Published on *The National Law Review* https://natlawreview.com

Workplace Monitoring – New Guidance from the ICO

Article By:

Intellectual Property and Technology Squire Patton Boggs

Workplace monitoring has become a matter of particular contention in recent years. In a world where remote and hybrid working practices have become the norm, many employers have concerns about what their employees are actually doing while 'at work' elsewhere. This has led to an increasing amount of discussion about monitoring employees who are working from home and where the acceptable parameters rest.

Trade Unions are concerned that the increase in workplace monitoring and surveillance is pandemic-induced and that whilst surveillance technologies are to some extent 'accepted' in the workplace, this does not automatically justify their usage in a way that would fundamentally breach employee's privacy rights. Indeed, 70% of respondents to a recent ICO survey reported they feel it would be intrusive to be monitored by an employer, with one in five stating they feel they have been monitored by an employer. "Feeling monitored" is an odd concept on which to base action, however, since anyone who works for someone else is necessarily monitored to some extent – did he come into work, did he do his contracted hours, was his productivity acceptable, is he doing something inimical to our best interests, etc? These are issues any employer is entitled to reassure itself upon and not interests which

any employee could reasonably find (in principle, at least) either objectionable or surprising. The concerns lie at the margins, where monitoring does or may pick up irrelevant or unnecessary data or information which the employer cannot reasonably say it has a legitimate right to see.

Workplace monitoring can include:

- Webcam recording and screenshots from virtual meetings.
- Monitoring timekeeping or access control.
- Keystroke monitoring to track, capture and log keyboard activity.
- Productivity tools to log how workers spend their time.
- Tracking internet activity, often to assess whether employees are acting in accordance with acceptable usage policies.

There is even some degree of ‘monitoring’ in the use of RAG statuses on instant messaging features which will often tell you when an employee was ‘last seen’ online. In its most basic form, some would see this as workplace surveillance that could be used by an employee’s managers and even peers – despite it not necessarily being a useful indicator of an employee’s performance.

The Trade Union Congress asserts that assessing employees in this way is an example of employers putting too much decision-making in the hands of technology. The methods of monitoring imposed by the introduction of AI systems in the workplace are forming the basis of important decisions relating to hiring and performance management, opening up employees to inadvertent or systemic discrimination in the operation of those systems.

The ICO’s Commissioner for Regulatory Policy has spoken about the potential negative impact upon employee wellbeing if

monitoring is not conducted lawfully. The ICO's guidance does primarily place responsibility on the employer and stresses the importance of its ensuring that employees are aware of their privacy rights in an employment setting, with a view to 'empowering' employees to 'challenge intrusive practices.'

Admittedly, the ICO has a bit of a tough gig with this one – balancing employees' privacy rights with the commercial need for employers to be able to monitor their employees. In response to these growing concerns, the ICO has refreshed its guidance on workplace monitoring.

Here are some key takeaways from the ICO's most recent guidance:

- **Pay practical attention to Article 8**: Whilst data protection legislation is key, the interplay between data protection laws and the Human Rights Act is important. Moving into a hybrid working environment, Article 8 of the European Convention on Human Rights, as brought into UK law by the HRA (respect for private and family life) is pretty central to discussions around employee monitoring. The expectation which an employee has around their privacy at the office will be different from the expectations they may reasonably have at home.
- **There are 6 lawful bases for monitoring employees – try to get it right first time round**: In order to lawfully monitor employees, the employer must identify **at least one** lawful basis for doing so. If you can identify more than one, then even better, but try and choose correctly in the first instance as it can be difficult to change horses on this without a good reason at a later point.
- **A Data Protection Impact Assessment (DPIA) is a good idea**: Not only is it a helpful compliance and accountability tool

but it can help employers identify and manage the risks that inevitably turn up when monitoring is being undertaken. In any event, employers must complete a DPIA where processing of personal data would cause high risk to workers' and other peoples' interests.

- **Trust and confidence**: Aside from the legality of monitoring employees at work, employers also need to keep in mind the message they send out to staff if workplace monitoring is introduced. It can impact the trust between employee and employer and has been shown to affect employee wellbeing if not properly implemented. As usual, communication with employees is key. A basic plank of this will be that in most cases, something which doesn't require to be monitored in the workplace does not need to be kept an eye on when the employee is WFH. The reverse is also true – if you trust me to WFH without monitoring a particular function or activity, why do you need to do so in the office?
- **Answering the obvious questions**: Employees are bound to ask their employers why they're being monitored. Defining the purpose of workplace monitoring is not just a mechanism of providing employees with an answer, but it is a key principle of data protection law. However, as is a common theme throughout data privacy advice, just because monitoring is documented or explained does not automatically render it lawful or non-excessive.
- **Including the workforce in the decision-making process**: This is not a 'must do', but employers should ideally seek their workers' views if they plan on introducing monitoring into the workplace, and this step should not be skipped unless there is a good reason. This is a smart move from a risk management perspective, as involving the workforce from the start can prevent future complaints arising.
- **Going undercover**: Covert monitoring is difficult to justify in

the workplace, and employers would need to demonstrate an exceptional circumstance for doing this, e.g. to help identity the perpetrator of thefts in the workplace. However, for 'business as usual' practices, it is advisable for employers not to entertain covert monitoring. If employers can demonstrate an exceptional circumstance, then they must follow the guidance issued by the ICO.

Despite the obvious risks of not conducting workplace monitoring appropriately, such as damaging employer/employee relationships, there are also specific consequences that can be imposed by the ICO including some very hefty fines for 'excessive monitoring'. Further to this, disgruntled employees can also seek their own recourse through the courts.

We would recommend that employers who do, or intend to, conduct workplace monitoring have a thorough read-through of the ICO's latest guidance. It is rumoured that we will also be seeing a draft AI and Employment Bill in early 2024 – something to keep an eye out for! What the Bill will cover remains to be seen but we can be clear that there is one point it will miss – that where issues of fairness, proportionality, reasonableness and other fair dismissal considerations are concerned, artificial intelligence is no substitute for the real thing. Many of the potential risks from employee monitoring arise less from the monitoring itself and more from the decisions which may be made on the back of it. So your activity tracking flags up that your employee is looking at porn during his working day, for example. Very bad news in the office, obviously, but if that gets him through his working day at home without any obvious adverse impact on his output, can your position genuinely be the same? Employers can't trumpet the flexibility of their hybrid working arrangements and yet still get in a tizzy if the remote-working employee steps offline for a period during the day. And so

on, since the possible permutations of facts and circumstances are endless and each one requires individual consideration, however the employer has obtained its “evidence”.

Amelia Durkin also contributed to this article.

National Law Review, Volume XIII, Number 303