ROPES & GRAY

CORONAVIRUS
INFORMATION & UPDATES

May 7, 2020

Life After Lockdown: The Challenges of Creating a Safe (and Smart) Working Environment in the UK

Attorneys
Juma Weeks

The daily 5pm Downing Street briefings have become routine in most households across the UK, perhaps giving *some* much-missed structure to what are very unusual times. As the nation carefully follows every word from Government for signs of a relaxation of, or perhaps rather ambitiously, an end to, lockdown, and with Boris Johnson confirming that the UK is now "past the peak", employers are starting to consider what a return to the workplace might look like. In Europe and the USA, where restrictions are already easing, the use of tech is proving to be one of many important tools to facilitate a safe return to the workplace. Below we consider three possible tech options that employers could use, and the potential privacy issues associated with them.

<u>What tech is out there?</u>

Thermal-imaging cameras

One option is the use of thermal-imaging cameras or so-called fever-screening solutions at the entrance of a workplace to identify individuals (e.g. employees and visitors) with a raised temperature—one of the key symptoms of COVID-19. A number of leading security companies have announced that they have developed, or are developing, this type of technology to support businesses on the frontline of the pandemic and those preparing to re-open workplaces post-lockdown, particularly those with large numbers of employees (e.g. office premises) or visitors (e.g. retailers and event spaces).

The cameras in effect measure how much heat people emit relative to their surroundings. They require less time, human intervention and contact than forehead or inner-ear thermometers. The technology on offer varies from hand-held units to mounted cameras. Some check large numbers of people at once, whilst others operate on an individual basis. The accuracy of the readings varies from between 0.3°C and 2°C.

One company using this technology is Amazon, which publicly promoted (through TV commercials) its adoption of thermal technology at its warehouses to screen for feverish workers who could be infected with COVID-19. We're also aware of trials at Bournemouth airport, NHS hospitals and various restaurant chains. Early indications are that this tech will be fairly widespread.

Wearable tech (watches, rings, proximity sensors and other IoT devices)

We may also see novel uses of existing technology. Wearable tech — personal accessories with embedded digital technology — has been around for some time. In fact, I wrote an article about the widespread uptake of wearable tech five years ago. Many of us have Apple Watches, Fitbits and the like, all of which do an impressive job of tracking our vital signs. Of course, these are generally designed for personal use, working-out and occasionally for medical purposes, such as detecting irregular heart rates and notifying emergency services (a feature on the Apple Watch).

However, one option could be for employers to encourage employees to use their smart watches (or rings, or other internet-enabled devices) to track body temperature and other vital signs that could detect the earliest stages of COVID-19 (such as heart rate and skin temperature, which are known to elevate when the body is fighting off an infection). Using this data, an employer could then instruct an employee to remain at home.

At least 2,000 emergency medical workers in San Francisco have already begun wearing rings that track their vital signs in an attempt to identify the early onset of COVID-19. In addition, Stanford Medicine researchers and their collaborators, Fitbit and Scripps Research, are launching an effort that aims to detect early signs of viral infection through data from smartwatches and other wearable devices.

Closer to home, in the UK, we've seen examples in the construction industry of embedding proximity sensors into workwear such as high-viz jackets. If one sensor detects another within the two-metre social distancing range, an alarm is sounded to alert an employer that the area is potentially overcrowded or employees are breaking the distancing rules. Data can also be stored on a centralised database, which may be useful for small-scale contact tracing, if needed. It's reported that this tech will be rolled out to construction workers in the UK on the government's HS2 project. There are also potential wider applications of this tech to offices.

COVID-19 testing kits

As the tech behind infection testing becomes more widely available and more reliable, and as the public health and clinical implications of antibody testing are identified, testing employees as part of direct employee health procedures is likely to become an option for some employers.

One example of this we've seen in the UK is in the retail food industry. In late March, following a surge in orders, online UK food retailer, Ocado, sourced 100,000 COVID-19 tests, at a cost of £1.5m. The tests will be used to protect staff and customers in an effort to keep its food delivery business going throughout the lockdown.

What laws do employers need to think about?

When considering the use of new technology to facilitate a return to work, employers in the UK should think about the interplay between:

- their obligations as an employer under the Health and Safety at Work etc. Act 1974, including general duties to provide a safe working environment; and
- their responsibilities as a controller under the General Data Protection Regulation (GDPR) as implemented in the UK by the Data Protection Act 2018.

What privacy issues should employers be aware of?

In addition to issues such as accuracy and efficacy, the tech options discussed in this article will each involve the processing of personal data, and therefore employers will need to ensure that their collection and processing of this data is in accordance with the GDPR (particularly with reference to the following principles: (1) lawfulness, fairness and transparency; (2) purpose limitation; and (3) data minimisation and documented in a data protection impact assessment).

Lawfulness, fairness and transparency

Employers must establish what is known as a "lawful basis" for processing (e.g. "compliance with a legal obligation") and—as the information collected relates to an employee's health, which is a "special category"—an additional more limited legal basis (e.g. "compliance with health and safety obligations in the field of employment law" or "for reasons of public interest in the area of public health"). These bases are specifically called out by the European Data Protection Board (EDPB) in its COVID-19 guidance (21 April 2020).

As the EDPB also notes, employee consent is unlikely to constitute a valid legal basis to process health data, as it is difficult for an employer to demonstrate that consent has been “freely given” (one of the key requirements of valid GDPR consent). This is due to the imbalance of power in the employer-employee relationship and the fact that employees would essentially be given no choice but to consent if they wanted to gain access to the workplace. For consent to be valid, it is likely that employees would need to be given an entirely free choice as to whether they consented or not, without detrimental effect (including financial) if they did not wish to participate.

In addition, employees have the right to be informed about the collection and use of their health data by employers. This is a key transparency requirement under the GDPR. An employer, therefore, must provide its employees with information including: why their health data is being processed, what it will be used for, how long it will be kept, and who it will be shared with. The UK data protection regulator, the Information Commissioner’s Office (ICO), also stipulates that the privacy notice should be concise, transparent, intelligible, easily accessible and use clear and plain language. Communication of the use of this tech to employees will be key to ensuring compliance with the GDPR.

Purposes and data minimisation

Somewhat helpfully, the ICO confirms that it is likely to be reasonable for employers to process certain health data about their employees and other visitors to their premises during the current epidemic, but emphasises that data collected must be limited to what is necessary. The ICO makes no reference to specific technologies, such as those in this article, and, therefore, as with the adoption of any new tech that uses health data, employers should be cautions in their approach. As a rule of thumb, new health-related tech should only be used where:

- **it is necessary**, e.g. where employees are required to attend work premises in person (and so cannot work from home) or where there are no other more appropriate alternative measures available;

- **the health data is adequate, relevant and limited** to what is necessary for the purposes of ensuring a safe work environment, e.g. recording only the data associated with those employees that have an elevated temperature (excluding those in the normal range);

- **appropriate safeguards are implemented** – this may include: putting in place policies and procedures to ensure that data is only used for denying entry to those with a fever and nothing more; automatically deleting data when no longer needed; periodically checking to ensure that the processing remains necessary, reasonable and proportionate (taking into account current circumstances and Government guidance on COVID-19); limiting access to the health data to certain named individuals (such as security and HR personnel); and using technical measures such as encryption and password protection; and

- **a documented plan or policy has been put in place** governing the use of the tech and its cessation when no longer needed (e.g. following a transitional phase, once a vaccine is available or in accordance with Government guidance).

Data protection impact assessments

As the types of tech discussed in this article are new (or use established tech in new ways), use health data and may also involve making automated decisions (such as denying access to work premises) or employee monitoring, there are inherent risks that use of data could be seen as intrusive, excess or disproportionate. To mitigate the risks, and to ensure employers can demonstrate to regulators that they have considered the issues and made informed and thoughtful decisions, employers will need to do a formal and detailed data protection impact assessment setting out the proposed use of the tech and a consideration of the risks to the rights of employees and others.

<u>The ICO's approach</u>

The ICO's approach to enforcement is developing. On 15 April 2020, it published a document detailing a "*flexible and pragmatic*" approach during the period of the epidemic. This includes taking a more lenient approach with employers that are currently under resourced and, when assessing GDPR compliance, keeping in mind the compelling public interest in respect of the epidemic. However, this is clearly a temporary measure aimed at giving comfort to employers for more routine activities, which may fall by the wayside during the crisis (e.g. responding to subject access requests). It should not be interpreted as a green light for employers to undertake high-risk activities without thought or those that would ordinarily be unlawful. In the words of Elizabeth Denham, the UK Information Commissioner: "*We must reflect these exceptional times. We will continue to recognise the continuing importance of privacy protections, and the value of transparency provided by freedom of information. These rights are a part of modern life we must not lose. But my office will continue to safeguard information rights in an empathetic and pragmatic way that reflects the impact of coronavirus.*"

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.