19 May 2020 - **Ed Houghton, Head of Research and Thought Leadership**

Coronavirus and the workforce: 'workplace' monitoring and surveillance

Why organisations must exercise caution around the use of technology in their response to COVID-19

The COVID-19 pandemic has caused many organisations to radically shift the way they organise and manage work. Organisations with roles that are commonly office-based have shifted towards supporting homeworking, using technology to enable workers to continue to work where possible. Much debate has centred on the immediate positives and negatives of this for workers, including shifting work-life balance, and mental and physical wellbeing. However, surprisingly little time has been spent exploring another key risk to workers: the potential data privacy and security risks that come with 'working from home'. This is commonly considered under the catch-all phrase 'monitoring and surveillance in the workplace'.

The lack of discussion on this is perhaps surprising. A common gnomic rolled out in articles about technology and its impact is that of Professor Melvin Kranzberg, who in 1986 outlined the unintended consequences of technology in social ecosystems, and the risks that can arise when using technology in different contexts: something quite apt in the current setting.

> 'technology's interaction with the social ecology is such that technical developments frequently have environmental, social, and human consequences that go far beyond the immediate purposes of the technical devices and practices themselves… technology can have quite different results when introduced into different contexts or under different circumstances.'

In short, while COVID-19 may present an interesting opportunity to use technology to

enable homeworking and monitor working practices, it also presents considerable risks that may give rise to many unintended consequences. This could radically shift how organisations apply technology today and into the future.

What is workplace monitoring and surveillance?

Monitoring and surveillance in the workplace involves any form of observation or supervision of workers. In recent years, software that monitors internet use, calendar use, and keyboard strokes has become more commonplace. Spot checks or active monitoring (for example, randomly scanning emails for keywords or phrases) can now be carried out fairly regularly using modern software.

Earlier this year a high-profile case at Barclays highlighted the risks associated with employee monitoring. New technologies, while promising greater management and insights, can have a serious impact on trust, employee relations, and employee morale.

Clearly, during the current crisis there are important considerations that must be taken into account. There may be perceived value in increasing the extent to which employees are monitored while they are working away from the office, but there are also real risks that must be considered.

Is employee monitoring appropriate during COVID-19?

Under normal conditions many employers may have legitimate cause for actively monitoring workers. This may include workers handling stock, or those working in high-pressure or high-stakes roles. A key concern in these contexts is security, but there are also productivity benefits to monitoring and using the resulting data appropriately.

However, COVID-19 presents a unique set of challenging circumstances within which monitoring may occur. Enhancing productivity, or at least maintaining it, may be a potential driver for monitoring – even though it may take some time for homeworkers to achieve of pre-COVID-19 productivity. An important consideration must be: what will monitoring provide management and HR that can't otherwise be understood through effective line management?

Employees will consider monitoring in the home to be highly invasive. Software that records videos or monitors audio is likely to cross the line of privacy that employees expect when working from home. Other technology such as screen capture and keyboard tracking is also likely to be considered overly intrusive.

Many employees will be using their own device to work at home, for example, when accessing work files and emails. Clearly organisations should not use technology to scan or access personal files of employees, nor should security (for example, anti-virus

software) actively access these files. This again is highly inappropriate.

COVID-19 may present a new case for increasing employee monitoring, but employers must consider the benefits and drawbacks of implementing monitoring technology.

Steps employers can take to protect workers, and the organisation

A key challenge at present may come from the desire to make the best use of technology to support workers at home, without considering the long-term implications of initiating large-scale monitoring. As well as the obvious risks to workers, employers that rush into adopting new monitoring practices may risk breaching employees' fundamental rights to privacy. As well as the legal ramifications resulting from any breach of the General Data Protection Regulation (GDPR), which may be enforced by the Information Commissioner's Office (ICO), employee trust, wellbeing and morale can also be severely affected.

There are however useful principles which employers should look to consider which have been described by the ICO in its guide to the GDPR:

- Expectations of privacy: Employee expectations must be considered when any monitoring technology is being considered. During COVID-19 workers at home are likely to have far higher expectations of privacy which must be considered.

- Ensure safeguards are in place: these safeguards should ensure that any personal data obtained through monitoring is used only in the manner originally described to the employee; and accessed only by trained employees who observe the confidentiality and security requirements of the data.

- Fair processing of information: employees must receive information detailing how monitoring data will be used. Employers should outline why the monitoring is being carried out, which policy it applies to, how information will be used and to whom it will be disclosed, and the safeguards being used to mitigate against risks to personal data.

- Monitoring should be proportional and have a legal basis: legitimate reasons for collecting data must be balanced against employee rights and expectations for privacy. A proportionality test should be carried out.

- Impacts should be assessed, and risks mapped: Monitoring should only occur when a formal data protection impact assessment (DPIA) has been completed.

While technology may present the opportunity for monitoring and surveillance, it's clear that the benefits must be weighed up against the drawbacks. Clearly technology is currently connecting workers and enabling work for many in a way that even a decade ago

was not possible. Organisations that would have stopped operations are today keeping their lights on, even if those lights are in the homes of workers and not the office. We should both celebrate and be cautious of technology for its ability to support people and business through this crisis. As Kranzberg outlines in his seminal work, the decision of how we apply it is ours to make: 'technology is neither good nor bad, nor is it neutral'.

Explore our related content

Surveillance in the 'data-driven' workplace: is this the new norm?