt outs would be "unsuitable".

In reality, the ICO found that if staff objected they were offered a discussion about privacy, but told they would have to continue using the system – and it was implied that biometrics were necessary to ensure staff would get paid.[33]

The ICO's enforcement notice stated that Serco had failed to show that the processing of biometric data was necessary to meet its employment law obligations – and outlined how RFID smartcards, fobs and manual sign in sheets would all be reasonable alternatives to biometrics. Due to this the ICO found that the Article 6 basis (justification for processing personal data) of Serco's legitimate interests did not apply, as less intrusive means of data processing could meet the same interests.[34]

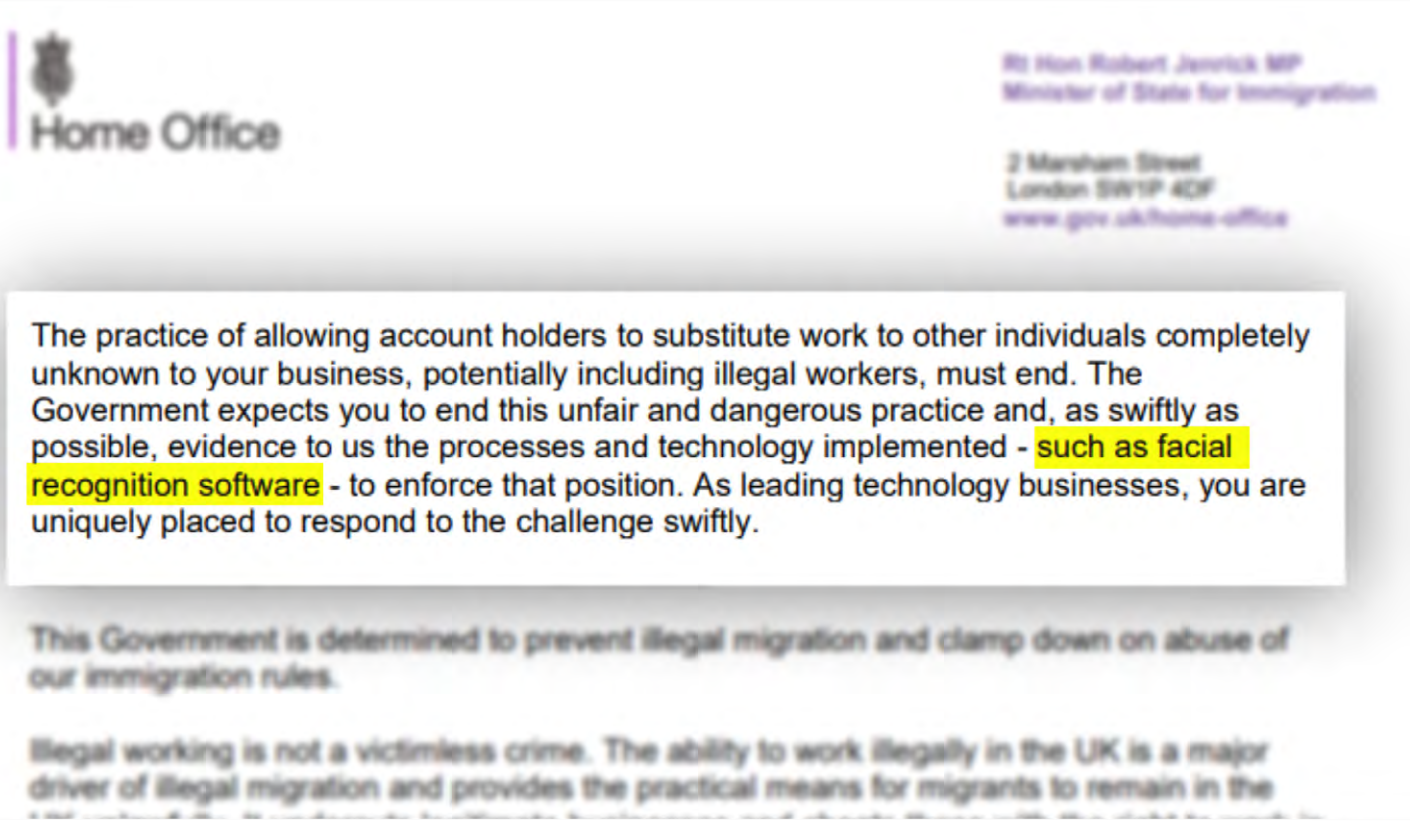
By taking action, the ICO set down a marker for the use of biometrics at work, putting regulatory weight behind the principle demonstrated in John's case study from 2020 that coerced "consent" to use biometrics is not lawful and that employee privacy and a genuine ability to freely choose are key considerations for organisations introducing the technology.

Gig Economy, Facial Recognition, Self Employment & the Home Office

App-based working platforms are increasingly common, and for the most part this report does not cover the surveillance of workers in this sector due to the prior publication of excellent work by organisations including the Workers Info Exchange.[35,36] Pre-existing research already offers significant insights into the algorithmic monitoring and supervision of platform workers, the use of facial recognition and GPS location check-ins.

32 Serco Leisure Operating Limited Enforcement Notice, Information Commissioner, 23rd February 2024, https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts
33 Ibid
34 Ibid
35 Managed By Bots, Worker Info Exchange, December 2021, https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_8d720d54443543e2a928267d354acd90.pdf
36 Hired, Six Months Undercover In Low Wage Britain, James Bloodworth; Atlantic Books, 2018

More recently there is an aspect of platform worker surveillance that has seen less attention stemming from media coverage of the growing second-hand market in accounts for platforms such as UberEats and Deliveroo: the Home Office's push to put the platforms in the role of border guard.[37] As nominally self-employed people, platform workers have the right to send a substitute to do the work in their place – and this has led to a growing grey market in courier app accounts for rental in addition to the formal in-platform substitution processes[38]. Signed-up account holders rent these out to other people for a fee, often outside the platforms' official channels to do this - which does break platform rules but is a commonplace practice.[39] On some occasions the renters are not subject to right-to-work checks and do not hold documents authorising them to work lawfully in the UK.



Home Office

The practice of allowing account holders to substitute work to other individuals completely unknown to your business, potentially including illegal workers, must end. The Government expects you to end this unfair and dangerous practice and, as swiftly as possible, evidence to us the processes and technology implemented - such as facial recognition software - to enforce that position. As leading technology businesses, you are uniquely placed to respond to the challenge swiftly.

Renting courier platform accounts has become a route for some undocumented

37 Takeaway Conmen Rent Their Identity To Your Driver – Then Steal Their Earnings, The Sunday Times, 3rd June 2023, https://www.thetimes.com/article/jobs-for-rent-the-black-market-behind-your-takeaway-2gdrh9wlf

38 Government and Delivery Platforms Join Hands To Throw Delivery Workers Under The Bus, Worker Info Exchange, 20th May 2024, https://www.workerinfoexchange.org/post/government-and-delivery-platforms-join-hands-to-throw-migrant-workers-under-the-bus

39 Identity Verification Checks, Uber, accessed 23rd August 2023, https://help.uber.com/driving-and-delivering/article/identity-verification-checks?nodeId=aa821486-c8d1-42b7-b784-2fc24eb85f93

people to find work,[40] which opens them up to other kinds of exploitation, but has also brought the platforms to the attention of the UK immigration authorities. There have also been some safety concerns raised about grey-market account renting, particularly by women's groups, as it would allow people to deliver to homes having not undertaken or failed criminal records checks, and without being traceable.[41]

Unions representing platform workers told Big Brother Watch that facial recognition use by the platforms has ramped up significantly after the phenomenon of account renting garnered significant public attention. Couriers at UberEats and Deliveroo get random requests to re-verify themselves throughout the time they are working. This is designed to continually verify and check in on the worker as they work, and is suggestive of a zero-trust environment between the platforms and those who work for them.

The Home Office has met with the major food delivery platforms to discuss "tackling illegal working".[42] While facial recognition was not mentioned in the minutes from the meeting they did state that ministers and platforms agreed that "the use of technology to enhance processes" to verify workers was a likely way forward. A letter from then-Immigration Minister Robert Jenrick to the platforms in November 2023, preceding the meeting, explicitly suggested facial recognition technology as a solution that could be used.[43]

Representatives of platform workers told Big Brother Watch that they believed that immigration concerns were behind the rollout of more frequent facial recognition checks, as a technological solution to Home Office pressure to crack down on undocumented people working illegally. Platform workers are some of the most precarious in society, and the Home Office minutes acknowledge the risk that constant re-verification poses to self-employed status as a result of the limitations this places on the ability of a self-employed person to freely substitute.[44]

Constant biometric reverification is an example of intrusive identity checking, which is exacerbated by the growing role of platforms as ersatz immigration officers. It is not just jobs that could be lost, but vulnerable and precarious workers could be put into serious hardship in the short term.

Worker Info Exchange (WIX) reported in June 2024 that repeated errors in identity

40 Inside The Thriving Black Market For Illicit Deliveroo, Uber Eats & Just Eat Drivers, I News, 15th March 2024, https://inews.co.uk/news/delivery-riders-account-sharing-facebook-black-market-2957089
41 Inside The Thriving Black Market For Illicit Deliveroo, Uber Eats & Just Eat Drivers, I News, 15th March 2024, https://inews.co.uk/news/delivery-riders-account-sharing-facebook-black-market-2957089
42 Round Table Event Minutes, FOI2024/00400, Home Office, 8th February 2024
43 Letter From Robert Jenrick To Online Delivery Platforms, Home Office, 14th November 2023, https://assets.publishing.service.gov.uk/media/655389d43718980013d296b8/Minister_public_letter_to_online_delivery_platforms-_FINAL_PDF.pdf
44 Round Table Event Minutes, FOI2024/00400, Home Office, 8th February 2024

checks led to one UberEats rider being wrongly suspended from the platform twice in four months.[45] After the first suspension it supported the rider to challenge the suspension and the platform recognised that an error was made, and that his documents were correct. Months later another check saw him suspended again - before WIX intervened again to get it lifted. The checks appeared to be on the worker's documents, with a face scan to verify, regardless of the route of identity checks, error can lead to suspension and automated systems are liable to repeat similar errors, and as with this example it could lead to workers being repeatedly suspended wrongfully for failing verification checks.

Meanwhile the long term increasing digital identity checks by bosses in the name of border security could see further pressures from the Home Office for similar checks to roll out into other industries.

POLICY ANALYSIS

Employers must not rush into deploying such intrusive technologies as, in the words of the Information Commissioner, "biometric technologies cannot be deployed lightly".[46] In the exceptional circumstances where these technologies are used in the workplace, the systems must be able to support the work conditions, outcomes, safety, and well-being of workers, and designed, used, and governed to respect their rights.[47] As biometric information qualifies as special category data, processing it requires higher levels of protection and increased diligence. The case studies above show how this is even more the case in the workplace, where biometric surveillance is often neither necessary nor proportionate and it is difficult for consent to be either fully informed or freely given.

Necessity & Proportionality

Given the increased risk to people's privacy rights that biometric technologies pose, employers should never deploy them without very good reason. There may be circumstances in which biometric methods could be legitimate in the workplace, such as on the grounds of security where employees are accessing highly dangerous materials in a laboratory or military facility and there is no less

45 Absurd AI-Powered Worker Surveillance: The Latest From Our London Casework, Workers Info Exchange, 7th June 2024, https://www.workerinfoexchange.org/post/absurd-ai-powered-worker-surveillance-in-london

46 ICO Orders Serco Leisure To Stop Using Facial Recognition Technology To Monitor Attendance Of Leisure Centre Employees, Information Commissioner's Office, 23rd February 2024: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/

47 A Policy Primer And Roadmap On AI Worker Surveillance & Productivity Scoring Tools, Merve Hickok & Nestor Masley, 20th March 2023, https://link.springer.com/article/10.1007/s43681-023-00275-8684.

intrusive alternative.[48] However, these cases will always be the exception to the rule.

Biometric technology should never be introduced in the workplace to surveil or monitor staff or because employers consider it to be a useful, convenient, or effective method, unless it is introduced as an option individuals can freely consent to. For instance, it would not be appropriate for a company to introduce a mandatory fingerprint scanner to prevent employees from losing or breaking their swipe cards, nor is it acceptable for an organisation to use biometrics to automate shift clock-ins. There are a wealth of existing methods employers can use to monitor employee attendance including timesheets, signing in with a PIN code, a swipe card, an app, etc. There are some instances where use of the technology may never be acceptable, such as so-called 'emotion recognition' technology, as the encroachment on worker privacy is far too severe to outweigh any purported 'benefit'.

Consent

The UK GDPR requires that if using a biometric recognition system, the processor must identify a lawful basis and a separate condition for processing special category biometric data.[49] ICO guidance also identifies explicit consent as the most appropriate condition in the majority of circumstances.[50] If using consent as the basis for appropriate lawful processing, the UK GDPR requires that employees must provide full, informed, and freely given consent for the collection to be lawful.[51]

While this might seem simple enough at first glance, consent is a complex issue in the workplace. Power imbalances means that workers may not genuinely have an option to withhold consent without fear of repercussions. Consent can also be obfuscated by other factors, including a lack of transparency surrounding technology deployments and workers not being given a proper explanation regarding the systems in place and their related data rights. Despite the constraints of achieving free and informed consent in the workplace, it is nevertheless important for employers to support employees in understanding what their rights are and how to exercise them.

48 Monitoring And Surveillance Workplace Policies, UNISON, July 2020, https://www.unison.org.uk/content/uploads/2020/07/Monitoring-and-surveillance-at-work-1.pdf 30.
49 How Do We Process Biometric Data Lawfully?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/#canweuse
50 Ibid
51 Ibid

Alternatives

Consent is not legitimate if a person has no real choice.[52] An alternative must always be provided for those who wish to opt out of biometric data use, and employees must never be pressured into biometric checks for fear of the threat of disciplinary action or dismissal, being passed over for promotion, or other negative consequences. Employers have plenty of options available – for example, a swipe card and PIN could be used in combination for an extra level of security when biometrics are used for access; although, as noted in the section above, this raises questions as to the necessity of biometric checks in the first place.

Examples from abroad demonstrate the extent to which the consent process can go wrong. A particularly chilling example is when Amazon delivery drivers in the U.S. were presented with a 'biometric consent' form that granted Amazon permission to monitor drivers' location, movement, and biometric information, including facial recognition.[53] Drivers who did not sign the forms were told they would lose their jobs, and many who signed suffered the stressful impact of being subject to intrusive biometric monitoring by their employer.[54] Such practices raise significant privacy and ethical concerns and jeopardise trust between employers and employees. Although this took place in the U.S. where there are different biometrics and data protection laws, it illustrates how international companies have overstepped in other contexts and serves as a warning of the extent to which some employers are willing to go.

Detriment

Excessive and compulsory checks undermine worker autonomy and dignity, such as when platform workers in the gig economy have to register themselves through facial recognition scans and constantly reverify their identities throughout a shift. For people who need the income, platforms ask them to choose between their ability to earn a wage versus their sensitive biometric data being collected. Most people will not have the luxury of prioritising the latter. Taking a picture of your face and uploading it multiple times a day could cause anxiety, feel demeaning and make workers feel constantly surveilled. Making all platform workers participate in these kinds of checks is incredibly intrusive, subjecting many dimensions of their

52 Data Protection And Monitoring Workers, Information Commissioner's Office, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf 6-7.

53 Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job, Vice News, 23rd March 2021, https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job

54 Amazon's AI Cameras Are Punishing Drivers for Mistakes They Didn't Make, Vice News, 20th September 2021, https://www.vice.com/en/article/88npjv/amazons-ai-cameras-are-punishing-drivers-for-mistakes-they-didnt-make

lives to control and oversight simply for working in the gig economy.

Bias

Surveillance technology is a risk to everyone, but the often low levels of accuracy of some forms of biometric surveillance disproportionately impact marginalised or vulnerable people. For example, research indicates that many of the algorithms underpinning facial recognition technology disproportionately misidentify[55] black[56] and minority[57] ethnic[58] groups, making its increasingly prevalent use in workplaces particularly alarming.

This is exemplified in the gig economy where jobs are held disproportionately by people of colour,[59] often migrant workers.[60] This effectively subjects people who are often marginalised or vulnerable to increased scrutiny from private companies with a higher chance it will go wrong. In March 2024, a gig economy worker received a payout from Uber Eats after racially discriminatory facial recognition checks prevented him from accessing the app to secure work.[61] This emphasises the real harm using such technologies in the workplace can cause, underscoring the need for biometrics to only be used cautiously, in a non-discriminatory way, and lawfully, which is likely to be only in exceptional circumstances. There are many other ways for platform workers to prove their identity – the app could prompt riders to provide a randomly generated code, answer security questions, or issue a unique QR code or barcode to scan at the beginning and end of shifts.

Although biometrics should never be the first port of call, more safeguards are needed for when employers can justify their use. To address the issues caused by hidden biases and prejudices within algorithmic systems, a legal obligation could be placed upon companies to perform bias testing before using a system.

55 Managed By Bots, Worker Info Exchange, December 2021, https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_8d720d54443543e2a928267d354acd90.pdf;

56 Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Joy Buolamwini and Timnit Gebru, Proceedings of Machine Learning Research, 2018, 81:1-15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf ;

57 Federal Study Confirms Racial Bias Of Many Facial-Recognition Systems, Casts Doubt On Their Expanding Use, Drew Harwell, Washington Post, 19th December 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

58 Racism and AI: Here's How It's Been Criticized for Amplifying Bias, Forbes, 25th May 2023, https://www.forbes.com/sites/ariannajohnson/2023/05/25/racism-and-ai-heres-how-its-been-criticized-for-amplifying-bias/

59 Race And The Platform Economy, London School of Economics, 9th November 2021, https://www.lse.ac.uk/research/research-for-the-world/race-equity/race-and-the-platform-economy

60 Racism And Food Delivery Platforms: Shaping Migrants' Work Experiences And Future Expectations In The United Kingdom And Chile, Macarena Bonhomme and James Muldoon, 20th May 2024, htttps://www.tandfonline.com/doi/full/10.1080/01419870.2024.2349268.

61 Payout For Uber Eats Driver Over Face Scan Bias Case, BBC News, 26th March 2024, https://www.bbc.co.uk/news/technology-68655429

This would obligate employers to proactively prove that technologies used in the workplace are not biased, rather than burdening employees with the difficult task of proving that they are. This recommendation will be explored in further depth in the chapter on AI in hiring.

Transparency & Explainability

There are clear problems around the ability of workers to provide meaningful consent to the use of biometrics within the workplace, as highlighted through John's case study and others where workers are often given little to no information relating to privacy policies or data rights.

The conditions of consent are satisfied in part by the extent to which a person understands what they are agreeing to. Even when workers are given privacy policies for biometric checks, many may not understand the full complexity of the data collected, the inferences made about them, or the extent of potential harm.[62] This is because privacy policies are often impenetrable documents designed with the legal protection of the data controller in mind rather than the benefit of the data subjects, which can make it very difficult for people to understand the reality of how their personal and sensitive data could be used.[63] The content of a privacy policy is largely decided by the company and is often incredibly vague – for example, the phrase "improve products and services" can refer to very broad data use, such as data being used in training AI or machine learning.[64] This is even more concerning within the context of biometric data as it is unique to individuals and cannot be reset or restored. Similarly, privacy policies can be updated. While consent must be re-obtained for new data processing purposes[65], it is very possible for these new uses to be buried deep within the depths of privacy policy texts - which the majority of people do not actually read.[66] This leads to the conclusion that 'consent' requirements and privacy notices provide inadequate protection against the expansion of intrusive workplace surveillance and further protections are needed.

For any process that is likely to result in a high risk to people's rights and freedoms, UK GDPR requires that a data protection impact assessment (DPIA) must be

62 A Policy Primer And Roadmap on AI Worker Surveillance And Productivity Scoring Tools, Merve Hickok & Nestor Masley, 20th March 2023, https://link.springer.com/article/10.1007/s43681-023-00275-8
63 We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, The New York Times, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html
64 Here's What You're Actually Agreeing To When You Accept a Privacy Policy, The New York Times, 14th April 2023, https://www.nytimes.com/wirecutter/blog/what-are-privacy-policies/
65 Should We Test, Review And Update Our Privacy Information?, Information Commisioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/should-we-test-review-and-update-our-privacy-information/
66 I Tried To Read All My App Privacy Policies. It Was 1 Million Words, The Washington Post, 31 May 2022, https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/

performed.[67] DPIAs help employers to identify, analyse and minimise the data protection risks of a project by requiring a description of processing operations and purposes, an assessment of the risks to the rights and freedoms of individuals, the measures envisaged to address those risks, and the safeguards, security measures and mechanisms in place to ensure the personal data is protected.[68] This can help individuals impacted by the processing to understand the nature and purpose of the processing. However, the effectiveness of a DPIA depends significantly on workers' or their representatives' involvement and proper consideration of their views.[69]

Moreover, publishing a DPIA is not currently a requirement of UK data protection law, although the ICO recommends doing so where possible.[70] Organisations may choose to make them available on a generic basis, or in the instance of an individual request, but companies can refuse such requests by claiming that the information is commercially sensitive. Having access to a DPIA can empower employees to see how their data will be used and why and hold data processors to account. In the instance of processing special category information such as biometrics data, there should be a legal obligation for organisations to make DPIAs available to workers and unions upon request.

Enforcement

While some of these issues are covered by existing legal requirements or ICO guidance, a gap remains between theory and practice. As the case studies demonstrate, many workers continue to have systems imposed on them despite a lack of meaningful consent, proper alternatives, or accessible information, prompting the need for more stringent worker protections.

Many of the case studies demonstrate a lack of enforcement of existing safeguards, suggesting a systemic issue where organisations routinely sidestep legal requirements without consequence.

To address this, there needs to be increased accountability for organisations

67 When Do We Need To Do A DPIA?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

68 Data Protection impact assessments, Information Commissioner's Office, https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-impact-assessments/

69 Bargaining Over Workers' Data Rights: How Unions and Works Councils Can Use Collective Bargaining to Specify Workplace Data Protection Norms, Friedrich Ebert Stiftung, June 2024, https://library.fes.de/pdf-files/bueros/bruessel/21313.pdf 6.

70 Data Protection Impact Assessments, Information Commissioner's Office, https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-impact-assessments/

processing biometric data. Currently, companies processing personal data must register with the ICO. However, there is no requirement for them to record that they are processing biometric data specifically, despite it being a uniquely sensitive type of data. This means that the ICO has oversight of who is processing data in general, but not over who is processing some of the most sensitive types of personal information.

Processing high-risk data should incur increased accountability. The ICO should open a register for processors of biometrics data which all individuals or organisations processing biometric data should be required to join. A dedicated biometrics processing register would enhance the ICO's ability to oversee and monitor companies handling sensitive biometric data more effectively than the current general data processing register allows for as, unlike the existing register that covers all forms of data processing, a biometric data processors' register would list which organisations are engaging specifically in this kind of sensitive and high-risk processing. This would better position the ICO in understanding the scope and scale of biometric data usage and exercising its role as a regulator to ensure compliance with data protection laws unique to biometric data.

Requiring organisations to register as biometric data processors creates a formal record and acknowledgment of their responsibility to comply with data protection law. The case study of construction workers demonstrates how many employers who introduce biometrics in the workplace either do not fully understand their data protection obligations or, if they do, fail to properly fulfil them. A biometrics register would encourage visibility of biometric data processors both to the ICO and the public. Requiring organisations to declare themselves as such could encourage them to both better understand and properly adhere to their responsibilities regarding the collection, use, and storage of biometric data, given the increased visibility that a register would give rise to. This would create a clear record of which organisations are involved in processing biometric information, which would provide the ICO with a clearer overview of biometrics use within the workplace surveillance landscape.

Registering as a biometrics data processor could easily be streamlined into current processes, for example, by the ICO adding a simple checkbox to the existing data processor registration form and requiring further information about biometrics processing, or requiring companies to contact the regulator if already registered. If an individual or organisation stopped processing such data, they would be obligated to promptly notify the ICO, ensuring their swift removal from the register. This would enable the ICO to have a comprehensive and up-to-date register of biometric data processors, enhancing accountability through a simple mechanism.

Many workers are not properly informed of the importance of biometric data or the reasons for and implications of its processing. While the onus should be on employers to get such processing right, it is important that employees know their rights to prepare them for the possibility for it to go wrong. Although there are some tools in place to support transparency, such as DPIAs, these do not necessarily educate employees on their specific rights in the context of data-driven technologies. It is good practice for employers to go beyond the requirements of a DPIA in such a high-risk context, providing employees with clear information regarding their rights and what steps to take if they suspect data misuse. Such information could be delivered in a variety of ways, ranging from informative leaflets to videos, or a talk from an organisation's Data Protection Officer. This provides workers with the power to advocate for themselves, whilst simultaneously supporting employers in creating more trust within the workplace by reducing information asymmetry.

Biometrics & Mission Creep

'Mission creep' is where data is used for objectives beyond that which it was collected for. Data collected by companies is ripe for being put to other uses than what employees might expect.[71] For instance, Uber's privacy notice states that driver and delivery persons' location and demographic data can be used for analysis, machine learning, and training, which is an incredibly broad scope of activities.[72] The lack of transparency and insight employees often have into the surveillance process can make it very difficult for an individual to know if their employer has used their data in an unacceptable way.

As per the Information Commissioner's ruling against Serco, employers must always be able to prove that any personal data processing used is the least intrusive method to achieve the intended aim.[73] According to the principle of purpose limitation enshrined in the UK GDPR, unless there is a compatible purpose, legal requirement, or consent is sought for a new purpose, the data provided must not be repurposed for any reason beyond which it has been collected, and this must be strictly defined and justified.[74] For instance, fingerprint scanners might be permissible for accessing high-security areas of military bases. However, this data

71 Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees, Amy Vatcha, iS Channel, September 2020, https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf 6.

72 Uber's Privacy Principles, Accessed 23rd August 2024, https://www.uber.com/global/en/privacy/overview/?_csid=LGdMllNU-xtKHLpXtJKBbQ&state=UvNd6ZBJu3qXCd6x2xWQddUkcas-EUDozvxV6O2PvBE%3D&effect=

73 Serco Leisure Enforcement Notice, Information Commissioner, 19th February 2024, https://ico.org.uk/media/action-weve-taken/enforcement-notices/4028 590/20240219-serco-leisure-operating-limited-en.pdf

74 Principle (b): Purpose Limitation, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/

must not ordinarily be repurposed beyond the reason it was originally collected, such as using the data collected from fingerprint access for general monitoring of an employee's movements in the workplace.

RECOMMENDATIONS

1. Although employers deploying biometric technologies, systematic monitoring, automated decisions and other high risk data processing in the workplace must produce Data Protection Impact Assessments, there is no current requirement for them to publish them. There should be a legal obligation for organisations to make DPIAs available to workers and unions upon request, enabling increased awareness and scrutiny from employees and unions.

2. The ICO should open a biometric data processing register which all companies processing employees' biometric data must register with.

PRODUCTIVITY TRACKING

Monitoring how workers spend their time is common in some workplaces, with bosses wanting to maintain productivity and ensure staff are focussed on the task at hand. This traditionally involves human intervention, such as supervisors physically observing employees. However, the evolving nature of the workplace, particularly the work from home revolution since the Covid-19 pandemic, and rapid technological advances are leading to increasingly insidious and invasive surveillance practices that raise significant concerns about fundamental privacy rights.

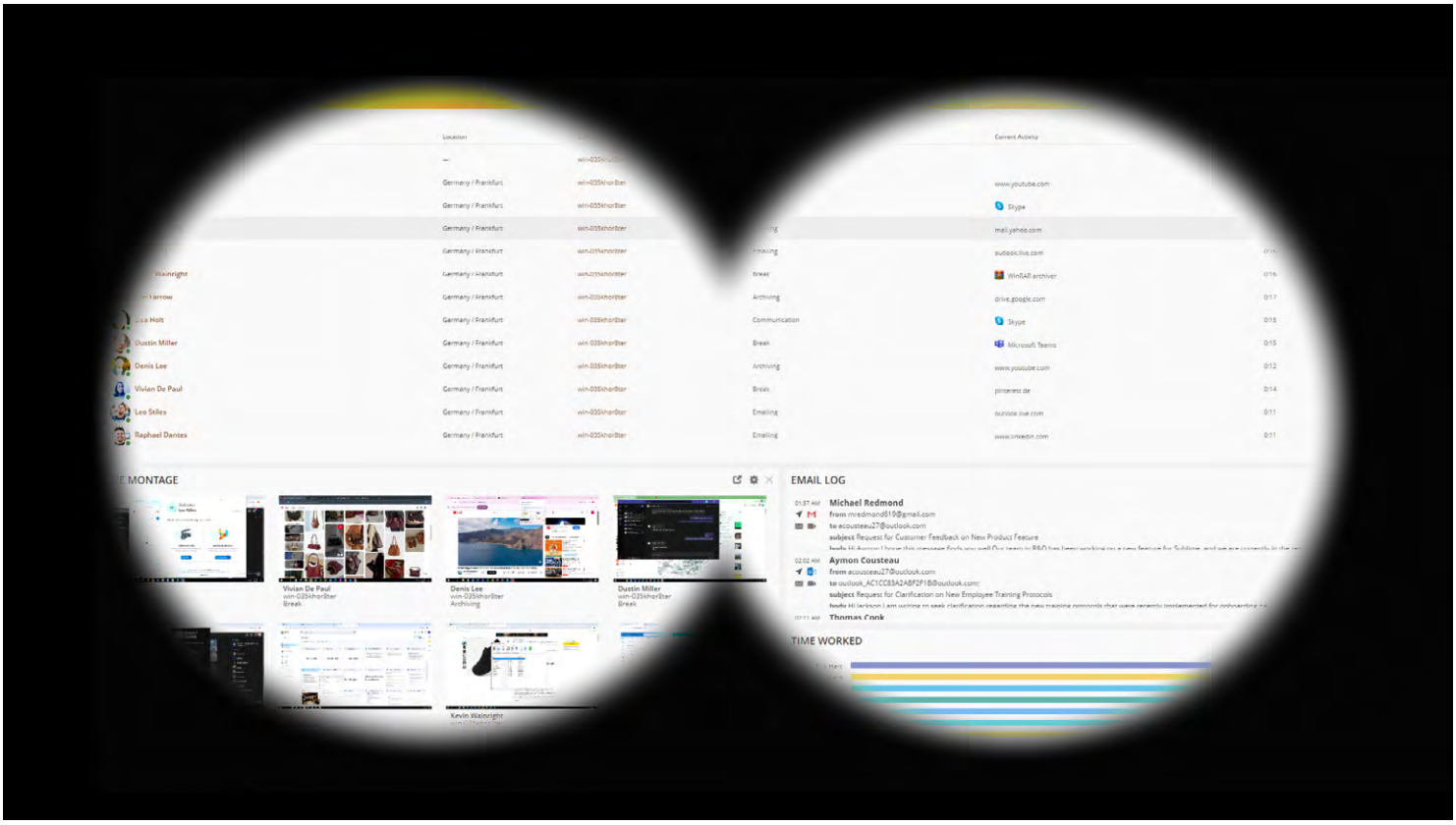
Productivity tracking varies widely across industries. For desk-based workers this could be keyloggers on computers, desk presence sensors or periodic webcam photos, while a warehouse worker could be tracked by software on their work device or a GPS wearable. Many intrusive productivity tracking methods are rooted in bosses' lack of trust and desire to keep an automated eye on their staff as frequently as possible.

Employers often think that detailed data about what workers are doing will be useful for decision-making and ensure that employees remain productive, especially for remote workers. This has coined the term "productivity paranoia", where managers interpret a lack of visible activity or face-to-face contact as a sign that employees are not working hard enough, leading them to mistrust or micromanage their teams.[75] Prompted by this suspicion, many bosses are turning to digital tools to track and measure productivity to the extent that surveillance technology has become "unblinking" and "ever-present" for both on-site and remote workers.[76] The heightened scrutiny on employees vastly increases the amount of data collected on them and can make people feel stressed, anxious, and under 24/7 monitoring; feelings that further erode trust in the workplace.

Surveillance does not have to be extreme to have a negative impact. Even shallower productivity monitoring from commonly used tools can amount to intrusive monitoring when it becomes all encompassing.

75 The 'productivity paranoia' managers can't shake, BBC News, 19th October 2022, https://www.bbc.com/worklife/article/20221014-the-productivity-paranoia-managers-cant-shake

76 Amy Vatcha, Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees, London School of Economics, iS Channel, https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf



Teramind

Some so-called productivity monitoring tools installed on workers' devices are closer to full-on spyware, picking up every click and keystroke. There are a string of hyper-intrusive tools on offer for organisations to monitor their workers - Teramind's software is one of the most infamous for the level of monitoring.[77] The US-based company keeps its client list secret, but corporate intelligence firms claim that UK based insurers CRL Management and Blackfriars Insurance Brokers are customers.[78][79] It is also sold via the UK government's Digital Marketplace, a database of digital services available to the public sector.[80] Broadly its uses are outlined as including:

- User activity monitoring
- Insider threat detection
- Content discovery and classification
- Clipboard monitoring
- Compliance management
- Risk management

77 The Creepy Rise Of Bossware, WIRED, 23rd July 2023, https://www.wired.com/story/creepy-rise-bossware

78 Teramind, Enlyft, accessed 10th July 2024, https://enlyft.com/tech/products/teramind

79 Teramind, 6Sense, accessed 10th July 2024, https://6sense.com/tech/employee-monitoring/teramind-market-share

80 Teramind, UK Digital Marketplace, accessed 10th July 2024, https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/991609227879572

Under the hood, Teramind is capable of tracking almost everything that goes on on the computer it is installed on. Bosses are able to see a live view of their employees' screens, allowing them to virtually watch over workers' shoulders every second that the software is running.[81] This has potentially devastating privacy implications, as it would allow companies to see anything and everything on a workers' screen. Activities such as emailing a trade union representative would be viewable in the live screen-share feed.

The software can also provide a dashboard showing what all workers' are doing at any moment including automated 'break' detection; the programs in use; and in the case of web browsing, the site that an employee is using.[82] The dashboard gives supervisors granular, instant, updates on what each member of staff is doing – an approach which will make it clear to every employee that they could be being watched every moment of the working day.

Teramind goes even further in facilitating intrusive surveillance of employees – its dashboard has a "monitoring" tab where bosses can get detailed records of all the activities workers have performed on their computers, sorted by type. This includes "web pages", "file transfers", "social media", "emailing" and more. In each category there are lists of every action of this type taken, and a search bar that would allow, for example, a boss to search all instant messaging apps for a certain word such as "trade union" or "grievance".[83] There is even an advanced computer vision tool that allows for a search of all screen recordings for certain terms. Effectively every single click, keystroke, file opened or webpage visited by staff is archived and searchable at will.

The data collected can also be used to trigger "behaviour alerts" for violations of pre-set rules – an alert might just be a pop-up on a workers' screen, but could also be as serious as locking a user out of their account.[84] Some of the example rules in Teramind's demo centre on compliance issues, including using unauthorised applications, using private or Tor (anonymised) web browsing, screenshots being taken or sending an email to a non-business address. This is clearly very close surveillance of workers, that could only be potentially justified in rare circumstances when people have access to incredibly sensitive data and there is a high risk that it could be used inappropriately.[85]

81 Liveview Demo, Teramind, accessed 10th July 2024, https://democompany.teramind.co/player#/live/b25zaXRlOzQwOzM7NTk2Mjc=

82 Dashboard Trial, Teramind, accessed 10th July 2024, https://democompany.teramind.co/?_gl=1*1gusr36*_gcl_au*NTk4NTY2NTk4LjE3MjA3OTA0NTg.*_ga*MTA0NTI4ODU2Ny4xNzIwNzkwNDU5*_ga_2JLHVL0KM2*MTcyMDc5MDQ1OC4xLjEuMTcyMDc5MjAzNy42MC4wLjA.#/report/Focus+Dashboard

83 Reports IM Monitoring Trial, Teramind, accessed 10th July 2024, https://democompany.teramind.co/#/reports/im-monitoring

84 Behaviour Data Telemetry, Teramind, accessed 10th July 2024, https://www.teramind.co/solutions/behavior-data-telemetry

85 Behaviour Alerts Trial, Teramind, accessed 10th July 2024, https://democompany.teramind.co/#/tma/behavior_alerts

Some of the pre-set rules in the trial provide stronger evidence of the control over employees Teramind seeks to offer companies. An employee detected accessing job listing websites can trigger an alert, as can emails the software thinks have "angry" sentiment or instant messages deemed "accusative", or an outgoing email with a CV attached.[86] The fact that these options are suggested in a sandbox version of the software is suggestive of the all-encompassing surveillance of workers Teramind seeks to empower employers with.

In addition to recording and archiving everything done on a computer while Teramind is running for live viewing by employers, the software also produces analysis reports for bosses – estimating how long a worker was active or idle, and the financial cost of this.[87] Detailed reports for all kinds of activity can also be produced, including company wide analysis of what the most popular search terms are on Google, the most popular words in social media posts or heat maps of behaviour alerts.

Teramind bills itself as a productivity, cybersecurity and data risk solution all rolled into one – but it is clear that some of its features offer such close monitoring of workers that there is a risk that employees could feel controlled. Although the services sold to UK companies by Teramind are unknown - so it is unclear whether the full surveillance suite is available in the UK – deploying such intrusive surveillance would raise novel legal issues, test the principles of necessity and proportionality, and raise the question as to whether existing UK laws are adequate to protect workers from the spectre of intrusive modern surveillance.

The company also claims that it "is not a 'big brother' solution" and that it does not "advocate unchecked surveillance", despite providing the technical capabilities to do just that.[88] Teramind's privacy guide on its how-to page for customers appears to place responsibility for employee privacy squarely on its clients, rather than itself. Companies using the software are helpfully offered tips on how to customise the monitoring, including only keylogging on certain websites, only recording staff screens when a rule violation is detected, or having an auto-delete for screen recordings. There are also instructions on how to suspend keylogging for password fields, a major threat to employee privacy, which implied passwords are logged by default.

86 Behaviour Policies Trial, Teramind, accessed 10th July 2024. https://democompany.teramind.co/#/behavior-policy

87 Productivity Trial, Teramind, accessed 10th July 2024, https://democompany.teramind.co/#/productivity

88 How To Set Up Teramind For Privacy-Friendly Monitoring, Teramind, accessed 10th July 2024, https://kb.teramind.co/en/articles/8791138-how-to-set-up-teramind-for-privacy-friendly-monitoring#h_01F1T1YKPNYBBNPFRNTCEWE560

It also suggests that instead of running Teramind software silently in the background, companies could be shown a privacy notice so they are aware of the monitoring, or could opt for the "revealed agent" – meaning staff can choose when to activate Teramind surveillance. At a minimum, a privacy notice would be legally required in the UK. With a nod to the Right of Access in the UK and Europe, the company also suggests that this right could be fulfilled by proactively giving employees access to all the data collected about them.

The overarching impression is that Teramind wants to put the privacy issue in the hands of employers – offering guidance on how to tone down its digital panopticon, but emphasising that "businesses can decide how they want to use it". If used to the fullest extent, Teramind's software amounts to total surveillance of a computer that gives employers the ability to see everything that happens on a device. In all but the rarest of circumstances this appears to be unjustifiable, and there is a serious risk to worker privacy.

Teramind Case Study

Teramind software has been linked to an unfair dismissal case in Manchester in 2019.[89] The software played a role in gathering information on an employee which ultimately led to his sacking, in a case that a judge found amounted to unfair dismissal.

At the crux of the case, employee Chris McCarthy was looking to branch out from the recruitment company he worked for and to set up his own company. He was accused of taking meetings on work time and using his work laptop for personal use – including looking at business plans and communications with potential future partners – in breach of company policy. He was dismissed from his job following the allegations in a process that an employment judge ruled was unfair.

The company's policies said that employees should devote all their work hours to the business, that visits to non-work related websites should be restricted outside of core hours, and that computer monitoring could be used by the company. This could include checking web browsing history, and "additional monitoring" where it was necessary for a given purpose, adding "employees are aware of when, why and how monitoring is to take place".

The software was installed on Mr McCarthy's work laptop by the IT department at Adam Recruitment, as his bosses became "suspicious" of him after his

89 Reserved Judgement, Mr C McCarthy v Adam Recruitment Ltd: 2404552/2019, Employment Tribunal, 17th December 2019, https://assets.publishing.service.gov.uk/media/5df7b320ed915d093a15d232/Mr_C_McCarthy_v_Adam_Recruitment_Limited_-_2404552_2019.pdf

“

The software played a role in gathering information on an employee which ultimately led to his sacking, in a case that a judge found amounted to unfair dismissal.

”

communication levels dropped – despite the employee continuing to meet all of his financial targets. Employment Judge Ross found that the software captured every event that happened on the laptop. Some of these were found to be relevant to his work conduct, such as opening up a copy of a personal business plan on the laptop, but the court also said that the software allowed Adam Recruitment to see into personal accounts from the employee and his family, when accessed on the laptop, as well as his work email account – with Mr McCarthy telling Big Brother Watch that some screengrabs were timestamped before 8am or after 5:30pm.

The judge acknowledged that the use of Teramind "raises difficult issues of privacy" – but did not elaborate much further on the privacy question in his ruling. Speaking to Big Brother Watch, Mr McCarthy said that the software was installed without his knowledge, as he was told that the IT department was adding antivirus software to the device – tallying with paragraph 41 of the ruling which said the screen recording footage was "covert".

This raises questions about the transparency principle around data protection and also appears to conflict with the policy of employees being aware of any monitoring. Both of these feed into further questions around the proportionality of the surveillance, especially when it looks to go beyond the company's policies around the monitoring of employee devices.

Mr McCarthy told Big Brother Watch that if he had been aware of his employer's total surveillance of his work laptop, he would not have looked at any of his personal documents or files on the device. He also outlined what kind of data was harvested from Teramind monitoring and presented as evidence during his dismissal hearings at Adam Recruitment, as well as at his employment tribunal. It ranged from his web browser usage to screen shots, and he said that the keylogging even recorded logins and passwords to sites he, and his family, accessed on the laptop.

Teramind's monitoring went beyond checking internet usage, or even what files were stored on a work device – monitoring which may have been proportionate to determine if non-work sites or files were being used on the laptop. ICO guidance on employer surveillance, albeit that which postdates the case by several years, states that the "least intrusive" means of monitoring must be used to achieve the purpose of the monitoring.[90] The extent of Teramind's monitoring of Mr McCarthy, including the capturing of passwords, does not appear to be the least intrusive means of achieving the stated goal, that is to show unreasonable personal use of an office laptop.

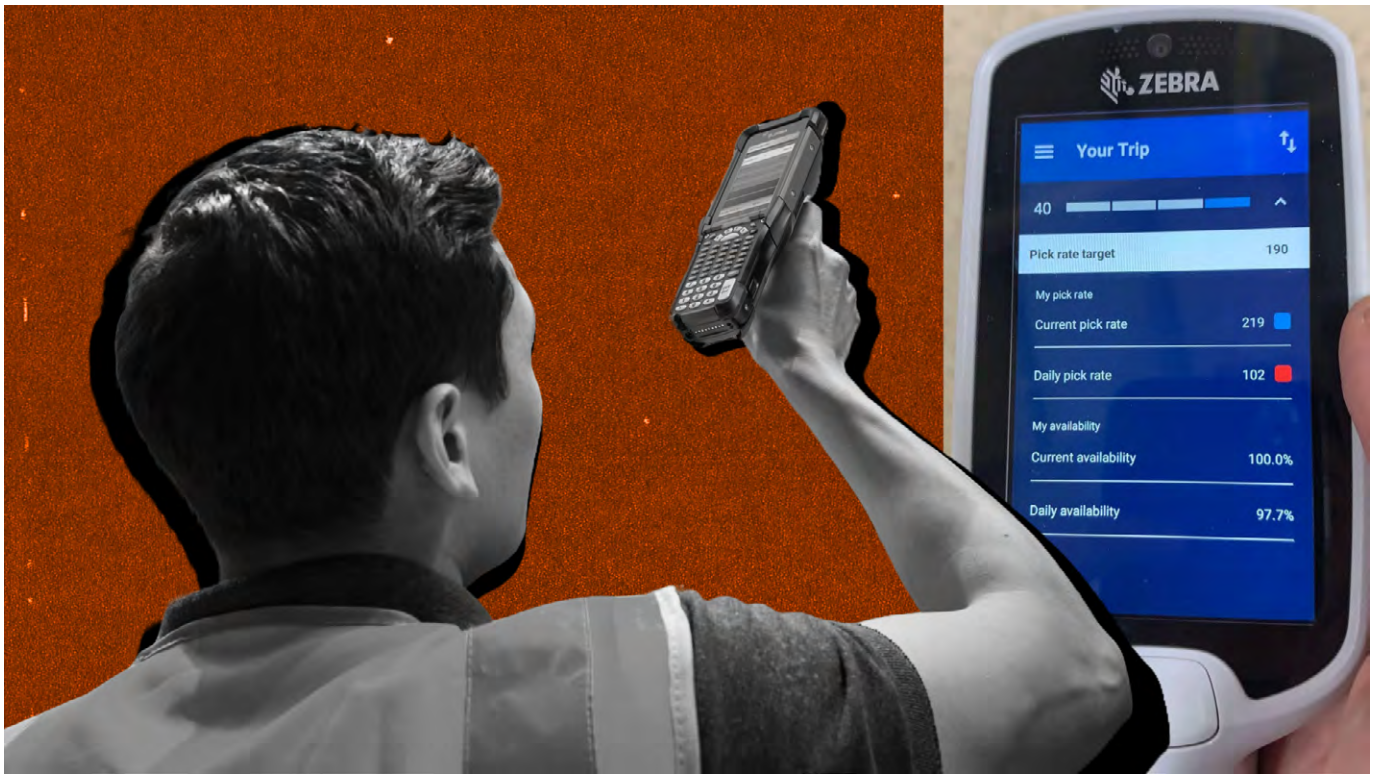
90 Data Protection and Monitoring Workers: Employment Practices and Data Protection, ICO, accessed 3rd September 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers

It also comes with additional data risks when used covertly as the employee is unable to make decisions to protect any sensitive or private data that may be collected from the use of Teramind. Even if it can be argued that monitoring browsing history is justifiable for a purpose of enforcing a work contract which forbids personal use of the web, collecting private information from this browsing such as passwords or personal emails clearly is not proportionate.

Although this case study is complicated by laws around wrongful and unfair dismissal, it nevertheless demonstrates how Teramind can pose an incredibly severe threat to worker privacy and how monitoring software can be used in a way that violates data protection principles.

Zebra Devices

Handheld scanners and portable computers are a staple of many kinds of work, including warehouse and supermarket staff, delivery people, and others who track the journey of items as part of their role. Specific applications vary depending on a worker's role and industry, but personal digital assistants (PDAs) are generally used to tick off and track tasks, provide a virtual to-do list for a worker, and sometimes monitor their location too.



Zebra, a US-based mobile computing company, is one of the biggest players in this market having supplied devices to major supermarkets including Tesco and

Sainsburys, Royal Mail and parts of the NHS. As with many kinds of technology there is potential for positive and justifiable use cases. During the pandemic a NHS Trust in Yorkshire used Zebra devices to allow for real-time documenting by medical staff at the bedside, with the barcode scanner allowing medics to access records quickly – and the devices were even used to facilitate video calls from locked down wards.[91]

However, as with many technologies and tools, it is as much how they are used as their capabilities which can lead to negative or harmful outcomes. Handheld devices can monitor not only the speed and accuracy of certain tasks but also the employee's movements and location. While these technologies are claimed to boost efficiency and accountability, they clearly exacerbate constant surveillance. Workers may feel pressured to maintain constant metrics that suggest high performance, knowing that any natural variations in their pace are closely monitored and recorded. This can lead to increased stress, reduced job satisfaction, and a diminished sense of autonomy and dignity, ultimately impacting overall well-being and productivity.

Supermarket workers have told Big Brother Watch that Zebra devices are used for algorithmic management of their workloads, while the digital assistants were found to use location tracking technology to compare planned and actual routes taken by Royal Mail delivery workers.[92] High capability devices that can collect large quantities of data, allocate work and analyse how it is done lay the groundwork for increased monitoring of workers, and management by machine.

Royal Mail Workers & Zebra PDAs

In 2023, it came to light that postal workers at Royal Mail were being monitored and pressured via their Zebra devices, known as PDAs, to work faster. The revelations came in front of the House of Commons' Business, Energy and Industrial Strategy Select Committee, after senior executives had initially denied that the PDAs were used to surveil workers.[93]

Giving evidence before the committee on January 17th 2023, and in a subsequent letter dated 20th February, Royal Mail's then CEO Simon Thompson said that the PDAs were not used to monitor workers or "nudge" them to go faster, and that

91 Innovative Use Of The Zebra TC51-HC At Calderdale & Huddersfield NHS Foundation Trust, Zebra Technologies, YouTube, 21st January 2022, https://www.youtube.com/watch?v=zDmkuS9AUlU

92 Royal Mail, Seventh Report Of Session 2022-23, House of Commons Business, Energy and Industrial Strategy Committee, 17th March 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmbeis/1045/report.html

93 Royal Mail Boss Blames Rogue Managers For Tracking Devices On Workers, The Guardian, 22nd February 2023, https://www.theguardian.com/business/2023/feb/22/royal-mail-boss-blames-rogue-managers-for-tracking-devices-on-workers

the tracking elements were used to provide customers with estimated delivery windows. Mr Thompson refuted comparisons with how Amazon used similar tools to track their workers.[94] In his follow-up letter Mr Thompson said that PDAs "do not track our people in real time", "do not tell people to walk more quickly" and that "data cannot be used in a disciplinary process except in exceptional, limited circumstances", which involved sign off from a HR professional. He added that there were only 16 cases in the 3 months from 1st November 2022.[95]

He also said that data from the Zebra PDAs, known as "outdoor actuals", is only available to supervisors the day after each shift. This data consists of start/end times, GPS comparison of actual and planned routes with mapping, activity breakdowns and movement classification, and transactions (such as delivery scans). The data can be used to infer information such as how a postal worker complied with the expected route and if they have complied with break rules.[96] An agreement between the Communication Workers Union and Royal Mail states that data should only be used in a de-identified and aggregated way.[97]

In his January 2023 evidence session, Mr Thompson told MPs that he was unaware of reported incidents of postal workers being challenged over alleged delays in deliveries linked to PDA data, assuring the committee that "being hauled into the office is not our standard practice. That is for sure."[98]

However, in the days following Mr Thompson's January 2023 appearance, the committee said it "received a large number of emails from postal staff saying that PDA data was indeed assessed for the purpose of individual performance management." [99] Some of these emails contained evidence published by the committee, including the account of one employee who said that he faced an hour-long interrogation from their manager over a minute-by-minute analysis of their PDA data after management accused them of being not productive enough, despite completing their deliveries.[100]

---

94 Simon Thompson, CEO, Royal Mail, Oral Evidence, House of Commons Business, Energy & Industrial Strategy Committee, 17th January 2023, https://committees.parliament.uk/oralevidence/12541/pdf/

95 Letter from Simon Thompson to Darren Jones MP, House of Commons Business, Energy and Industrial Strategy Committee Chair, 20th February 2023, https://committees.parliament.uk/publications/34034/documents/187363/default/

96 Letter from Simon Thompson to Darren Jones MP, House of Commons Business, Energy and Industrial Strategy Committee Chair, 20th February 2023, https://committees.parliament.uk/publications/34034/documents/187363/default/

97 RM & CWU National Agreement Covering the Use of PDA Outdoor Actuals, Letter to Branches, Communication Workers Union, 3rd May 2018, https://www.cwu.org/wp-content/uploads/2018/05/LTB-261.18-RM-CWU-National-Agreement-Covering-the-Use-of-PDA-Outdoor-Actuals.pdf

98 Royal Mail, Seventh Report Of Session 2022-23, House of Commons Business, Energy and Industrial Strategy Committee, 17th March 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmbeis/1045/report.html

99 Royal Mail, Seventh Report Of Session 2022-23, House of Commons Business, Energy and Industrial Strategy Committee, 17th March 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmbeis/1045/report.html

100 Extracts From Written Submissions, Simon Thompson Oral Evidence, 22nd February 2023, House

Other evidence showed printouts of anonymised PDA data of how long postal workers were stopping for on their delivery routes, sometimes linked to maps. Some printouts claimed to be "GDPR compliant" because names and dates were removed.[101] One example flagged three staff for stopping for more than an hour on their delivery routes, with the message "don't get caught... this is showing who is stopping on delivery". All of this is suggestive of PDA data being used for real time, routine monitoring of staff – rather than on an aggregated basis or for rare disciplinaries.

At Mr Thompson's second evidence session on 22nd February, after the committee recalled him due to their view that he had not given "wholly correct" answers, the Royal Mail CEO defended his position.[102] Senior Royal Mail officials claimed that these uses of PDA data, as routine workplace monitoring, were breaches of policy – effectively suggesting data was abused by rogue managers rather than a general policy of surveillance.[103] The Committee concluded in its report that it was worried by the gap between policy and reality when it came to PDA data use for staff monitoring, and demanded the Information Commissioner investigate. In December 2023, the ICO concluded that no further action was necessary following a scoping exercise, during which Royal Mail addressed some of the Committee's concerns and took feedback from the ICO on its data policies.[104]

Whether Royal Mail had a tacit understanding that PDA data would be used to surveil and manage employees, or it was rogue managers exploiting the system, is unclear. Either way, PDAs were able to gather huge amounts of data about how delivery workers went about their shifts, and this data was accessible to supervisors with few barriers. A data use policy, absent other practical protections, was inadequate to stop data being misused or repurposed for intrusive monitoring, and the Royal Mail PDA scandal is a warning that unless data is properly protected, mass workplace data collection can lead to unjustified surveillance either by whole organisations, or rogue managers.

---

of Commons Business, Energy and Industrial Strategy Committee, https://committees.parliament.uk/publications/34114/documents/187705/default

101 Slideshow, Extracts From Written Submissions, Simon Thompson Oral Evidence, 22nd February 2023, House of Commons Business, Energy and Industrial Strategy Committee, https://committees.parliament.uk/publications/34033/documents/187694/default

102 Simon Thompson, CEO, Royal Mail, Oral Evidence, House of Commons Business, Energy & Industrial Strategy Committee, 22nd February 2023, https://committees.parliament.uk/oralevidence/12700/pdf

103 Royal Mail, Seventh Report Of Session 2022-23, House of Commons Business, Energy and Industrial Strategy Committee, 17th March 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmbeis/1045/report.html

104 Letter to House of Commons Business and Trade Select Committee, ICO, 21st December 2023, https://committees.parliament.uk/publications/42747/documents/212705/default

Zebra In Supermarkets

Zebra devices are used by staff at Tesco and Sainsburys, two of the UK's largest supermarkets, both by workers and occasionally by customers using 'scan as you shop' options. Worker use of the devices relies on the combination of a high-tech scanner and a computer which can allocate and manage workloads.

Sainsburys employees told Big Brother Watch that Zebra devices are used both by delivery workers and in store "pickers" who gather items for click-and-collect or delivery orders. Pickers, who work on the supermarket floor – some of whom work while shops are open to the public – told us that the Zebra devices are a key way that their performance at work is monitored.

One staff member, who spoke to Big Brother Watch, said: "The managers, upon viewing each shopper on the computer, can see when we log on and off the handsets, where we are in the store and our picking speed."

The key metric used is IPH (items picked per hour), which hovered at around 190 for the worker speaking to Big Brother Watch. This level is "only really achievable if you're lucky enough to get bulk orders; that is multiples of the same item where, for instance, you may be standing in one spot picking, say, thirty tins of soup."

Smaller shops, or lists with diverse sets of items that require a lot of walking between shelves, push down the number of items staff can pick per hour, and in this case Big Brother Watch was told that the IPH target becomes "virtually unachievable" making it "appear that you've not been working fast enough". In the case of the worker who spoke to us, adjustments to the device-defined target are not made for orders collected when customers are in the store which necessarily slows work.

Workers could face sit downs with supervisors, observations and even disciplinary action if the Zebra devices record them consistently missing the rigid IPH targets. The employee who spoke to us said that how the IPH data is used varies between managers, with some understanding that variance in shop size or other factors could reduce the number of items collected, while others take a more black and white approach to the target. They told us that the monitoring via the devices make them "feel uncomfortable knowing that everything I do is monitored and potentially could land me in their bad books, despite the fact I'm working my best".

Posts on the social media site Reddit illustrate a similar use case in Tesco for Zebra devices – with a photo uploaded showing the workers' pick rate target, current

and daily pick rates, and the availability percentage of items on the pick list.[105] Discussion below the photo suggest that many workers infrequently meet pick rate targets, and how they are sometimes increased by management in response to staff consistently hitting targets.

Another worker who contacted Big Brother Watch about Zebra devices in use in their workplace drives deliveries for Argos and Sainsburys. Known as "pods" to the delivery drivers, they said that the devices act as a wider workplace computer. Capabilities include phone calls, GPS tracking and maps – and the driver expressed concerns that the GPS data is used to monitor workers.

Constant digital monitoring even of top-level statistics suggests that workers are not trusted to get on with the job, and that managers increasingly rely on quantified performance metrics rather than holistic management skills. This is compounded when computers are treated as the font of truth and objectivity, such as when the Sainsburys worker told us that some managers do not take other factors into account when assessing performance against the digitally-monitored targets. Seemingly low-level productivity tracking – using a computer to monitor how staff perform in a binary way against pre-set targets – can create a general atmosphere of distrust among staff, who feel like they are being constantly watched and unfairly judged in a one-dimensional way.

Amazon Warehouses

Amazon's warehouses are known to be hotbeds of workplace surveillance. From atomisation, meaning the breaking down of work into discrete tasks and separating workers from the overall task, to algorithmic management, the e-commerce giant has been at the forefront of efforts to digitally monitor workers.[106] Thousands of workers across the world, including more than 250 in the UK, have expressed concern about Amazon's level of monitoring in the workplace.[107]

Some of the company's workplace surveillance technology is exemplary of modern threats to workers' digital rights – for example, the bracelet tracker patented by Amazon in 2018. It could precisely track where workers were in the warehouse down to where their hands are near on a shelf – and even vibrate to nudge them in the right direction. These kinds of technologies pose new privacy problems in light of monitoring and surveillance within the workplace that are completely

105 Only Started Dotcom 4 Days Ago Can Someone Please Explain These Numbers, r/Tesco, Reddit, 21st August 2023, https://www.reddit.com/r/tesco/comments/15xfgup/only_started_dotcom_4_days_ago_can_someone_please

106 Hired, p.16, James Bloodworth, Atlantic Books, 2018, ISBN: 9781786490162

107 Life In The Amazon Panopticon: An International Survey Of Amazon Workers, UNI Global Union, January 2023, https://uniglobalunion.org/wp-content/uploads/UNIAMZN_Report.pdf

disproportionate to productivity goals. The Amazon bracelet was covered with shock in the press, but trade unions in the UK told Big Brother Watch that they have never seen it in action.[108] However, the fact it was patented underlines how intensely Amazon thinks it could monitor its workers.

Handheld devices, often made by Zebra, are used to instruct and monitor workers in Amazon's huge warehouses across the country[109]. James Bloodworth, a journalist who worked in an Amazon warehouse as research for his 2018 book 'Hired', said that pick rates were a key metric, as with supermarkets, and were monitored via handheld scanners. Data was fed back to line managers who send digital instructions to workers as needed, usually criticism or demands to speed up.[110] "Idle" or so-called non-productive time was also monitored, including necessary breaks such as using the bathroom – and Bloodworth said that this was often used as a way to criticise workers at the start of their shifts.[111]

The account in Bloodworth's book tallied with what Dr Tom Vickers, an academic at Nottingham Trent University and Director of the Work Futures Observatory, who was seconded to the GMB union in the Midlands during the first part of 2024 i told Big Brother Watch. GMB had been fighting to get recognised as a representative union at Amazon's Coventry warehouse, but narrowly failed to win a ballot in the face of a brutal campaign by the American company to crush unionisation efforts.[112] Dr Vickers told us that digital monitoring, including "idle time", is used to discipline workers – and a lot of line managers' time is spent considering how to react to data gleaned from surveillance.

Similar technology is deployed via cameras, rather than handheld devices, to monitor how workers stow items in some warehouses. A 2024 report by Fairwork, an academic project looking at fair standards in the future of work, following up on work by The Bureau of Investigative Journalism, outlined how some warehouses use the Nike Intent Detection System (IDS), where cameras feeding into computer vision tools automatically detect where items are stored.[113][114] This system is known to be used at at least one Amazon warehouse in Bolton, in the north west. The TBIJ investigation found that the Nike system went beyond just tracking where

108 Amazon Patents Wristband That Tracks Warehouse Workers' Movement, The Guardian, 1st February 2018, https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking
109 Life In The Amazon Panopticon: An International Survey Of Amazon Workers, UNI Global Union, January 2023, https://uniglobalunion.org/wp-content/uploads/UNIAMZN_Report.pdf
110 Hired, p.16, James Bloodworth, Atlantic Books, 2018, ISBN: 9781786490162
111 Ibid. p.48
112 'Just The Beginning': GMB Launches Legal Action Against Amazon As Workers Lose Union Vote, Sky News, 17th July 2024, https://news.sky.com/story/amazon-workers-lose-union-vote-13178306
113 Transformation Of The Warehouse Sector Through AI, Fairwork Amazon Report 2024, June 2024, https://fair.work/wp-content/uploads/sites/17/2024/06/Fairwork-Amazon-Report_June24-2.pdf
114 The Eyes of Amazon: A Hidden Workforce Driving A Vast Surveillance System, The Bureau of Investigative Journalism, 21st November 2022, https://www.thebureauinvestigates.com/stories/2022-11-21/the-eyes-of-amazon-a-hidden-workforce-driving-a-vast-surveillance-system

items were stored - without the need for handheld scanners, it was also able to see if workers made errors when stowing items and generate error reports for management, which could be used in disciplinaries.

Surveillance often goes hand in hand with workers becoming increasingly siloed and assigned a narrow set of tasks, which are subject to digital monitoring. Activists said that workers are given a set of tasks on their handheld device, or workstation, but are not told what their exact targets are – however, their performance is still tracked and compared against colleagues. Lower performers can then be disciplined just for being in the bottom percentile, potentially even if their targets are met.

The monitoring technology is also capable of auto-reporting rule breaches into the disciplinary system, such as too much idle time, according to Dr Vickers.. GMB union added that the machine-monitored targets are generally either used with sanctions, with missed goals leading to management intervention, or lead to ever-increasing targets if workers meet their goals. Research in Italian Amazon warehouses suggest a physically demanding "Amazon pace", effectively a very brisk walk, is required for workers to meet their targets, with constant productivity monitoring keeping this in check.[115] Additional research has suggested that where Amazon uses robots more frequently walking demands on workers drop, however physical demands on workers remain high due to the nature of warehouse work.[116]

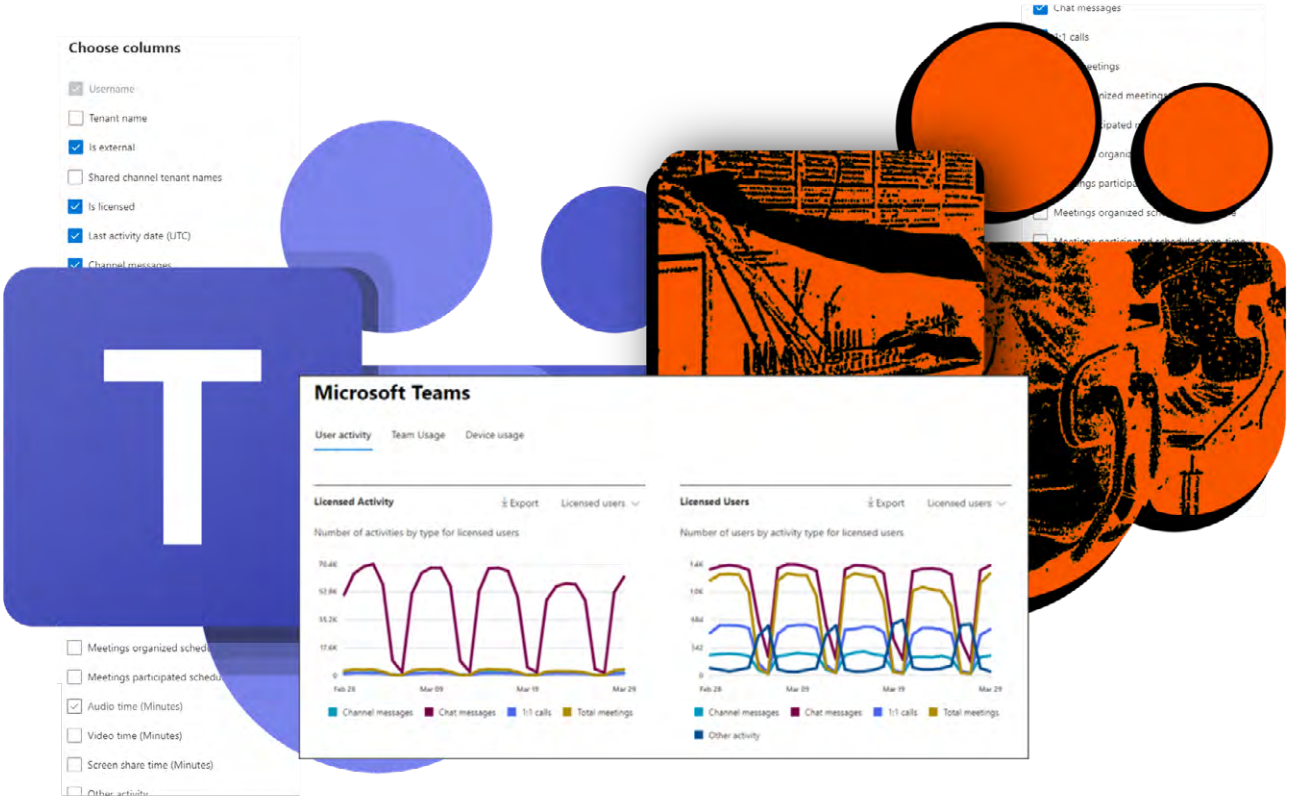
As with the supermarkets the monitoring focus is speed, though the intensity is greater. Beyond supermarkets, the unions and other research suggest that algorithmic management, and the monitoring which feeds in, forms the basis of praise and discipline in the warehouses, with managers effectively triaging surveillance data to supervise workers. The pre-eminence of data and machine management can only demoralise workers, as human nuance cannot be taken into account in the same way that a real life supervisor might do. Constant monitoring, nudging and feedback from digital devices creates the impression that workers are simply part of the machine.

At Amazon there appears to be a secondary impact of atomising work and removing all sense of knowing what the greater task at hand is. Agency is removed as workers are given minute instructions, only seeing part of what is going on – effectively becoming a cog, governed by a machine, rather than contributing to a wider goal in the workplace.

115 Machinic Dispossession And Augmented Despotism: Digital Work In An Amazon Warehouse, Allesandro Delfanti, New Media & Society 23(1), January 2021, https://doi.org/10.1177/1461444819891613
116 Unfulfilled? Evidence Review on Work, Labour and Employment in Amazon's Fulfilment Centres, Dr Dominic Holland and Dr Tom Vickers, Work Futures Research Group, Nottingham Trent University, 2021, https://www.ntu.ac.uk/__data/assets/pdf_file/0034/1579327/Unfufilled-Evidence-Review.pdf

Microsoft Teams

Not all forms of workplace surveillance stem from monitoring-specific tools – so-called 'bossware' is becoming increasingly embedded in all kinds of work-focussed software. Microsoft Teams is used by thousands of organisations across the country from the NHS, to Whitehall departments and consulting giant Accenture. Known best as teleconferencing and work channel messaging software, under the hood Teams has a string of capabilities that can be used by bosses to closely monitor their staff.[117]



With the pandemic-driven rise in working from home Teams has become a common tool used by many formerly office-based workforces, acting as a central platform for work-related communications for workers spread out geographically. Beyond just facilitating communications, Teams also collects huge quantities of data about how workers use it and packages this up in a way that allows companies to analyse worker activity.

117 Microsoft Teams Analytics and Reporting, 3rd March 2023, Microsoft, https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-user-activity-preview?view=o365-worldwide

When using Teams as a standalone piece of software to instant message colleagues and schedule meetings, rather than solely as a videoconferencing platform, it publicly displays a users' activity status to colleagues who click on their profile by default – this may be available, busy (generic busy/call/meeting), do not disturb (focusing/presenting), away, be right back or offline.[118] This allows bosses to quickly see what people might be doing – and the away status which is triggered after a few minutes of inactivity suggests that someone may be away from their desks. The auto-switching to "away" and supervisor check-ins on Teams statuses was a key trigger for the explosion of so-called "mouse jigglers", software and/or hardware that simulates the movement of a computer mouse by automatically moving the cursor - which led to efforts from Microsoft to stop them working.[119] [120] Although mouse jigglers became something of an online meme, they represent the normalisation of low-level workplace surveillance.

Supervisors can generate 'user activity' reports for their staff on Teams, which can pull together a huge number of data points including last activity dates, the number of messages or posts in shared and private chats, the number of meetings and calls someone has had, duration of screen, audio and video sharing, and the number of meetings scheduled.[121] By default this data is identifiable, and only a top-level administrator can choose to anonymise the data and limit the granular analysis of individual workers.

Teams also integrates with other Microsoft products, including OneDrive (a cloud drive platform), Outlook/email, and Edge (Microsoft's web browser) and collects cross-tool data in a similar way to how it collates data for activity on Teams. Analytics reports for OneDrive, which are linked to specific users, allow bosses to see how many files a user opens, edits, shares and deletes.[122] Integration with email gives supervisors insight into email inbox capacity and last used date, frequency of emails being sent, received and read and email-related follow ups such as meetings scheduled.[123]

On top of the standard user-level data available to organisations, Microsoft also

118 User Presence In Teams, Microsoft, 9th August 2023, https://learn.microsoft.com/en-us/microsoftteams/presence-admins

119 Idle No More: How Automatic Mouse Jigglers Are Taking On Nosy Bosses, The Guardian, 6th March 2023, https://www.theguardian.com/technology/2023/mar/05/idle-no-more-how-automatic-mouse-jigglers-are-taking-on-nosy-bosses

120 Mouse Jigglers Do Not Work In New Teams, r/MicrosoftTeams, Reddit, 23rd April 2024, https://www.reddit.com/r/MicrosoftTeams/comments/1cb62iy/mouse_jigglers_do_not_work_in_new_teams/

121 Microsoft Teams Analytics and Reporting, 3rd March 2023, Microsoft, https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-user-activity-preview?view=o365-worldwide

122 Microsoft 365 Reports In The Admin Center - OneDrive Activity, Microsoft, 3rd January 2021 https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/onedrive-for-business-activity-ww?view=o365-worldwide

123 Microsoft 365 Reports In The Admin Center - Email Activity, Microsoft, 3rd April 2024, https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/email-activity-ww?view=o365-worldwide

offers a software link which allows for further integration with Microsoft 365 services (including Office and Calendar), in addition to Windows tools such as printing and on-device activities into the data collected on workers.[124] As the API tool is not a standard or pre-set service, it is not clear how it is used in practice to monitor staff but it provides additional capabilities if required. Integrating data collection with further Microsoft services has the potential to increase worker monitoring, as it would allow bosses access to even more data to observe and analyse.

Microsoft Teams exemplifies how pervasive surveillance can become a routine part of daily life, with monitoring built into general use software. It increases the amount of data available on employees, transforms worker behaviour into data points that could be misused, and creates conditions where performance is equated to non-stop working and employees are constantly nudged to be perpetually busy, making the workplace more stressful and jobs more demanding. Concerns have been expressed, including by Privacy International, about the impact of the low hum of surveillance underpinning Teams – but the backlash has been minimal.[125,126]These kinds of systems are embedded into work processes, meaning that low-level surveillance has quietly become the norm for many despite eroding the quality of many jobs.

POLICY ANALYSIS

Although workplace surveillance and employer fixation with tracking employee behaviour to monitor and measure productivity is not new, there is currently very little effective policy implementation or regulatory intervention for these practices in place.[127] As noted by the ICO, excessive monitoring can have a negative impact on the rights and freedoms of workers, as well as undermine their privacy and mental well-being.[128] What constitutes 'excessive' will depend on the context and application in which the monitoring occurs, but even monitoring that falls short of the 'excessive' threshold can still be detrimental to workers.
While workers are entitled to greater privacy at home, some employers view the

124 Microsoft Graph Reports API Overview, Microsoft, 2nd January 2024, Microsoft Graph reports API overview, https://learn.microsoft.com/en-us/graph/reportroot-concept-overview?view=graph-rest-beta
125 How Does Microsoft Teams Track User Activity, TechTarget, 24th October 2023, https://www.techtarget.com/searchunifiedcommunications/tip/How-does-Microsoft-Teams-track-user-activity
126 WFH - Watched From Home: Office 365 And Workplace Surveillance Creep, Privacy International, 15th June 2022, https://privacyinternational.org/long-read/4909/wfh-watched-home-office-365-and-workplace-surveillance-creep
127 Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees, Amy Vatcha, London School of Economics, iS Channel, https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf
128 Data Protection And Monitoring Workers, Information Commissioner's Office, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf

physical disconnect as justification for increased surveillance. Although employers have understandable reasons to want to ensure efficiency and productivity, electronic surveillance often exceeds proportionate worker management and becomes a spying tool.

Monitoring an employee's use of a business-issued laptop to access work emails during work hours is very different to an employer being able to see every single activity through intrusive apps such as Teramind that permit continuous monitoring. The surveillance is comprehensive and collects a large amount of data on workers in a way that contravenes the GDPR principles of data minimisation.[129] Management gets instantaneous information as the data is collected in real time, the equivalent of having a boss looking over an employee's shoulder and recording their every action for the entire shift. These kinds of digital monitoring surveillance systems can capture communications between a worker and their union representative or private correspondence, raising significant concerns for privacy and freedom of expression. There are plenty of less intrusive methods for ensuring staff productivity that the ICO recommends, such as staff training and carrying out performance reviews.[130] However, the rapid development and prevalence of remote working surveillance and the consistent issues with enforcing existing data rights as outlined in this report suggest that new worker protections are needed to deal with advancing technology, and to ensure that existing rights are properly protected.

Keystroke logging is perhaps one of the most invasive forms of monitoring and is completely unacceptable in all but the most exceptional of circumstances. In Germany, monitoring is only allowed when an employer has a concrete suspicion of an employee committing a criminal offence or serious breach of duty.[131] This demonstrates how workplace surveillance can be restricted to prevent intrusive systems from impacting the majority, instead only being deployed in the most serious of circumstances. Despite different national contexts, both Germany and the UK's laws are based on GDPR, which makes this example relevant and worthy of reflection.

In the limited cases where these technologies are justifiable, it is imperative that the data is not accessed or used unless absolutely necessary. There is a significant difference between recording this kind of data and accessing or using

129 Principle (c): Data Minimisation, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/

130 Employee Monitoring – Is It Right For Your Business?, Information Commissioner's Office, https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/employee-monitoring-is-it-right-for-your-business

131 German Court: Monitoring Of Employees By Key Logger Is Not Allowed, 8th August 2017, Christopher Ritzer, https://www.dataprotectionreport.com/2017/08/german-court-monitoring-of-employees-by-key-logger-is-not-allowed/

it. Data collected from keystrokes should never be accessed unless illegal activity is suspected, in which case it should only be looked at for the purpose of that specific investigation. It is crucial that employers do not use intrusive systems as a catch-all solution; just because a form of monitoring is available does not mean it is the best way to achieve their aims.

Automated Decision-Making

Over-reliance on data-driven management is incredibly risky, even more so when decisions are automated. Increasingly, complex decisions ranging from task allocation to pay and progression are being made or heavily influenced by algorithmic management tools and automated or semi-automated decisions (ADM).[132]

Article 22 of the UK GDPR largely prohibits the automated processing of personal data for decisions about individuals that would have 'legal or similarly significant' effects unless there is a contract, consent or legal authorisation. It means that there must always be "human involvement" in significant decisions, such as a performance review at work. However, the example of the Post Office tracking scandal makes clear that, even when there is a human in the loop, the potential for error, biases, and harmful consequences remains high.

Combining surveillance technology and algorithmic systems can be disastrous. Automated systems that analyse this data can result in a false sense of precision in measuring employee performance, risking unfair assessments.[133] This is particularly sensitive in the employment context due to the well-documented occurrences of bias in algorithms and AI systems, as errors could put people's jobs on the line.

Article 22 of the UK GDPR prohibits solely automated decision-making processes, including profiling, that produces legal or other significant effects unless specific conditions are met, such as explicit consent or substantial public interest. Individuals have the right to be notified when such automated decisions are made and to request human intervention or challenge the decision. However, these protections may not always be effectively communicated or implemented by employers in practice.

UK data protection law provides some protection against automated decision-making where there is no human intervention in a decision that has legal or

132 Watching Me, Watching You: Worker Surveillance In The UK After The Pandemic, Institute for Public Policy Research, March 2023, https://ippr-org.files.svdcdn.com/production/Downloads/worker-surveillance-mar23.pdf 14.

133 Final Agenda for Scottish Trade Union Congress 127th Annual Congress, Mike Arnott, 2024, https://www.stuc.org.uk/resources/final-agenda-2024-digital.pdf 28.

similarly significant effects under Article 22 of the GDPR.[134] Human intervention is not clearly defined in law but ICO guidance says it must be "active and not just a token gesture" with a key test being if a person can alter a decision, or simply rubber stamp it.[135] However, this is currently only guidance rather than law. The vagueness around the term "human intervention' creates a loophole for employers to claim humans have been present in a decision when the involvement has been purely administrative. Taxi drivers previously brought legal challenges against Uber concerning surveillance technology that triggered the dismissal of multiple drivers, in which the Netherlands Court of Appeal decided that three of the four workers had been robo-fired by means of unlawful automated management decision making.[136] While Uber argued that the decisions to dismiss the workers were reviewed by a team at a service centre in Poland, the workers were given no opportunity to answer the allegations made against them and the human review of the automated decision was "no more than a symbolic gesture".[137] This example demonstrates that the ambiguity around the level of human intervention required in the decision-making process creates space for companies to try and sidestep it – even though, in the case of Uber, it was found to be unlawful.

Clarification is needed to specify that a decision based on solely automated processing is one that involves no meaningful human involvement, an issue that Big Brother Watch has long campaigned for.[138] Our concern was echoed during the passage of the Data Protection Bill in 2017 by the Deputy Counsel to the Joint Committee on Human Rights, who warned that "There may be decisions taken with minimal human input that remain de facto determined by an automated process".[139] Regrettably, this has proven to be true in the years since its enactment. In 2023, the previous Government sought to rectify this issue in the Data Protection and Digital Information Bill: Article 22A(1)(a) sought to amend UK GDPR by defining a decision based on solely automated processing as one that involves "no meaningful human involvement". This was an important clarification that would have prevented merely administrative approval of an automated decision being considered adequate to qualify a decision as a human one and thus exempt from the legal safeguards that

134 Rights Related To Automated Decision Making Including Profiling, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib4

135 Ibid

136 Amsterdam Court Of Appeal Rules In Favour Of Uber And Ola Cabs' Drivers, Fieldfisher, 20th April 2023, https://www.fieldfisher.com/en/insights/amsterdam-court-of-appeal-rules-in-favour-of-uber-and-ola-cabs-drivers

137 State of Surveillance in 2023, Big Brother Watch, December 2023: https://bigbrotherwatch.org.uk/wp-content/uploads/2023/12/State-of-Surveillance-Report-23.pdf

138 For example, see Big Brother Watch's Briefing on the Data Protection Bill for Committee Stage in the House of Commons, March 2018, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/03/Big-Brother-Watch%E2%80%99s-Briefing-on-the-Data-Protection-Bill-for-Committee-Stage-in-the-House-of-Commons.pdf 5.

139 Note from Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017: https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

should apply. Despite this, the Bill was incredibly damaging to data rights in many other respects and was dropped during the wash-up after the General Election was called.[140] However, it remains that this amendment is critically needed to ensure that decisions that have either no human involvement or only tokenistic involvement will be considered solely automated. Creating this threshold would reduce ambiguity and safeguard against the context-specific harms that arise from wholly automated decisions in the workplace.

Transparency

Increasing levels of surveillance tech and the corollary exertion of control in the workplace can feel oppressive. Research shows that placing workers under surveillance leads to decreased job satisfaction, increases risk of physical health conditions, infringes upon autonomy and dignity, and lowers organisational trust.[141] Low levels of trust are exacerbated when surveillance is hidden behind impenetrable algorithms, introduced by stealth, or not explained to workers, or when systems initially are introduced for one reason but then are used for further surveillance goals without transparency.

Workers and their representatives should be included if an organisation is planning to introduce monitoring, an opinion shared by the ICO.[142] To start with, workers should be actively involved in deciding what technology will be used, the purposes for data collection, who will have access to this data, how long it will be retained, and ensuring that technology is there to help rather than surveil or threaten employees. Staff must not be left in the dark over how systems are being used to make decisions that affect them, which is why transparency from the employer and early engagement and consultation with workers and their representatives is key. One way to achieve this is to create a legal obligation for employers to conduct algorithmic impact assessments, which will be explored further in the chapter on AI in the hiring process.

140 Data Protection and Digital Information Bill, last updated 5 May 2023, https://bigbrotherwatch.org.uk/wp-content/uploads/2024/03/BBW-DPDI-Briefing-for-House-of-Lord-Committee-Stage.pdf Article 22(1)(a)

141 Watching Me, Watching You: Worker Surveillance In The Uk After The Pandemic, Institute for Public Policy Research, March 2023, https://ippr-org.files.svdcdn.com/production/Downloads/worker-surveillance-mar23.pdf 15.

142 Data Protection And Monitoring Workers, Information Commissioner's Office, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf 19-20.

RECOMMENDATIONS

3. Create a legal requirement for employers to perform algorithmic impact assessments prior to any implementation of AI or algorithmic-based technologies likely to result in a high-risk to the rights and freedoms of workers or job applicants. This should be accompanied by a framework issued by the Secretary of State that organisations conducting an AIA must follow. This must include a requirement for a mandatory bias testing to proactively ensure any such system is compliant with the Equality Act 2010, even if the system is procured from a third party.

4. Amend Article 22 of the UK GDPR to clarify that human involvement in a decision involving automation must be meaningful, if the decision is not to be considered 'solely automated'.

AUDIOVISUAL SURVEILLANCE

Technology that may be seen as "traditional surveillance" – video and audio monitoring – is not uncommon in the modern workplace, and is now increasingly coupled with new technological add-ons to make the monitoring even more intrusive. Consumer, worker and public safety are promoted by employers as the benefits that justify increasing levels of surveillance. CCTV cameras are ubiquitous in many workplaces with improvements to technology allowing them to appear on workers' chests, in cars, and in fixed buildings.

Audiovisual surveillance that which is camera or microphone based, has been around for a long time but it remains a visceral and often impactful form of monitoring. The presence of physical devices acts to underline that the subject is being watched, potentially creating an atmosphere of suspicion and distrust.

As with other forms of CCTV and audio surveillance, companies are required to demonstrate that the use of this technology is lawful, fair and transparent. For example, CCTV might be installed outside a certain door in a building to deter theft, but efforts must be made to ensure that areas of no legitimate interest are not monitored.[143] The ICO states that it is "likely that employees would not always reasonably expect to be monitored by video or audio surveillance systems in their day-to-day roles" and this expectation of privacy should be taken into account when considering if surveillance is justified.

Continuous audio and video monitoring are particularly intrusive and the ICO states that this "is only likely to be justified in the rarest of circumstances", and that in all circumstances consultation with workers and unions should happen before surveillance tech is installed.[144]

However, many companies take liberties with these requirements, using limited justification to install continuous surveillance or undertaking only the most limited consultations with third parties – workers across industries have told us that panopticons of cameras are common, even when appearing to be unnecessary. There are of course circumstances when limited camera use could be justified, but the approach taken by some companies appears to be one where workers are treated with suspicion by default.

143 How Can We Comply With The Data Protection Principles When Using Surveillance Systems?, Information Commissioner, accessed 2nd July 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems

144 Ibid

Audio Recording On Buses

A bus company in Brighton was accused of secretly recording audio from both passengers and drivers by the trade union Unite.[145] The Brighton & Hove Bus Company, owned by the multi-national transport group Go-Ahead, was allegedly making audio recordings onboard its buses - without placing warning signs up to make passengers or staff aware of the secret listening devices, which is a legal requirement under the UK GDPR.[146]

Unite said that its members were not consulted about the installation of the audio recorders on the Sussex buses, despite drivers' safety being the supposed aim of the scheme – specifically to protect from verbal abuse.[147] The union said that as well as catching drivers' conversations, there was a high risk of passengers' conversations not only with the driver but among themselves being recorded too if they were close to the vehicle cab.

145 Brighton Buses Accused Of Big Brother Bugging Of Drivers And Passengers, Unite, 30th May 2024, https://www.unitetheunion.org/news-events/news/2024/may/brighton-buses-accused-of-big-brother-bugging-of-drivers-and-passengers

146 How Can We Comply With The Data Protection Principles When Using Surveillance Systems?, ICO, accessed 23rd August 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems

147 Sussex Bus Company Accused Of 'Big Brother' Style Audio Recordings, HelloRayo, 31st May 2024, https://hellorayo.co.uk/greatest-hits/sussex/news/sussex-bus-company-accused-of-big-brother-style-audio-recordings

The drivers' union reacted furiously to the installation of secret audio recording devices by the bus company, with Unite general secretary Sharon Graham branding the move as "outrageous Big Brother-style behaviour from the bus company, who are secretly recording drivers and their passengers without warning." As of May 2024, the union was balloting on industrial action in response to the sound recording devices, although the company has disputed the union's assertions that recording was taking place.[148]

Audio recording is considered to be "more privacy intrusive" than video recording, and the Information Commissioner states that organisations "should not normally use surveillance systems to directly record conversations between members of the public".[149] This sets the bar to justify sound recording much higher than video recording, particularly when the surveillance is continuous rather than activated on-demand for a legitimate purpose. A particular need must be identified to justify the recording, other less intrusive methods must have been considered and rejected and audio recording must be made explicitly clear.

The negative reaction from the bus drivers' union suggests that the identified issue did not justify the recording, while the lack of alleged signage -as claimed by United - failed to comply with legal obligations.

Brighton & Hove buses is not the only operator in the UK to deploy in-cab audio recording. Transport for London has admitted that some of its contracted operators choose to install listening devices, although these operate under each operator's rules rather than TfL's centrally, so it is unclear what signage and trigger requirements are in place.[150] Lothian Buses, in central Scotland, also state in their conditions of carriage that they may have in-cab audio recording – but state that signage warning passengers and staff is available.[151]

Defending itself, the Brighton bus company claimed that audio recording is routine among some other operators.[152] However, the similar use of audio recording by operators including Lothian Buses and some TfL subcontractors does appear to stretch the legal boundaries of UK GDPR and contradict the ICO advice that audio recording for workplace surveillance is only justifiable in "exceptional

148 Brighton and Hove Disputes Unite Claim Of On Bus Audio Recording, Route One, 31st May 2024. https://www.route-one.net/news/brighton-and-hove-disputes-unite-claim-of-on-bus-audio-recording

149 How Can We Comply With The Data Protection Principles When Using Surveillance Systems?, Information Commissioner, accessed 2nd July 2024. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems

150 Recording Devices In Buses, FOI-0748-2122, Transport for London, 5th August 2021, https://tfl.gov.uk/corporate/transparency/freedom-of-information/foi-request-detail?referenceId=FOI-0748-2122

151 Conditions of Carriage, Lothian Buses, June 2024, https://www.lothianbuses.com/conditions-of-carriage

152 Brighton and Hove Disputes Unite Claim Of On Bus Audio Recording, Route One, 31st May 2024. https://www.route-one.net/news/brighton-and-hove-disputes-unite-claim-of-on-bus-audio-recording

circumstances" and should be off by default, unless such circumstances apply.[153]

Having a fly on the wall, listening to every comment and utterance thought throughout the working day, clearly has a significant negative impact on privacy even in a public facing role. Ordinary interactions will naturally be more reserved given the chance that the boss could listen in later, and workers will no doubt feel on edge – negatively impacting their comfort in the workplace.

AI Powered Fatigue Monitoring

Advances in technology mean that cameras are able to do a lot more than record video in 2024. Computer vision and artificial intelligence allow camera feeds to be used for facial recognition, object identification and more. For workers who drive for a living, whether in HGVs, coaches or vans, high-tech cameras are increasingly being deployed to monitor their behaviour and attempt to detect tiredness every second they are at the wheel.

National Express, one of the UK's biggest coach companies, openly subjects its drivers to second-by-second analysis of their wakefulness, well-being and focus while at work.[154] The monitoring works both by providing immediate alerts if the system is triggered, as well as generating longer term performance evaluations of drivers. It is promoted as a safety feature for customers, but the impact of surveillance on workers appears not to have been considered.

On National Express's latest coaches the behaviour analysis driver camera is provided by Lytx, with the press release announcing this claiming that the in-vehicle cameras would "enhance driver performance", making no mention of public safety.[155] Lytx's DriveCam is much more than a simple in-cab camera; it has a host of powerful high-tech features that underline its potential to be a spy-in-the cab. It is not clear which of these features National Express deploy beyond knowing they focus on alertness, focus and well-being of drivers.

The company claims to use machine vision and artificial intelligence to "detect and deter risky and distracted driving in real time".[156] Driver facing cameras are

153 How Can We Comply With The Data Protection Principles When Using Surveillance Systems?, Information Commissioner, accessed 2nd July 2024. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems

154 Our Coaches, National Express, accessed 2nd July 2024, https://www.nationalexpress.com/en/help/our-coaches

155 National Express Unveils First Of 25 New Van Hool Altano TDX21 Coaches, National Express, 15th March 2024, https://www.nationalexpress.com/en/news/national-express-unveils-first-of-25-new-van-hool-altano-tdx21-coaches

156 Machine Vision + Artificial Intelligence, Lytx, accessed 2nd July 2024, https://www.lytx.com/features/machine-vision-and-artificial-intelligence

said to be able to detect risky driving incidents, trigger real-time alerts for drivers and even collate incidents, either for individual or fleet level analysis by employers. Other surveillance capabilities include live streams of video feeds from inside cabs, in addition to standard recording, audio recording, and risk detection without video recording for "fleets with particular sensitivity to driver privacy" – suggesting that always-on recording is the default option.

Risky behaviours scanned for by the in-cab camera include a driver smoking, eating or driving, mobile phone use, inattentiveness and a lack of seatbelt use.[157] The mechanics of this appear to be fairly clear with computer vision algorithms "seeing" infringements on the video feed. How Lytx detects fatigue is less clear, but US-based case studies suggest triggers attempt to detect "nodding off at the wheel".[158]Questions about the accuracy of the system will remain while the company fails to be transparent about how its technology works - a paper from the Transport Institute at Virginia Tech in the US argued that it is difficult to properly assess AI-powered driving evaluators with the limited information available.[159] Regardless of the lack of clarity, it is clear that driver behaviour and cues are

157 Machine Vision + Artificial Intelligence, Lytx, accessed 2nd July 2024, https://www.lytx.com/features/machine-vision-and-artificial-intelligence

158 How Ryder Is Staying One Step Ahead of Driver Fatigue, Lytx, 1st February 2023, https://www.lytx.com/newsletter/how-ryder-is-staying-one-step-ahead-of-driver-fatigue

159 Comprehensive Assessment of Artificial Intelligence Tools for Driver Monitoring and Analyzing Safety Critical Events in Vehicles, Yang et al, Virginia Tech, Sensors (Basel) 24(8), April 2024, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11055067

constantly analysed by the in-cab camera to make judgements about alertness, wakefulness and performance.

Data from the AI-powered behaviour monitoring is then packaged up by the software and displayed on a dashboard that suggests how drivers can "self-correct" as well as providing employers with a granular overview of every minor infraction or event for their whole roster of drivers.[160] The result is a constant stream of surveillance data, potentially picking up every movement and sound in a cab, being sent back to supervisors – while AI analyses the minutiae of a driver's performance.

Addison Lee

Private hire firm Addison Lee began fitting all its vehicles with in-cab cameras beginning in the winter of 2023 to 2024. Drivers for Addison Lee rent their cars from the company, and can use them as they please when not working. The Independent Workers of Great Britain (IWGB) trade union, which represents many Addison Lee drivers, told Big Brother Watch that the company began by quietly including cameras in vehicles as they were replaced – before requiring drivers of existing vehicles to come and get cameras fitted later on.

IWGB said that drivers were not given much in the way of information or explanation about the installation of cameras in their vehicles; they simply appeared in replacement cars or were fitted compulsorily in cars still in use. The lack of consultation in installing an always-on surveillance device is concerning, and the lack of privacy and data protection information given to the drivers raises legal issues. The union told us that some drivers questioned why the cameras were being installed, and several answers were given including insurance requirements to justify the cameras, while some drivers were given a holding response.

IWGB told Big Brother Watch that Addison Lee uses Samsara cameras in its vehicles. Samsara does offer AI-powered driver facing cameras, with many of the features outlined in the National Express case study.

The dual-role Addison Lee cars play for their drivers, as both personal and work vehicles, creates a minefield in terms of surveillance. Always-on monitoring equipment in this context will undoubtedly capture private moments, whether that is parents driving children to school or sensitive off-the-clock phone conversations, and significant protections need to be put in place to protect driver privacy.

160 Fleet Safety Program Powered By Video, Lytx, accessed 2nd July 2024, https://www.lytx.com/fleet-safety

For months this was not the case at Addison Lee – the driver facing cameras were always on and the workers were told that they could not deactivate or cover them up when not on the clock, the union told us. Disregarding the privacy impact of surveillance in work hours, as outlined in the National Rail example, here workplace monitoring became constant monitoring. IWGB said that drivers who questioned the 24/7 activation of the in-vehicle cameras were told that for insurance reasons they could not be covered up even in personal time. The union said that it knows of at least 3 drivers subject to disciplinary action for covering up their cameras when on private journeys.

Effectively, Addison Lee had a spy in the car not just for work trips but anytime the vehicle was running – meaning drivers were never truly alone in there. IWGB said that drivers had expressed concerns about their children being recorded, or female family members caught on camera adjusting their hijabs - potentially serious invasions of privacy.

According to the union, most drivers for the company work paycheck to paycheck, meaning that pushing back against their employer could put them in a difficult position. New drivers are also subject to a 3-month minimum term for their vehicle hire, meaning that if they decided to reject the surveillance in the cars they could be out of pocket to the tune of thousands. The financial pressures in combination with the limited information given to drivers about the data protection considerations or justifications suggests a serious disregard for driver privacy.

After months of questioning Addison Lee, IWGB got journalists involved and passed them the story – with the private hire firm telling reporters the same story as the union, that 24/7 operation of in-cab cameras was an insurance necessity. IWGB says that there had been no change in the insurance documentation held by drivers before and after the camera rollout, suggesting that was not necessarily the case. The union then demanded a copy of the master document from the company to verify the claims.

Shortly afterwards, Addison Lee issued a so-called clarification – it claimed that drivers had misunderstood the policy and that cameras could be covered for private journeys. Given the union has said that drivers were disciplined for covering them up when off-the-clock, and journalists were told that 24/7 operation was an insurance requirement, this appears to be a sharp U-turn under pressure, rather than a multi-month misunderstanding.

Addison Lee drivers can now cover up their cameras when not working, and protect their private lives – after union pressure. However it is not clear that this is sufficient to meet Addison Lee's data protection obligations – the company

still needs to identify a legitimate purpose for intrusive recording and the onus is on the company rather than the data subject to ensure data is collected and processed lawfully. Whilst the U-turn is a significant win and shows that workers can resist surveillance, the constant at-work monitoring remains a problem and belies a lack of trust in workers by default that cannot be conducive to a positive workplace environment.

Bodyworn Cameras

Bodyworn cameras (BWC), sometimes referred to as bodyworn video (BWV), have become increasingly common among workers who have direct contact with the public, from shop assistants to train guards.[161] BWV is now common in shops, tourist attractions and even libraries. It is now Transport for London policy that 'frontline' staff wear the cameras, while manufacturer Axon markets its BWC as a tool to protect 'frontline workers' on 'every shift'.[162] These cameras are often promoted as a tool to "protect" workers and provide a deterrent to aggressive members of the public.[163] This is all in addition to the longer-standing use of BWV among police and security guards.

Generally BWC are small chest mounted devices which record audio and video footage when activated by the wearer, and otherwise record a short loop of a few seconds footage which is constantly overwritten to make sure that moments before an incident are also captured.[164] Depending on the model, the recorded footage may be stored on the device for later use, or it might be live-streamed to a control room once the recording is activated.

Some trade unions, including the Rail, Maritime and Transport Union (RMU) and shop workers' union USDAW, and professional bodies such as the Royal College of Nursing (RCN), have claimed that there are some benefits to workers from BWV.[165,166,167]

---

161 How Body Cams Create A Culture Of Fear, The Spectator, 22nd June 2024, https://www.spectator.co.uk/article/how-body-cams-create-a-culture-of-fear

162 Axon Body Workforce, accessed 29th August 2024, https://cdn.prod.website-files.com/63bffc98a9ee7d56338f1525/65b1bb825aeba85234744834_Axon_ProductCard_AxonBodyWorkforce_8-5x11_01c%20(1).pdf

163 Protecting Retail Heroes, Reliance Protect, accessed 29th August 2024 https://www.relianceprotect.co.uk/blog/article/protecting-retail-heroes

164 VT100, Reliance Protect, accessed 29th August 2024, https://www.relianceprotect.co.uk/body-worn-cameras/vt100/

165 RMT Guidance Of Bodyworn Cameras, Rail and Maritime Union, accessed 29th August 2024, https://www.rmt.org.uk/about/health-and-safety/health-and-safety-circulars/rmt-guidance-on-body-worn-cameras130524/

166 RCN Position On The Use Of Body Worn Cameras, Royal College of Nursing, 22nd May 2023, https://www.rcn.org.uk/About-us/Our-Influencing-work/Position-statements/rcn-position-statement-on-the-use-of-body-worn-cameras

167 Tesco Chief's Backing For A Law Change To Help Prevent Violence And Abuse Against Shopworkers Is Welcomed By USDAW, USDAW, 3rd September 2023, https://www.usdaw.org.uk/latest-news/tesco-chief-

However, they also acknowledge that the safety benefits come from BWV addressing the symptoms of aggression and abusive incidents rather than the causes of them. The RMU and RCN further have strong policies against the use of BWV to monitor staff, instead outlining how the cameras should only be used to protect staff rather than as a way of bosses surveilling their workers. However, workers have mixed feelings about BWC requirements and critics say the overuse of BWC "create a culture of fear".[168]

The privacy risks go beyond that of general use CCTV for several reasons. These include the recording of audio in addition to video which is viewed as more intrusive, and the directed nature of BWV which is unlike CCTV watching over a wide area. These risks apply both to the subjects of recording, and the workers wearing the cameras, as BWV footage also captures them at close quarters, and will capture anything they say on the audio feed - even if video is not captured.

Subjects' awareness of filming, or lack of, is another important privacy consideration - as there is a chance that BWC could be quietly activated without any communication of the fact - although many systems have a recording alert light in an attempt to remedy this risk. Unnotified recording could breach the transparency principle of data protection law, if a subject is unaware of filming. This consideration is less applicable to workers who in theory would know that they have activated their camera – although they could miss out on a colleague also activating theirs. Indeed, the Spectator reported that workers often inadvertently turn recording on without meaning to.[169]

The potential selectivity of BWV footage which may not capture an entire interaction or event is a wider rights risk to both the public and employees, as BWC are touted by suppliers as a way of recording evidence of incidents.[170] Incomplete records necessarily do not tell the full story of an incident, and this places both the public and workers at risk - as an incomplete story could lead to faulty conclusions being drawn and incorrect consequences following.
It has also been suggested that BWC make workers feel directly observed and put them on edge, with the Fire Brigades Union stating it has concerns "that the use of body worn cameras could create a hostile atmosphere and cause significant GDPR issues".[171] Further, aggressive members of the public may react poorly to being

s-backing-for-a-law-change-to-help-prevent-violence-and-abuse-against-shopworkers-is-welcomed-by-usdaw/

168 How Body Cams Create A Culture Of Fear, The Spectator, 22nd June 2024, https://www.spectator.co.uk/article/how-body-cams-create-a-culture-of-fear/

169 How Body Cams Create A Culture Of Fear, The Spectator, 22nd June 2024, https://www.spectator.co.uk/article/how-body-cams-create-a-culture-of-fear/

170 VT100, Reliance Protect, accessed 29th August 2024, https://www.relianceprotect.co.uk/body-worn-cameras/vt100/

171 Fire Brigades Union Response to the Independent Culture Review of the London Fire Brigade, Fire

recorded. Meanwhile, both the RMT and RCN called for training about data rules and the implications to be given to workers when BWC are deployed, suggesting that the complexity of data protection law also creates further space for inadvertent transgressions by workers.

Companies must demonstrate that they have a legitimate interest in deploying BWC in order to lawfully do so. As such, the data processing must be necessary and proportionate to meet those legitimate interests, balanced against the rights and interests of the data subjects. Clearly, worker safety will have significant weight in this assessment where genuine risks apply, but BWV's risks to the privacy of workers and the public, and the potential for negative impacts on dignity at work, mean that the use of the cameras cannot be said to be appropriate in all settings. The Spectator's reporting of BWC being procured at English Heritage sites and libraries in Essex cannot be compared to the use of cameras by police officers, for instance, and suggests that some cameras could be being used with inadequate assessments of the necessity.[172] Since no prior external authorisation is needed for a company to deploy BWC, workers and the public are often the regulators of last resort – enforcement action can only be taken to roll back illegitimate or excessive use of BWC if individuals complain.

Conclusions

Audiovisual surveillance tools are perhaps the most common in modern day workplaces, and they can serve a legitimate purpose – from protecting premises from theft to independently documenting any serious incidents. The question of how data is used, as well as how much is collected is key. There is a significant difference between data collected to be used legitimately for specific purposes, and unjustified constant data collection and monitoring of workers.

Advancing technology and capabilities of audio and video monitoring tools mean that the threat to data rights has only increased over the years – with surveillance now becoming more sophisticated, and machines not just recording what goes on but analysing workers for bosses' convenience too. A device constantly watching or listening in feels intrusive, and this feeling will only be exacerbated when the spy-on-the-wall can make predictions and evaluations about workers too.

The familiarity and commonality of these tools, particularly cameras, should not be an excuse for their inappropriate use in the workplace or for employers to

Brigades Union, 22nd February 2022, https://www.fbu.org.uk/sites/default/files/publications/LFB%20Culture%20Review%20response%20v6_1.pdf

172 How Body Cams Create A Culture Of Fear, The Spectator, 22nd June 2024, https://www.spectator.co.uk/article/how-body-cams-create-a-culture-of-fear/

deviate from the principles of necessity and proportionality. Rising use of CCTV and bodyworn cameras raises significant questions about whether the principle of necessity is being watered down in the absence of challenge, as it is not always clear that BWV rollouts are genuinely necessary, or the least intrusive option, to serve a company's legitimate interests. In the case of BWV, there also appears to be a contagion effect, as a growing number of workplaces are adopting the cameras and it is likely that the increasing commonality of BWC will lead more bosses to see their use as a standard procedure. However, just because another organisation uses surveillance tech inappropriately it does not justify others to do so. It is important that legitimate interests assessments are thoroughly considered, examined and where appropriate, tested to break the cycle of the unjustified surveillance creep and protect workers' and the public's data rights.

LOCATION TRACKING

Advancing surveillance technology constantly seeks to exploit new types of data about workers, enabling the datafication and quantification of activities and personal attributes that may not have previously been tracked in the workplace. The impact of this greatly has expanded the granularity, scale, and pace of data collection.[173] These surveillance issues are exemplified through location tracking and audiovisual monitoring, where employers have access to vast amounts of data that can build a picture of the day-to-day life of workers.

Clandestine minute-by-minute tracking of the exact locations of people and vehicles with hidden tracking devices is a common spy film trope. Tiny trackers are seen attached to suitcases, clipped onto cars or even inserted into flesh. Fortunately, employers do not go quite that far when monitoring where their staff are during the working day – but there is a growing trend of bosses collecting ever more granular data about where their workers are, and how they move through the world.

GPS tracking is now a common tool used to track journeys and, as such, people who drive for a living, whether Ubers, courier vans or huge trucks. Satellites are also used to locate individuals either on an ongoing basis as they move around their workplace, or as they "log in" between work sites. Vehicle tracking goes far beyond just the coordinates of the car or van - increasingly, advanced telematic devices are recording everything a driver does from their braking patterns to door slams, according to workers who spoke with Big Brother Watch.

Location and traditional surveillance in the workplace both come with a spatial limitation: "when I leave work, I am no longer visible".[174] However, workplace surveillance has metastasised beyond the confines of the office. Companies seeking to enforce back-to-office policies in the aftermath of the pandemic are deploying a host of tools to track who is in the building. In addition to swipe card data, which many workers might think is collected, information such as which devices connect to office Wi-Fi is being used to track and verify employees' presence in the building. As many people's livelihoods involve off-site working, the concept of the "workplace" requires extending and reframing as the "workspace".[175] The workspace provides the conditions for location and traditional surveillance methods to run rampant, as employees are at risk of constant monitoring.

173 Explainer: Workplace Monitoring & Surveillance, Data & Society, February 2019, https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf 1.
174 Ibid
175 Data Subjects, Digital Surveillance, Ai And The Future Of Work, European Parliamentary Research Service, December 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf 1.

Aside from when it is introduced strictly as a necessary health and safety measure, the use of GPS, video, and audio monitoring in the workplace is often based on the assumption that employees are not capable of working sufficiently without increased oversight. There is an emerging trend in which organisations are adopting a 'just more surveillance'[176] approach, where technology is applied as a quick-fix to problems in the workplace.

Lightfoot - Tech Deep Dive

Multiple companies offer granular tracking of drivers and vehicles used for work. UK-based Lightfoot is one of these, with its clients including Tesco, Asda, Virgin Media and Octopus Energy. While this can be justified to the extent of complying with working time regulations and handling liability if an accident occurs, the use of these technologies has seeped into performance monitoring and shaping driver behaviour.[177] The services Lightfoot offers go beyond traditional telematics to include AI-powered analysis of the person behind the wheel, and the gamification of all the data collected to shape worker behaviour to create social pressures and competition amongst drivers.[178]

Going beyond traditional black box telematics, Lightfoot gives bosses a real time feed of almost every aspect of a vehicle while it is on the move.[179] Data is packaged up and displayed for employers on a dashboard that helps them watch the status of their vehicles, and their drivers, in real time.

Telematics consist of driving data derived from a device connected to the vehicle, with non-workplace examples including black boxes for car insurance. Generally, the data collected will include location, miles driven, when a vehicle is driven, braking and turning data, acceleration and speed.[180]

Marketing materials claim that Lightfoot is "constantly bringing back data from in the vehicle and in the cab".[181] The types of data collected can be set by the companies who own the vehicles. Lightfoot is not transparent on its website about

176 'Just More Surveillance': The ECtHR And Workplace Monitoring, Michael Molè and David Mangan, September 14th 2024, https://journals.sagepub.com/doi/10.1177/20319525231201274?icid=int.sj-full-text.similar-articles.1

177 Electronic Monitoring And Surveillance In The Workplace: Literature Review And Policy Recommendations, Kirstie Ball, European Commission, 22nd September 2021 https://publications.jrc.ec.europa.eu/repository/handle/JRC125716 28.

178 Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk

179 Vehicle Telematics, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/vehicle-telematics

180 What Is Telematics, LV, 6th March 2024, https://www.lv.com/car-insurance/what-is-telematics

181 Vehicle Telematics, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/vehicle-telematics

what forms of data the device can collect on drivers, but it appears to include live GPS location, general telematics data, and a whole tranche of information from a vehicle's systems which feed back everything from fuel levels, to how turns are made and brakes applied, to whether dashboard warning lights are active.[182][183] Despite not outlining the specific forms of data collected, the implication is that almost every possible data point about how a vehicle is driven is hoovered up. Lightfoot also offers in-cab cameras, similar to those used by National Express – meaning Lightfoot offers near total surveillance of workplace vehicles.[184]

The Lightfoot platform feeds information back to employers, giving them granular data on how their employees drive every single mile they are on the job. It also analyses how drivers drive, allowing bosses to monitor incidents of speeding, harsh driving (such as fast acceleration and sharp turns), time spent idling and even fuel and emissions savings.[185] Rather than collecting driving data for use in case of incidents or issues, the dashboard is designed to allow bosses to constantly monitor driving performance for a vast number of reasons.

As well as providing monitoring feedback to bosses, the system also automatically

182 Vehicle Telematics, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/vehicle-telematics
183 Support, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/support
184 Dashcams, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/dashcams
185 Support, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/support

tries to "educate" drivers with "nudges" to get them to alter their driving behaviour.[186] With a focus on constant feedback on driving efficiency, the monitoring black boxes in the vehicle first warns drivers with lights and then with audible "nudges" in attempts to get them to correct "inefficient", but likely lawful, driving behaviour.[187] If nudges are not adhered to, a driving penalty is logged - these lower a driver's score on the Lightfoot ranking system. This pushes Lightfoot beyond surveillance into an automated behaviour-altering tool, that operates at a below-lawbreaking threshold.

The company even tries to get workers to be more accepting of the surveillance by gamifying it. Drivers are given a Lightfoot score, which rates the efficiency of their driving.[188] Workers can log in to see how their driving has been rated by the automated system, and a league table ranks drivers on their efficiency as well as the number of penalties received. High scorers are given "elite" status which allows drivers to enter competitions with cash prizes.[189] These prizes can be in the thousands of pounds, placing significant incentives on drivers to listen to the robot's nudges.[190]

Gamifying data poses a real risk to health and safety, which is particularly ironic given that many location tracking technologies are introduced under the pretext of improving it. For drivers, creating an environment driven by performance metrics can place extreme pressure to meet shifting thresholds that are often arbitrary and likely automated.[191] The trade union Unison describes such complications:

> *"In some circumstances this has led to employees being disciplined for accelerating a vehicle to avoid a collision; employees becoming distracted by monitoring telematic information, leading to road traffic accidents; employers inappropriately accessing private information about the lives of their employees."*[192]

There is also a risk that drivers may skate over critical but non-quantifiable aspects of their job, like safety checks, or take on extra risks to meet efficiency benchmarks or targets, like driving through bad weather.[193] They might feel pressured to justify

186 How Does Lightfoot Work, Lightfoot, 4th July 2023, https://support.lightfoot.co.uk/2023/07/04/how-does-lightfoot-work
187 Ibid
188 Lightfoot Brochure, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/docs/Lightfoot-Brochure-11.pdf
189 FAQ: What Are The Benefits Of Being An Elite Driver?, Lightfoot, YouTube, 7th September 2021, https://www.youtube.com/watch?v=DwLjSP9AKEw
190 Gamification, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/gamification
191 Explainer: Workplace Monitoring & Surveillance, Data & Society, February 2019, https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf
192 Monitoring And Surveillance Workplace Policies, UNISON, July 2020: https://www.unison.org.uk/content/uploads/2020/07/Monitoring-and-surveillance-at-work-1.pdf 28.
193 Explainer: Workplace Monitoring & Surveillance, Data & Society, February 2019, https://datasociety.

longer gaps in productivity or necessary stops, such as rest or bathroom breaks. This blinkered focus on competitive productivity becomes a real problem when drivers are more worried about their score than prioritising safe driving, compromising both their own safety and that of others on the road. Gamification of these roles can also erode dignity, with workers describing the experience as "almost like a hypnotic experience", leaving them feeling "like an android".[194]

Although companies will own the identifiable data, Lightfoot also claims the right to aggregate and anonymise driver data – arguing that it owns this anonymised, aggregated data.[195] Clients are also asked to ask drivers to allow data collection on both work and private journeys - although drivers cannot be lawfully forced to agree to this.[196] According to Lightfoot, whether or not drivers even have the capability to disable tracking for private use "depend(s) on which options their fleet manager has chosen" as "only management level are able to switch tracking on and off".[197]

Lightfoot claims that obeying automated orders from a surveillance system "grants drivers more autonomy in their work".[198] It also touts the benefit of managers not having to have awkward conversations with underperforming drivers. The price – constant monitoring, instead of vehicle data being analysed when a problem is noticed, means that workers are subject to 24/7 surveillance to correct the most minor of behavioural aberrations.

Reviews of the Lightfoot app on the Apple App Store are broadly damning, painting a picture of workers who argue that the monitoring and nudges around efficient driving lead to a style that is "simply dangerous", with one person saying "as a fuel saving device in urban areas it is excellent however it does not promote safer driving".[199] Although the reviews cannot be verified, the repeated similarity of these points suggest that the view is commonplace amongst affected workers.

The perma-monitoring embedded in the system, alongside the gamification of surveillance, data collection and abdication of responsibility to employers in relation to private journey tracking suggest that Lightfoot could pose a significant

net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf 12.

194 High Score, Low Pay: Why The Gig Economy Loves Gamification, The Guardian, 20th November 2018, https://www.theguardian.com/business/2018/nov/20/high-score-low-pay-gamification-lyft-uber-drivers-ride-hailing-gig-economy

195 Lightfoot Standard Services v3.5, 10th December 2019, https://www.lightfoot.co.uk/docs/Terms-for-Lightfoot-Standard-Services.pdf

196 Ibid, para. 11.5

197 How Do You Disable Tracking For Private Use?, Lightfoot, accessed 22nd July 2024, https://support.lightfoot.co.uk/2023/07/04/how-do-you-disable-tracking-for-private-use/

198 Gamification, Lightfoot, accessed 22nd July 2024, https://www.lightfoot.co.uk/fleet-management-products/gamification

199 Reviews, Lightfoot, App Store, accessed 22nd July 2024, https://apps.apple.com/gb/app/lightfoot/id1119563366?see-all=reviews

threat to worker privacy – particularly in dual use vehicles.

Location Tracking in Construction

Construction workers have told Big Brother Watch that some employers are requiring them to install GPS-tracking apps when on site. One app we were told is used in the UK is Chime, which markets itself as "the #1 time and attendance app for construction".[200] It is used by dozens of building companies across the country.

It goes way beyond digitising paper-based records such as timesheets, offering bosses the ability to get site sign-ins verified by photo and GPS tracking. It is not clear why this is necessary data to collect: Chime states "there's no more clocking off early", which is suggestive of a predetermined suspicious approach to workers.[201] Instead of trusting workers, Chime suggests that bosses resort to digital surveillance by default.

The GPS tracking is not limited to a single verification of check-ins to site - Chime allows bosses to constantly geolocate their workers throughout the day. One construction worker who contacted Big Brother Watch said that his employer told

200 Brochure, Chime, accessed 22nd July 2024, https://chimenow.my.salesforce.com/sfc/p/#8d00000AXynP/a/Sr000000ADK9/ MnWCectoEJoyoB2FIW_KTf3MkV5C0eigMa6aBXZ3Ti0
201 Brochure, Chime, accessed 22nd July 2024, https://chimenow.my.salesforce.com/sfc/p/#8d00000AXynP/a/Sr000000ADK9/MnWCectoEJoyoB2FIW_KTf3MkV5C0eigMa6aBXZ3Ti0

him it was a safety tool, but the impression was that it was mostly used to track employees' locations to improve workplace productivity.

He told Big Brother Watch that although bosses argued that GPS tracking apps were promoted as a safety tool by bosses, he could not see how they were – when site workers already have to complete rigorous safety courses and obtain industry ID cards to access the workplace, which require certification. He said that the consensus among colleagues was that the GPS tracking was to add an additional layer of supervision and amounted to an invasion of privacy in his view. He told us that he had chosen to only work for companies not deploying the tracking tech, as he thought it was unjustified when he could already show he was qualified to work safely.

The privacy policy on Chime's website is not clear as to whether and how they process the data for their own purposes beyond feeding back information, including GPS data, to employers.[202] For example, the policy very broadly states that "We may process your data when it is reasonably necessary to achieve our legitimate business interests" without providing further information on those interests or the nature of the potential processing. The worker added that some construction companies ask constructors to install the app on their personal phone.

Lone working on a construction site can be a dangerous task, and in certain safety contexts there could be a justification for a technology that may allow a worker to be found if they fall or go missing. Chime is a long way removed from such safety situations, instead allowing bosses to GPS track workers every minute they are at work.

Data protection rules require processing to be necessary and proportionate. However, it is difficult to argue that constant GPS surveillance on ordinary construction sites could be either, especially without a clear reason as to why non-tracking based solutions could not serve the same end of protecting safety and ensuring accurate time-cards.

Nationwide Presentee Checks

After the pandemic's mass-scale readjustment of working practices, many businesses have been left with empty offices for large parts of the working week. In attempts to bring workers back to the office, some have instigated minimum attendance policies to compel staff to be in the building for at least some of the

202 Privacy Policy, Chime, accessed 22nd July 2024, https://www.chimesoftware.co.uk/s/privacy-policy

week – which has been met with resistance in some workforces.[203]

As a result, some companies have decided to no longer rely on an honour system and co-operation to enforce their attendance policies, turning to workplace surveillance to ensure that their staff attend in person for the requisite days. This includes the building society Nationwide, which is collecting a string of different data points to check if staff members are complying with their office attendance policy. An employee at the building society told Big Brother Watch that as well as monitoring swipe card data, Nationwide could check whether a worker's devices had connected to the building's WiFi or if they accessed wired internet networks to see if they had been on site.

In a set of FAQs, the company said that swipe card and internet access data could be used to generate monthly reports for bosses who would check if workers were attending the office as often as required, with non-compliance leading to disciplinary action. A privacy policy claims that data will not be used for performance measuring or comparing staff, but solely for enforcing the attendance policy.

The worker told Big Brother Watch that the policy was imposed from above, with comments under the announcement on the intranet turned off – limiting employees' ability to share their views on the introduction of attendance surveillance, and said that they were not personally aware of prior consultation with staff on the policy of data collection. They added that this has created a "toxic" work environment.

Companies are entitled to ask their staff to attend the office for a number of days per week, unless they have a home-working contract, but the principles of necessity and proportionality must be considered when choosing how to monitor it. In buildings where swipe cards are used, use data is often collected as a matter of course – often for fire safety reasons – but there are legitimate questions as to whether and how such data should be repurposed.

It is unclear how the collection or use of Wi-Fi and internet access data could be seen as necessary and proportionate, particularly if Nationwide already has access to swipe card data to enforce its attendance policy. Data collection must be as limited as possible under the data minimisation principle and collecting multiple forms of data for the same purpose does not appear to be in that principle's spirit.[204]

In addition to the necessity and data minimisation issues, there is the wider issue of worker perception of data collection to proactively enforce attendance

203 Stats Officials Refuse Two-Day Week In Office, BBC News, 27th April 2024, https://www.bbc.co.uk/news/articles/cqqnz7g4451o

204 Data Minimisation, ICO, accessed 4th September 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/

policies, which may make employees feel distrusted in a way that checks following suspicion of non-compliance may not. Similarly, the introduction of data collection for this reason when workers feel they have not been properly consulted could contribute to greater feelings of distrust in the workplace.

Birdie - Tracking Care Workers

Birdie is an app used by care workers that presents itself as a one-stop-shop for social care administration.[205] It allows carers to make digital notes and observations and share these with bosses, colleagues, and clients' families. It contains profiles of carers and clients, and acts as an admin hub with rotas and hour logging.[206] It also facilitates the surveillance of carers' whereabouts by their bosses, either through check-ins or GPS tracking.

One of the features of the Birdie app offered to bosses is call (home visit) monitoring, with the company claiming that it aids staff safety and compliance - "know that your staff are safe and everyone is where they should be at all times".[207] There are three options for this:

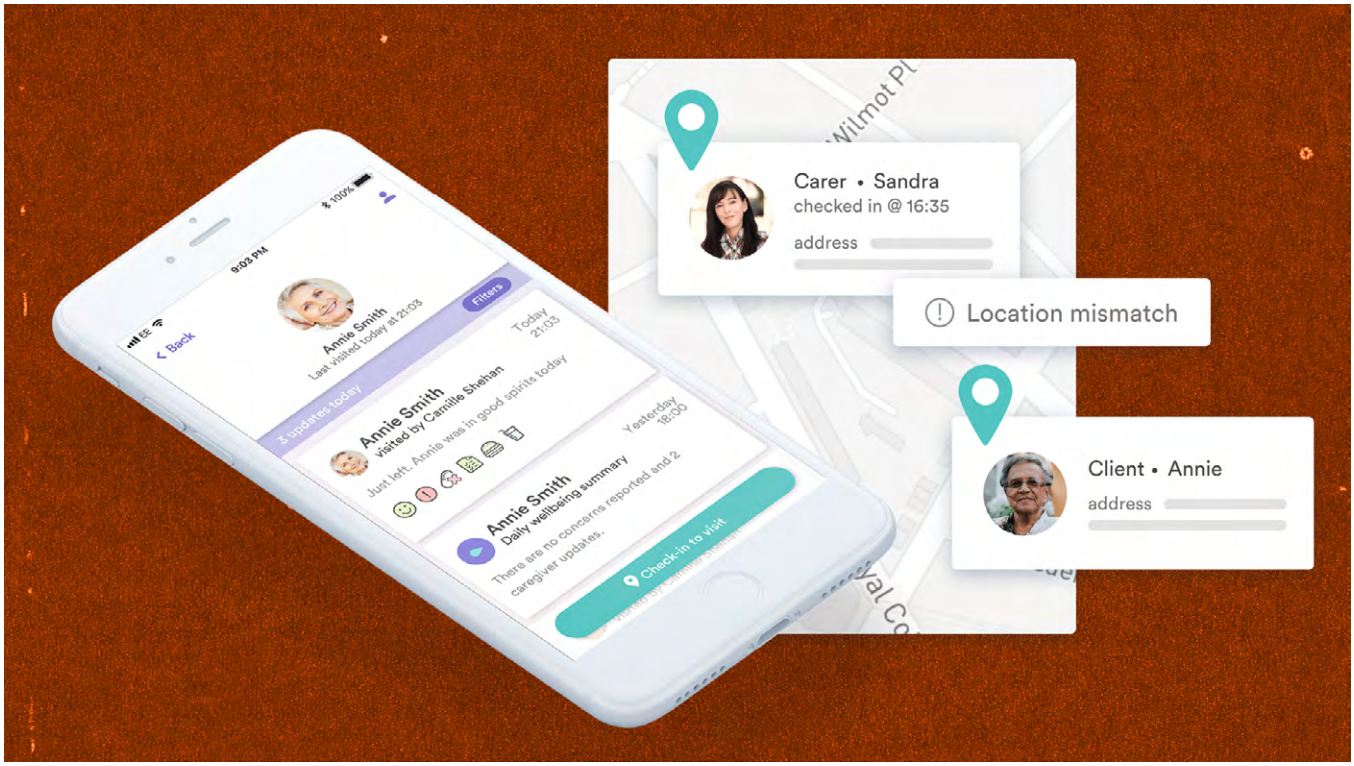
- A device generating a One Time Password (OTP) can be installed in a client's home, with the code being entered in the app to verify the carer is there
- A QR code can be scanned at the client's home to verify that the carer is there
- GPS tracking can be used, with satellite location verifying that the carer is in the vicinity of the client's home

A care worker whose employer imposed the app on them said the app, and the check-ins, came in without much consultation and without their consent. The location tracker can be turned off on a client-by-client basis, but does not appear to be variable depending on the care worker.[208] This implies that location-tracking check-ins are a default option, rather than being a specific monitoring option in response to concerns about a worker's behaviour – such as saying they were at a client's home earlier than they were. Surveillance as a business as usual practice may not be necessary and certainly implies a lack of trust between supervisors and workers. Speaking to Big Brother Watch, the care worker said that the move to the digital system with location-tracking check-ins made her feel "spied on at all

205 Birdie, accessed 22nd July 2024, https://www.birdie.care/product-features/carer-app
206 Birdie app, App Store, accessed 22nd July 2024, https://apps.apple.com/gb/app/birdie-care/id1254394392
207 Call Monitoring Software, Birdie, accessed 22nd July 2024, https://www.birdie.care/call-monitoring-software
208 Secure Call Monitoring, Birdie, accessed 22nd July 2024, https://help.birdie.care/en/articles/3106792-secure-call-monitoring

times". This went beyond the system it replaced, the carer said, with monitoring replacing a call from the office if issues arose.

The carer also said they were told their profile on the app had to include a photograph of them, which was visible to anyone looking at their client's notes – such as the client's family who would not just see their notes and a name, but the carer's face too. Although the carer said they were more than happy to carry an ID badge to identify themselves to clients, the potential of being clocked in public by a stranger related to a client and potentially asked questions felt like a step too far as it would undermine the carer's ability to go about their business outside of work peacefully.



Knowing which workers are where is clearly valuable information to bosses who want assurance that vulnerable people are being cared for at the right times, or to check in on performance. But routinely tracking location throughout the working day can be an intrusive form of monitoring, and using it as a default tool does not appear to be necessary nor proportionate, when other options are available. Instead of trusting workers to be where they should be, the deployment of location tracking technology implies a pre-existing distrust of employees which can only undermine workplace morale.

In The Workplace

If devices or vehicles are linked to a specific person and information collected can be linked to a worker, this qualifies as personal data under data protection law. There are often less intrusive methods or tools available, ones that do not exacerbate the information and power asymmetry characteristic of workplace surveillance. Using intrusive technology to pursue company policy, rather than to genuinely protect workers, is rarely ever justifiable.

Nationwide's reliance on monitoring technology to ensure in-person attendance is an important example of this, as the method used was not the least invasive, and a worker told us that, to their knowledge, there was little to no consultation. The levels of Nationwide employees' dissatisfaction at the "toxic" workplace highlights the importance of involving employees and unions in the introduction of new monitoring policies so that they do not feel that management is spying on them. Similarly, the installation of secret audio recording devices on buses demonstrates a method completely disproportionate to the supposed aim of 'driver safety' - especially when drivers said that the imposition of constant monitoring made them feel quite the opposite.

Consultation plays an important role in making a workforce feel valued and involved in decision-making, which feeds into a positive and high-performing workplace.[209] The precedent to consult is well established in employment law, as employers must consult employees or their representatives on introducing measures that may substantially affect health and safety at work, including the health and safety consequences of introducing new technology.[210] To address the rights and freedoms issues specific to workplace surveillance, a new duty should be established for employers to consult workers and their representatives before introducing high-risk or other potentially invasive technologies in the workplace. This threshold could be drawn from the ICO's guidance on examples of processing likely to result in high-risk that require a DPIA, given the contextual similarities. Many of these examples specify risks that arise in employment, such as data processing at the workplace; data processing in the context of home and remote working; processing location data of employees; processing of biometric data including facial recognition systems and workplace access systems and identity; using technologies such as AI, machine learning and deep learning; and large-

209 Involving Your workforce In Health And Safety - Guidance For All Workplaces, 2015, Health and Safety Executive, accessed 29 August 2024, https://www.hse.gov.uk/pubns/priced/hsg263.pdf 8.
210 Consulting Employees On Health And Safety' 2013, Health and Safety Executive, Accessed 29 August 2024, https://www.hse.gov.uk/pubns/indg232.pdf

scale profiling.[211] If the processing is risky enough to potentially have a detrimental impact on workers, then they should be consulted in whether it should be used.

Some level of consultation is always encouraged during the DPIA process. Although ICO guidance stipulates that workers should be consulted during a DPIA unless there is a good reason not to, this is not a legal requirement.[212] Further, this process primarily focuses on documenting the risks to privacy and data protection rights. A consultation is a more open forum for employees to express a wider range of concern and, if done properly, can make them feel heard and considered. For that to happen, consultations need to be meaningful processes and not just a formality.

Establishing a new right to consultation for the introduction of high-risk or other potentially invasive surveillance technologies reflects calls from unions for increased consultation rights,[213] and is a key opportunity to ensure that the processes are meaningful. For example, the consultation period will vary depending on the complexity of the issue and how many people are being consulted. Employment law generally only requires an employer to consult in good time, rather than setting a time limit.[214] However, in the context of high-risk surveillance technology, it is reasonable to assume that these issues will require more discussion and therefore require a minimum time frame for consultation. There should be a mandatory three month period before announcing the intention to introduce a new technology and being able to introduce it in which the consultation can take place. This would ensure that employees were granted enough time for them to have a proper consultation process and not rush their feedback, as well as giving employers enough time to reflect upon employees' input.

Although consulting workers and their representatives on technology in the workplace is important, it is not a sufficient basis for employers to introduce intrusive tracking tools. While it is important for employees to be meaningfully consulted in the consideration of these technologies and to be informed on how collected data will be used, these guardrails do not eliminate the harm inherent in privacy-invasive technologies.

While location tracking can play an important role in health and safety, such as for workers on a construction site, it is crucial that employers adhere to the principles

211 Examples Of Processing 'Likely To Result In High Risk' ICO, accessed 2 September 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

212 How Do We Do A DPIA?, ICO, accessed 29 August 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7

213 Intrusive Worker Surveillance Tech Risks "Spiralling Out of Control" Without Stronger Regulation, TUC Warns, Trades Union Congress, 28 February 2022, Accessed 29 August 2024, https://www.tuc.org.uk/news/intrusive-worker-surveillance-tech-risks-spiralling-out-control-without-stronger-regulation

214 'Consulting Employees And Representatives: When Consultation Is Required', ACAS Accessed 29 August 2024, https://www.acas.org.uk/consulting-employees/when-consultation-is-legally-required.

of data minimisation and purpose limitation so that the minimum amount of personal data is only collected for specific, legitimate purposes. This also applies to cameras in vehicles. While there may be some benefits to drivers having video monitoring in their cars – such as verifying an insurance claim in an accident – it is rarely justifiable to have these cameras recording in the same car when a driver is picking up their family. There must be clear boundaries that differentiate between legitimate business needs and personal privacy. For example, data storage and access should be limited to key incidents, such as accidents or security breaches, rather than enabling constant AI or boss monitoring. Access to personal data must be restricted to specific, necessary circumstances in order to protect privacy and autonomy. Finally, surveillance should never be disguised as a health and safety measure. When employees feel they are being spied on by bosses, rather than genuinely protected for their health and safety, it creates a hostile work environment.

When it comes to data use, what matters is necessity, proportionality, and purpose. If monitoring technologies are introduced for a legitimate purpose but then reveal that an employee is engaging in gross misconduct, it may be possible for this data to be used in disciplinary proceedings. However, given the potentially intrusive nature of these types of data, particularly location data, this should only happen if there is reasonable suspicion of gross misconduct. The threshold of gross misconduct could reflect well-established principles in employment law, such as suspected fraud, physical violence, serious lack of care to their duties or other people ("gross negligence"), or serious insubordination.[215] For example, it might be reasonable for location data to be used in a disciplinary hearing to prove a construction worker was spending hours off-site without authorisation. However, it would not be appropriate to use this data to discipline them for minor infractions. Defining this threshold in the context of workplace surveillance would allow employers to use available evidence in serious cases while preventing inappropriate use of worker data.

In The Workspace

Drivers are among the groups most heavily impacted by forms of surveillance that span both their working and private lives. This is particularly in the case of audio and video monitoring, the latter of which has been criticised by the Communication Workers' Union for not only violating individuals' privacy, but creating a disincentive to attracting new recruits to an already suffering industry. Driver-facing cameras, in particular, make drivers feel surveilled and can be abused by employers as part of

215 Types Of Dismissal, ACAS, accessed 3rd September 2024, https://www.acas.org.uk/dismissals/types-of-dismissal

disciplinary proceedings.[216] This is only exacerbated when they are on 24/7. When these technologies are introduced legitimately, it is important that an employee receives clear details about why it is being introduced and the purpose of said tracking, which the Article 29 Working Party recommends is displayed prominently in every vehicle.[217] Despite the risks posed to drivers, it is clear that many employers have chosen to ask for forgiveness rather than permission when using intrusive technology, such as in the case of Addison Lee and bus drivers represented by Unite.

Maintaining a distinction between work and home life is crucial to prevent surveillance technologies from creeping further into people's private lives. Employees allowed to use work vehicles for their own use outside of work hours should be able to switch off a GPS or other location tracking device when they clock off shift. This is not possible when, for example, a tracking system is tied to the ignition. If monitoring technology is used, employees should receive instructions and any required training on how to disable it to support them in keeping their work and personal lives separate. Even if an employer can prove that GPS monitoring is justified, such as for anti-theft purposes to improve the chances of recovering a stolen vehicle, the tracking device must be used exclusively to monitor the vehicle when needed and not the employee. However, this becomes increasingly challenging when work and personal use of the vehicle overlap, complicating the separation between professional life and private life.

Geolocation data can be revealing and is considered high risk in nature, especially as the boundary between home and work life becomes increasingly blurred. It can disclose some of the most intimate details of someone's life, such as whether they've been to a place of worship or a healthcare appointment. GPS tracking is therefore not just about tracking someone's live location. If used pervasively, it gives bosses a way to know where an employee is outside of work and what they are doing in their personal life; "a pervasive intrusion for which the worker has no opt-out choice in his private sphere".[218]

Tying location data to job functions can prevent employees from properly carrying out their duties. When workers can only log their activities within geofenced zones, it can reduce their autonomy and flexibility and be potentially detrimental to the quality of care they provide. For instance, carers using Birdie have to verify their location through a GPS/QR code login at the client's home to start their shift. This

216 Final agenda for Scottish Trade Union Congress 127th Annual Congress, Mike Arnott, 2024, https://www.stuc.org.uk/resources/final-agenda-2024-digital.pdf 31.
217 Guidance Note: Employer Vehicle Tracking, Data Protection Commission, May 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-09/Employer%20Vehicle%20Tracking_May2020.pdf 4.
218 'Just More Surveillance': The ECtHR And Workplace Monitoring, Michael Molè and David Mangan, September 14th 2024, https://journals.sagepub.com/doi/10.1177/20319525231201274?icid=int.sj-full-text.similar-articles.1 696.

requirement prevents them from beginning work off-site, which limits their ability to complete necessary tasks in the most efficient order. For example, a carer might need to pick up groceries for a client, and it could be more time-efficient to go to the supermarket first if it is on the way to the client's home. However, a location verification requirement would force the carer to travel to the client's home first, then to the supermarket, and back to the client's home, resulting in unnecessary travel time that impacts the amount of work a carer can complete in a shift. These restrictions could reduce a carer's ability to provide timely and efficient care, ultimately impacting the client, who is likely to be a vulnerable individual.

The accuracy of location data can also cause problems. GPS may register a location incorrectly, which can lead to workers being unfairly penalised if their reported locations do not match authorised areas.[219] This could result in denied payment, other disciplinary action, and a breakdown in trust between employees and bosses.[220] Employers should recognise the far-reaching impacts of surveillance technologies from employees to clients, and therefore, use these technologies only when absolutely necessary and make human checks before making these kinds of decisions in accordance with Article 22 UK GDPR rights.

Behaviour Shaping Surveillance

Any employer wanting to monitor workers must do so in line with data protection law, which begins with identifying a lawful basis.[221] The GDPR sets out six bases: employee consent, performance of a contract, compliance with a legal obligation, protection of the vital interests of an individual, performance of a public task, or the employer's legitimate interests.

Legitimate interest tests are a well established balancing exercise and often the primary lawful basis that employers opt for when processing employee data. There are some restrictions around what constitutes a legitimate interest, as the data processor (in this context, the employer) must be able to demonstrate that the monitoring is necessary to achieve the legitimate interest. The ICO says that:

> *"This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. [...] It is not enough to argue that processing is necessary because you have chosen*

219 Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care, Data & Society, November 2021, https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf 52.
220 Ibid, 17.
221 Data Protection And Monitoring Workers, Information Commissioner's Office, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf 5.

to operate your business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of your chosen methods."[222]

However, legitimate interest tests are not always completed appropriately in the workplace. Criticism has highlighted that what constitutes a legitimate interest "remains uncertain, context-dependent, and prone to abuse" and "changes over time, in different contexts, and across business models", prompting the question of who determines what is considered legitimate and under what circumstances.[223] After all, employers can easily claim that any form of monitoring and surveillance is necessary and proportionate for their business objectives, including productivity, efficiency, and innovation, as they define these purposes themselves. Trade union representatives told Big Brother Watch that surveillance and performance management are often linked to monitoring for fraud detection purposes, and that this is a very difficult guise to challenge or obtain information on.

It is clear that many employers are using software that goes beyond what would be permissible under data protection law. Under the DPA and UK GDPR, employers are required to process data in ways that are fair and transparent.[224] The purposes for which the data is collected, used, retained and disclosed must be specified and not further processed in a way that is incompatible with those purposes.[225] According to the principle of data minimisation, data collected must be adequate, relevant, and limited to what is necessary for the intended purposes.[226]

Systems such as Lightfoot contradict virtually all of these principles. The fairness principle restricts personal data to being processed in a reasonably expectable way, and not in such a way that it has unjustified, adverse effects on data subjects. Location tracking has some valid applications in employment contexts, such as handling liability if an accident occurs. However, an employee would likely not expect for data, such as speed or standstill time, to be fed back to an employer for monitoring purposes. This also implicates the purpose limitation principle where personal data can only be used for a new purpose if this is either compatible with the original purpose, consent is given, or there is a clear obligation or function set out in law, as per ICO guidance.[227] In line with these principles, it may be reasonable for a lone worker on a construction site or member of a mountain rescue team to have

222 A Guide To Lawful Basis, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

223 Bargaining Over Workers' Data Rights: How Unions And Works Councils Can Use Collective Bargaining to Specify Workplace Data Protection Norms, Friedrich Ebert Stiftung, June 2024, https://library.fes.de/pdf-files/bueros/bruessel/21313.pdf 5.

224 Article 5(a) UK GDPR https://uk-gdpr.org/chapter-2-article-5/

225 Article 5(b) UK GDPR https://uk-gdpr.org/chapter-2-article-5/

226 Article 5(c) UK GDPR https://uk-gdpr.org/chapter-2-article-5/

227 Principle(b) Purpose Limitation: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/

their location recorded for health and safety purposes but using this information for another business purpose, such as in a disciplinary hearing, could potentially constitute illegitimate repurposing and a breach of data protection law.

The transparency principle requires organisations to be clear about what data they are collecting, why they are collecting it and how it is being used, yet the case studies show that this is often not what happens in practice. The Lightfoot system, for example, is relatively opaque about the extent of data it collects. This prevents employees from knowing what information is being collected and what it is being used for, exacerbating the power divide between employer and employee in a way that is contradictory to data protection law.

It is clear that many employers using surveillance systems interpret the "necessary" threshold as a "usefulness" one, exemplified by the Lightfoot case study. Although the ICO has issued guidance on data protection rules in workplace monitoring,[228] many of the cases highlighted in this report demonstrate that employers still do not follow the guidance, whether deliberately or through misunderstanding. Therefore, it would be beneficial for the ICO to provide more specific examples of types of workplace monitoring that meet or fall short of the 'necessary' threshold. Additionally, further guidance is needed from the ICO to clarify appropriate examples of legitimate interests in the employment context. Again, the existing guidance is useful but is limited in the examples that it provides. Given that companies are incorrectly interpreting legitimate interests in order to use surveillance technology, such as in the case of Addison Lee, more sector-specific guidance is needed to clarify to employers what is legitimate, and what is not. This in turn will influence the legitimate interests test that feeds into DPIAs, improving transparency and accountability processes for workers to leverage if they suspect surveillance has been introduced illegitimately. Providing more concrete, industry-specific examples would be useful for employers and workers alike, as it would make it harder for employers to misinterpret or bypass regulations and easier for workers to identify when their rights may be infringed upon.

Many of the issues in this chapter also apply to gamification. While gamification can have a place in the workplace, such as in online training programmes for employees,[229] its use in monitoring or manipulating employee performance can conflict with data protection principles, such as transparency, data repurposing, and consent. Despite this framework, it is clear that the vast amounts of data hoovered up by tracking systems are being used to nudge behaviours to increase

228 Data Protection And Monitoring Workers, ICO, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf

229 See for example Paula Bitrián, Isabel Buil, Sara Catalan, Dominik Merli, 'Gamification in workforce training: Improving employees' self efficacy and information security and data protection behaviours', Journal of Business Research, June 2024, 179

robot-like efficiency – often at the expense of safety. Autonomy in the workplace is crucial to workers' well-being. As the ILO highlights, "[a] key facet of autonomy and control over work is related to their ability to choose working hours and break times, as well as to decline certain orders, for reasons such as exhaustion or safety concerns".[230] However, the asymmetrical relationship between a company and its employees can undermine autonomy, which may be further impacted by the effects of gamification. As the level of data protection decreases, so too does workers' self-determination.[231] There are clear implications for equalities and discrimination as well as privacy, given that drowsiness detection estimates have been found to operate specifically poorly on racial minorities and males - the latter of which make up the majority of the driver workforce.[232]

The potential impact of intense gamification on data protection, equality, health and autonomy rights in the workplace demonstrates that it can be irresponsibly implemented by employers. Gamification can create constant competitive feedback loops that push workers towards excessively long hours and high-intensity work, which the ILO views as potentially injurious to health.[233] To address the ill effects of gamified work and constant behavioural nudging from a privacy-by-design perspective, employees should be able to turn off gamification systems while still being able to do their job. Data from workers choosing to use the systems should only be provided to employers in aggregate form. Recorded data should not be used to make any changes to productivity targets, working conditions, or performance expectations for all employees.

230 The Role Of Digital Labour Platforms In Transforming The World Of Work, ILO, February 2021, https://www.ilo.org/publications/flagship-reports/role-digital-labour-platforms-transforming-world-work 177.
231 Daniele Ruggui et al, 'Responsible innovation at work: gamification, public engagement, and privacy by design', Journal of Responsible Innovation, 9:3, June 2024, https://www.tandfonline.com/doi/full/10.1080/23299460.2022.2076985.
232 Ibid, 6.
233 The Role Of Digital Labour Platforms In Transforming The World Of Work, ILO February 2021, https://www.ilo.org/publications/flagship-reports/role-digital-labour-platforms-transforming-world-work 220.

RECOMMENDATIONS

5. Restrict the use of surveillance for behaviour-shaping by preventing the use of location, audio, and video data in enforcing arbitrary performance metrics.

6. Prohibit the use of intrusive location data in disciplinary proceedings unless there is suspicion of gross misconduct.

7. Create a legal requirement to consult staff, their representatives, and trade unions on the introduction of new high-risk or other potentially intrusive AI monitoring and automated decision-making technologies in the workplace.

8. The ICO should issue further examples of what constitutes a 'legitimate interest' in the workplace surveillance context.

9. The ICO should issue further examples of necessity and proportionality tests in the workplace surveillance context.

AI IN HIRING

Artificial intelligence tools, or programs that claim to use AI, are being used by increasing numbers of companies as part of the hiring process. Generative AI now allows recruiters to engage with potential new hires via chatbots and emails, while automated systems are used to triage and filter candidates, and even interview them.[234]

Algorithmic hiring processes are separate from surveillance in the workplace, insofar as they tend to relate to discrete events ahead of starting work, but are nevertheless closely linked as they rely on similar digital sorting and analysis systems to draw conclusions about human beings. Whether used to analyse and rank worker behaviour, or applicant potential, algorithmic systems used to performance manage or in hiring have fundamentally similar logics underpinning them.

However, AI-powered surveillance is potentially more difficult to shine a light on than other forms of surveillance of workers. The impermanence of the applicant-recruiter relationship and frequent lack of transparency about how hiring decisions are made more generally mean that people are usually left in the dark about what has happened between them going for a job and the outcome.

It is the use of AI and automation in assessing candidates CVs, cover letters and responses to tasks and interviews that mirror wider workplace surveillance most closely. AI used in communicating with candidates raises different data ethics issues but bears less resemblance to general workplace surveillance.

Any automated tool that profiles and classifies people, particularly when rooted in AI or machine learning, comes with a risk of bias and discrimination - even if the process is not wholly automated and therefore subject to Article 22 protections. The use case of hiring is no different, and there have been concerns raised about the training of these tools leading to unequal outcomes and disadvantageous candidates who do not meet the machine's standards.[235]

The technology involved in this space can significantly vary in sophistication, from basic robotic processing of CVs to pick out candidates who use certain key words up to AI evaluations of job interviews. This chapter will examine two forms of AI-based hiring and examine the privacy and data risks involved.

234 Top AI Recruiting Tools And Software Of 2024, TechTarget, 23rd January 2024, https://www.techtarget.com/searchhrsoftware/tip/Top-AI-recruiting-tools-and-software-of-2022

235 AI Hiring Tools May Be Filtering Out The Best Job Applicants, BBC Worklife, 16th February 2024, https://www.bbc.com/worklife/article/20240214-ai-recruiting-hiring-software-bias-discrimination

Automated Applicant Triaging

The use of algorithms to score or help filter job applications and screen candidates has become more common in recent years. A software industry survey found that 70% of large businesses in the UK use automated tools to screen applicants, with around 20% of small and medium businesses following suit.[236]

AI and automated tools used by companies to triage applicants are often called Applicant Tracking Systems (ATS) and integrate. There are dozens of companies offering similar tools to hiring managers, but most work in a similar way – processing CVs and applications through their AI system and identifying which match the job description or required competencies most strongly.[237]

Most systems claim to strip out personal data, such as names and addresses, to reduce bias from CV screening – but there is little transparency across providers on how their models are trained.[238] Time savings for recruiters are touted as the big benefit of automated AI, alongside claimed reductions in unconscious bias.

236 Applicant Tracking System Statistics (Updated for Q3 2024), Select Software Reviews, 5th July 2024, https://www.selectsoftwarereviews.com/blog/applicant-tracking-system-statistics

237 CV Screening, Get Staffed, accessed 29th July 2024, https://get-staffed.com/features/cv-screening/

238 CV Screening Software, CiivSOFT, accessed 29th July 2024, https://www.ciivsoft.com/solutions/fiilter/

However, bias can still exist in models, even if identifiable information is removed. In 2018, Amazon was forced to scrap a machine learning powered application screener after it was found to discriminate against women – because it was mostly trained on CVs from men.[239] A 2021 paper from New York University found that even when names were removed from CVs, as well as gender-suggestive words and hobbies, it was possible to write a language model that identified the gender of the person who wrote a CV around 75% to 80% of the time, significantly above the 50% hit rate that would be expected with random guesses.[240] This suggests that there is a reasonable possibility that some language models used to screen CVs could result in gender bias, even unintentionally, if the model is sophisticated enough to self-learn and evolve.

With a significant number of products on the market in the same space, it is not realistic to assess each technology supplier's attitude to human involvement in the rejection of candidates. Taking CiiVSOFT, based in Cheshire, as an example of the approach taken by companies offering ATS tools there appears to be attempts to acknowledge the necessity of a human to be involved in the decision to reject someone from a job.[241] In this case study, the company states candidates deemed unsuitable by the AI would be put into a stream for later human review or rejection, adding that it does not "automatically reject candidates". It appears that the key issue would be how the software was used, and if the recommendations were automatically accepted by human reviewers or subjected to a meaningful review.

There is significant depersonalisation in automated recruitment processes, with goals often being to reduce time spent reviewing CVs. To what degree will vary from company to company, but with a machine triaging CVs and recommending who is rejected or progressed to recruiters, it is not difficult to imagine that in some companies the human in the loop does very little. Rather than a human assess each application holistically, candidates are assessed by machine and evaluated in a certain way, potentially with minimal human input – bearing some similarities to automated productivity tools that are used to evaluate some workers.

HireVue

HireVue is perhaps the most well known and notorious provider of AI-powered recruitment software – best known for its AI led video interviews.[242] Founded in Utah

239 Amazon Scrapped 'Sexist AI' Tool, 10th October 2018, https://www.bbc.co.uk/news/technology-45809919

240 Degendering Resumes for Fair Algorithmic Resume Screening, Prasanna Parasurama & João Sedoc, New York University, 2022, https://arxiv.org/abs/2112.08910v3

241 Job Application Screening, CiiVSOFT + Lever, YouTube, 24th May 2023, https://www.youtube.com/watch?v=xLUAz0ZblXs

242 Video Interviewing Software, Hirevue, accessed 29th July 2024, https://www.hirevue.com/platform/online-video-interviewing-software

in 2004, the company has been subject to significant criticism over its use of AI to assess video interviews and make recommendations to companies on who the best candidates are, including in a 2022 BBC Three documentary "Computer Says No".[243]

HireVue's two main offerings in the realm of candidate evaluation are video interviews, and AI-powered psychometric and technical tests.[244] Often these are used in tandem. The company has a number of UK-based clients including Queen's University Belfast, the Co-operative Bank and Channel 4.

Video interviews

Video interviews on the HireVue platform can either involve a hiring manager or more often be completely virtual, with applicants answering pre-set questions in a sort of long-form video message.[245] It is the virtual interviews that pose the biggest potential risk to privacy and data rights, and are the core of HireVue's offering.
The company claims that its AI first acts as a speech-to-text engine, transcribing answers to written prose.[246] Natural language processing is then used to allow the AI to "understand" the interview answers, before the machine assesses and scores the answers. Candidates are scored against up to 20 competencies chosen by the hiring company, including "adapts to change", "leads others" and "communicates effectively".[247] This scoring is based on 125,000 evaluations of 500,000 video interviews, according to HireVue in its AI Explainability Statement, with the model trained to mimic how human evaluators assessed the training dataset.[248]

Effectively, an AI model processes and then scores a candidate's virtual video interview against a set of competencies set by the hiring company. Candidates are then ranked as top tier, middle tier and bottom, with the system suggesting that top candidates are put through to the next step, middle candidates reviewed by a recruiter for a decision, and low tier candidates reviewed for rejection.[249] The company claims that actual decisions are made by HR staff, rather than AI, but it is clear that the AI has a significant influence insofar that it automatically assesses and ranks candidates.

---

243 Computer Says No, BBC Three, 16th March 2022, https://www.bbc.co.uk/iplayer/episode/m0015gvw/computer-says-no
244 Assessment Software, Hirevue, accessed 29th July 2024. https://www.hirevue.com/platform/assessment-software
245 Video Interviewing Software, Hirevue, accessed 29th July 2024, https://www.hirevue.com/platform/online-video-interviewing-software
246 AI Explainability Statement, Hirevue, April 2024, https://webapi.hirevue.com/wp-content/uploads/2022/04/HV_AI_Short-Form_Explainability_1pager.pdd
247 Video Interviewing Software, Hirevue, accessed 29th July 2024, https://www.hirevue.com/platform/online-video-interviewing-software
248 AI Explainability Statement, Hirevue, April 2024, https://webapi.hirevue.com/wp-content/uploads/2022/04/HV_AI_Short-Form_Explainability_1pager.pdf
249 Ibid

Previously, HireVue used facial and emotional analysis as part of its assessment process, making judgements on candidates based on facial expressions to determine certain traits.[250] This was scrapped in 2021 after significant public outcry, but it was reported that analysis of tone and language choice is still in use. Emotion recognition, particularly when based on facial expression, is widely dismissed as inaccurate and the ICO warned of a high risk of discrimination.[251]

Game assessments

The task-based assessments consist of mini-games to assess candidates' cognitive capabilities, problem-solving skills, tolerance to risk and other emotional attributes, as well as technical evaluations for hard skills such as coding. After completing the tasks, the AI software generates a score for each candidate and takes this into account when suggesting shortlists of the top-ranking candidates

250 Job Screening Service Halts Facial Analysis Of Applicants, Wired, 12th January 2021, https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/

251 'Immature Biometric Technologies Could Be Discriminating Against People' Says ICO In Warning To Organisations, ICO, 26th October 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations

to the recruiters for the next stage of interviews.[252] [253] Scores are generated based on how many levels are completed and their difficulty – with a regression model comparing candidates to a training dataset who undertook both traditional and well-designed psychometric tests as a benchmark.

Candidate skill scores, both for interview and game-based assessments, range from novice, through developing and intermediate, to advanced and expert, and are displayed in a dashboard for recruiters – while candidates can be offered some insight into the AI's conclusions about them if companies wish to offer this.[254]

HireVue's AI Explainability statement is an attempt to offer some transparency about their AI-based assessment of people but it has been heavily criticised for being insufficient.

The Center for Democracy & Technology said that it "mostly fails" in explaining what the AI does.[255] It was specifically criticised for minimal explanation about how the games-based assessments were designed or validated, and a lack of transparency about the full set of competencies it can supposedly assess. Issues were also raised about HireVue's abdication of responsibility for data access rights, as it claims that because companies make the hiring decisions, it is companies who need to fulfil data access rights. However, as the customisation of the platform on a client by client basis is limited, and explainability documents are flawed, candidates' data access rights could be curtailed.

Generic training data is raised as a further issue, as the supposedly large set of training interviews were not tailored to specific industries, potentially limiting the AI's ability to assess candidates for specialised roles – particularly when competencies are exhibited differently in different industries.

Quite clearly, the role of AI, from conducting interviews and assessments to ranking applicants, means that the assessment of competency and skills by the machine will have a significant impact on hiring decisions. There is a strong resemblance between this kind of software, assessing performance in a single instance, and productivity management tools which assess how workers perform in a role over a period of time. Although it is not constant surveillance, it is on the same spectrum and endangers many of the same rights.

252 Assessment Software, Hirevue, accessed 29th July 2024. https://www.hirevue.com/platform/assessment-software

253 AI Explainability Statement, Hirevue, April 2024, https://webapi.hirevue.com/wp-content/uploads/2022/04/HV_AI_Short-Form_Explainability_1pager.pdf

254 AI Explainability Statement, Hirevue, April 2024, https://webapi.hirevue.com/wp-content/uploads/2022/04/HV_AI_Short-Form_Explainability_1pager.pdf

255 HireVue "AI Explainability Statement" Mostly Fails to Explain What it Does, Center For Democracy & Technology, 8th September 2022, https://cdt.org/insights/hirevue-ai-explainability-statement-mostly-fails-to-explain-what-it-does/

POLICY ANALYSIS

To some degree job applicants experience an even greater power imbalance than workers, as they are usually in the situation where there are multiple other candidates – while punishing an employee for challenging high-risk data processing usually has some associated costs. Deciding who to hire can have a significant impact on individuals' lives, and as a result there must be adequate legal frameworks and enforcement, as well as a particular commitment from recruiters to protect data rights and prevent discrimination – particularly as recourse in those situations can often be very limited.

Transparency & Accountability

The use of AI tools, particularly to screen or triage applications, is often opaque. Few companies clarify on rejection that a machine played a significant role in deciding whether someone was suitable for a role or not. Yet the transparency principle of the GDPR requires that organisations are "open and honest with people from the start about who you are, and how and why you use their personal data".[256]

Unless hiring companies are upfront about their use of AI and automation to assess applications and applicants, it is likely that this condition is not being complied with. It will often not be the case that applicants will expect the majority of their evaluation to be done by machine, especially if a company effectively only uses HR staff to rubber stamp decisions. Applicants are legally entitled to know if they are being assessed by a machine, to allow them to decide if they want their personal data used in that way and to ensure that they know how to challenge error properly if they think it has occurred.

The abdication of responsibility from technology providers to hiring companies over data rights, even if the company does not have significant understanding about how AI and the automated models work, is a threat to those rights. Applicants seeking to exercise their right to know what data was processed about them, and how, face being left in the dark if hiring companies are not sufficiently able to provide explanations about how their technology supported recruitment decisions. This is the case with HireVue, and may well be the case with the plethora of ATS systems available. A lack of technical knowledge should not preclude data rights being accessed, and it should be the case that hiring companies understand the technology sufficiently to explain the processing and uphold their legal obligations under Article 22 UK GDPR. Further, technology companies are joint data controllers

256 Principle (a): Lawfulness, Fairness and Transparency, ICO, accessed 29th July 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/#transparency

and also share legal responsibilities in many scenarios, including to process data subjects' right of access requests.

One step towards bridging the transparency gap is by creating an obligation for companies deploying AI systems to perform algorithmic impact assessments (AIAs). AIAs are a tool for assessing the potential societal impacts of an AI system before it is used and are a way to create greater accountability for the design and deployment of AI systems.[257] While DPIAs can protect rights beyond privacy, such as non-discrimination, they predominantly address the risks to these rights in relation to data processing rather than algorithmic processing specifically. As such, the scope of DPIAs does not extend to a wider consideration of possible harms that AI can give rise to in the workplace and are limited in the extent to which they can promote accountability and ensure fairness.[258]

The IFOW explains how AIAs focus on "key decision-making points in the design and deployment of an algorithmic system, requiring careful assessment of risks and impacts before real-world use".[259] AIAs build upon well established data protection, equality and human rights impact assessment methodologies, shaping them to specifically address the unique harms that algorithms can pose. Anyone performing an AIA would be required to conduct a rigorous ex ante assessment and evaluation of risks, impacts and anticipated impacts throughout development and deployment so as to future proof the model against unforeseen risks and address issues as they arise.

This process would require stakeholder engagement to support better understanding of real-life impacts as they evolve. In addition to ensuring rigorous evaluation, the dynamic nature of AIAs enables better articulation and measurement of risk; as well as supporting accountability, transparency and explainability through extensive record keeping. In this way, AIAs specifically allow for a holistic and context-specific approach that can prevent harm caused by ADM and AI in the workplaces in ways that DPIAs may not be able to.

An appropriate threshold for triggering an AIA could be drawn from DPIAs, which are required when personal data processing is likely to result in a high risk to an individual's fundamental rights and freedoms. The European Data Protection

257 'Algorithmic Impact Assessment: A Case Study In Healthcare', February 2022, The Ada Lovelace Institute, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/02/Algorithmic-impact-assessment-a-case-study-in-healthcare.pdf 14.

258 'Algorithmic Impact Assessments: Building A Systematic Framework Of Accountability For Algorithmic Decision-Making', Institute for the Future of Work, November 2021, https://cdn.prod.website-files.com/64d5f73a7fc5e8a240310c4d/64d5f73b7fc5e8a240311342_IFOW-AIA%20Policy%20Paper%20(v8-18.03.22).pdf 8.

259 'Algorithmic Impact Assessments: Building A Systematic Framework Of Accountability For Algorithmic Decision-Making', Institute for the Future of Work, November 2021, https://cdn.prod.website-files.com/64d5f73a7fc5e8a240310c4d/64d5f73b7fc5e8a240311342_IFOW-AIA%20Policy%20Paper%20(v8-18.03.22).pdf 8.

Board has confirmed that decisions that "similarly affect" individuals include ones that affect an individual for a prolonged period or have financial impacts, which the IFOW notes would include recruitment, pay, work allocation, and terms and conditions, as well as ones that impact job quality, such as social scoring in recruitment algorithms, systematic monitoring, the use of biometric data and/or location-based tracking – all of which meet the high risk definitions provided by the ICO and Article 29 Working Party guidance.[260]

Many of the case studies explored in our report emphasise the need for stronger and clearer processes to protect workers from the harms that arise from data-driven technologies in the workplace. Additionally, the UK government has acknowledged the potential of AIAs by piloting them in other sectors, such as the healthcare systems.[261] Despite the need for extra protections and clear value AIAs have, there is no current legal requirement for them to be conducted prior to any implementation of AI or algorithmic-based technologies. Further, there is no outline of the essential requirements necessary to complete one. It is important for AIAs to be made a legal requirement and for accompanying guidance to be issued to outline a framework of what an AIA should cover, including a detailed description of the system, a holistic assessment of the possible risks to worker privacy, equality, autonomy and dignity, measures taken to address those risks, as well as safeguards and mechanisms to ensure regulatory compliance. This would simultaneously support employers in assessing the possible risks of deploying AI in the workplace whilst holding them accountable in the instance risks occur.

In order to support transparency and accountability processes, there must also be a duty upon employers to make AIAs available to employees, unions, and other representatives upon request. This process can help employees and job seekers understand what systems are in place and what impact they have while supporting employers in evaluating and addressing the risks of such systems, thereby creating an important procedural safeguard concerning the use of AI and automated decision-making (ADM) in the workplace.

This accountability should also apply to bias and discrimination stemming from AI and algorithmic decision-making. Despite it being well established that AI and other automated systems can give rise to discrimination, this has not stopped bias resulting from their use.[262] Although the onus should be on the organisation using

260 'Algorithmic Impact Assessments: Building a systematic framework of accountability for algorithmic decision-making', Institute for the Future of Work, November 2021, https://cdn.prod.website-files.com/64d5f73a7fc5e8a240310c4d/64d5f73b7fc5e8a240311342_IFOW-AIA%20Policy%20Paper%20(v8-18.03.22).pdf 8.

261 UK To Pilot World-Leading Approach To Improve Ethical Adoption Of AI In Healthcare, Department of Health and Social Care, 8 February 2022, https://www.gov.uk/government/news/uk-to-pilot-world-leading-approach-to-improve-ethical-adoption-of-ai-in-healthcare

262 See for example Centre for Data Ethics and Innovation 'Review into bias in algorithmic decision-making', November 2020, https://assets.publishing.service.gov.uk/media/60142096d3bf7f70ba377b20/

the technology to prove that it is not biased rather than on the individual to prove that it is, this is not currently the case. In an analysis of AI, ADM and equality law, legal experts from Cloisters chambers found that:

> *"The existing legal framework giving effect to the principle of non-discrimination in the workplace is, in principle, capable of tackling discriminatory uses of AI and ADM, but can only be used effectively where transparency is guaranteed."*[263]

Given the lack of transparency around these systems, it is clear that more protections are needed to protect workers from the discriminatory impact of AI and automated decisions in the workplace. Further, there is currently a grey area where technology suppliers attempt to devolve responsibility for biased data outcomes to clients, while companies themselves may evade accountability by blaming the technology. Even when both organisations bear responsibility, the blurred lines of that responsibility can be difficult for individuals to navigate.

To address this, a legal duty should be placed on end user companies to demonstrate that there is no discrimination in the data processing prior to deployment through the AIA process. This suggestion has been made in applicable contexts, such as the Centre for Data Ethics and Innovation's recommendation that public bodies should have a legal obligation to test their algorithms for any direct or indirect discrimination under the Public Sector Equality Duty.[264]

Under existing laws, both the software developer and the end user may be considered joint data controllers, which means they share responsibility for how personal data is processed. While software developers should conduct and provide evidence of thorough testing for bias, there can be differences between the data on which a model is trained and ultimately used. To address this gap, the end user should be responsible for demonstrating that the algorithm does not introduce bias in their specific use-case. Organisations should use dummy data to avoid effectively deploying the technology on worker data. In addition to addressing contextual harms, this could also incentivise developers to perform thorough bias testing, as organisations would be more likely to purchase and trust software that has undergone rigorous evaluation and is more likely to pass their own bias tests.

Therefore, we recommend that an AIA framework includes a requirement for

---

Review_into_bias_in_algorithmic_decision-making.pdf

263 Technology Managing People - the legal implications, Robin Allen QC and Dee Masters, March 2021, https://www.tuc.org.uk/sites/default/files/Technology_Managing_People_2021_Report_AW_0.pdf 52.

264 See for example Chapters 1 and 2 of Review into Bias in Algorithmic Decision-Making - Summary, Centre for Data Ethics and Innovation, 27th November 2020, https://assets.publishing.service.gov.uk/media/5fbfbd0de90e077ee2eadc53/Summary_Slide_Deck_-_CDEI_review_into_bias_in_algorithmic_decision-making.pdf

companies to conduct bias testing of AI or other automated systems that are likely to be of high-risk to proactively demonstrate their full compliance with the Equality Act 2010. To guide these tests, the Government should issue guidance to clarify the Equality Act responsibilities of organisations using AI and automated decision-making systems, including guidance on the lawfulness of bias mitigation and testing techniques – a recommendation which reflects calls from the Centre for Data Ethics and Innovation's proposed roadmap to tackle bias in algorithmic decision-making.[265] The guidance should provide clear standards and best practices for organisations to follow, ensuring that AI systems used in employment-related decisions comply with existing equality and non-discrimination laws. By doing so, the Government would help to protect workers from potentially biased or unfair automated processes, while reducing ambiguity and legal risk for employers.

Emotion Detection Technology

Emotion detection technology has been widely criticised by privacy campaigners and trade unions alike. It has been criticised as inherently tied to mass surveillance and founded in pseudoscientific concepts, with the potential to threaten privacy rights, restrict access to services and opportunities, and undermine equality, non-discrimination, and freedom of expression.[266]

Emotion detection technology is ripe for misuse in the hiring context. It could also be used to manipulate or pressure candidates, such as assessing their stress levels to see how they handle pressure, which would not just be unethical but also lead to unfair evaluations. Candidates who know their emotions are being monitored may feel anxious or uncomfortable, which could negatively impact their performance during interviews as well as their overall perception of the company. Technical biases could build systematic bias into hiring processes, detrimentally impacting access to work for minority groups. It often relies on simplistic, ethnocentric and normative parameters, risking inaccuracy and discrimination against minority ethnic groups[267] and disabled and neurodivergent people.[268]

In its report on the human rights implications of emotion detection technology, ARTICLE 19 highlights the highly invasive nature of surveillance created by the

265 Review Into Bias In Algorithmic Decision-Making, Centre for Data Ethics and Innovation, 27th November 2020, https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making

266 Emotion Recognition Technology Report, Article 19, accessed 6 August 2024, https://www.article19.org/emotion-recognition-technology-report/

267 European Data Protection Supervisor, Tech Dispatch on Facial Emotion Recognition, 26th May 2021, https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf 3

268 Report Of The Special Rapporteur On The Rights Of Persons With Disabilities, Human Rights Council, 28th December 2021, https://documents.un.org/doc/undoc/gen/g21/397/00/pdf/g2139700.pdf 15-16.

"mass collection of sensitive personal data in invisible and unaccountable ways, enabling the tracking, monitoring, and profiling of individuals, often in real time".[269] The report calls for a complete ban on the technology, citing extreme risks of discrimination, inconsistency with international human rights standards, and its staggering potential to affect people's lives and livelihoods – including in the workplace.[270] Many trade unions share this stance, as union representatives told Big Brother Watch that emotion tracking is so open to misuse that there are no viable applications in the employment context. This position was reflected in the Trades Union Congress's proposed Artificial Intelligence (Employment and Regulation) Bill that would prohibit the use of emotion recognition technology in high-risk decision-making contexts that may be detrimental to a worker, employee or jobseeker.[271]

Automated Decision Making

Meaningful Human Involvement

There should be no place for ADMs in the hiring process – a human must ultimately make decisions with such significant effects at all times. Currently, UK data protection law provides some protection against automated decision-making, where there is no human intervention in a decision that has legal or similarly significant effects under Article 22 of the GDPR.[272] As explored in the productivity tracking chapter, the vague definition of 'human intervention' creates a legal loophole. The meaning of 'similarly significant effect' is also unclear – while the ICO confirms that hiring decisions are likely to qualify as such, this is again guidance rather than law.[273] Legal clarification is needed to specify that a decision based on solely automated processing is one that involves no meaningful human involvement.

If ATS systems are used to automatically reject applicants, or HireVue's rankings on who to reject are applied without a human check, it is very likely that Article 22 applies and this would qualify as a solely automated decision. To process data in this way an organisation must be able to show that using ADMs is authorised by law, is necessary to perform a contract or has the data subject's explicit consent.

---

269 Emotional Entanglement: China's emotion recognition market and its implications for human rights, ARTICLE 19, January 2021,https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf 15.

270 Emotional Entanglement: China's emotion recognition market and its implications for human rights, ARTICLE 19, January 2021,https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf 24.

271 AI Bill: Part 4: Prohibition On Detrimental Use Of Emotion Recognition Technology, Trades Union Congress, https://www.tuc.org.uk/node/529750

272 Rights Related To Automated Decision Making Including Profiling, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib4

273 Ibid

The latter is the only condition that could realistically apply in the circumstances of a job application, and there are serious questions over whether consent can be freely given due to the power dynamics between an applicant and a potential employer. Would an employer have a genuine second track, to ensure no detriment, for applicants refusing to be subject to ADM? This is not a likely scenario given the costs of a two-track process, in which case consent could not be considered to be lawful. As noted earlier in this report in relation to ADM, one of the most important and urgent changes needed to UK GDPR in order to safeguard against unfair AI decision-making is to amend Article 22 to ensure that human involvement in significant decisions is meaningful, in order to exempt a decision from the prohibition on solely automated decisions. This would require companies to ensure a meaningful human involvement in ADM contexts and understand what this requires, whereby there is a computer in the loop of human decision making rather than merely vice versa.

Significant Decisions

The other qualifying factor for Article 22 protections depends on whether a decision has legal or similarly significant effects.[274] The meaning of "similarly significant effect" is vague, although the ICO identifies a hiring decision as one such example.[275] There are a number of other examples that could meet the threshold of 'significant' in the context of workplace surveillance as management decisions are increasingly fed by performance metrics. For instance, data-driven technologies could make or support decisions to put an employee on performance review or give them a disciplinary point. Another example might be the use of ADM to set higher and higher targets, pushing workers' performance beyond practical limits and creating unreasonable and unsafe workloads. Although some automated decisions may not have an overt legal effect, they could potentially impact an employee's career progression, professional reputation, cause distress, and even impact their physical health by pushing workers carrying out physical tasks to their limits.

ICO guidance on rights relating to ADM offers some examples of similarly significant effects, but only one of these is relevant within the workplace context (i.e. e-recruiting practices in e-hiring).[276] The only example given in the guidance on data protection and workplace surveillance of a similarly significant effect is

274 Rights Related To Automated Decision Making Including Profiling, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib4

275 Ibid

276 Rights Related To Automated Decision Making Including Profiling, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib4

automated productivity monitoring, as it would impact pay.[277] Given the ambiguities surrounding the threshold and the extensive use of ADM in the workplace, the ICO should issue further sector-specific examples to clarify what sorts of automated decisions engage Article 22 rights within the workplace context. This would help workers and unions in challenging inappropriate use of ADM whilst simultaneously supporting employers in knowing when they can and cannot introduce automation to workplace tasks and processes.

RECOMMENDATIONS

10. The Government should issue guidance that clarifies the Equality Act responsibilities of organisations using AI and automated decision-making systems, including guidance on the lawfulness of bias mitigation and testing techniques.

11. The ICO should issue further workplace-specific guidance of what constitutes a 'similarly significant effect' in relation to Article 22 rights.

12. Parliament should prohibit the use of emotion recognition technology.

277 Data Protection and Monitoring Workers, Information Commissioner's Office, 4th October 2023, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf 27-28.

BigBrotherWatch.org.uk