I spy with your Wi-Fi: Legalities of monitoring employees who WFH

By Keketso Kgomosotho, with Johan Botes

3 Mar 2021

The Covid-19 pandemic has accelerated (and for some, cemented) the work from home (WFH) trend, which, before the pandemic, was limited only to a handful of forward-thinking companies. According to research from Slack, 72% of employees who work from home wish to continue with some form of hybrid WFH model, even after the pandemic. Even with the vaccine rollout, many businesses are still far from going back to the analogue workplace in a way that resembles the old-normal, and many businesses have abandoned the concept of going back to a physical workplace altogether. In a world that often rewards presenteeism, however, this trend introduces a new threat to employers' and managers' sense of control over employee productivity.

© vasin leenanuruksa – 123RF.com

Monitoring tech

No employer wants to pay someone to watch television, or scroll through their social media while lying on the couch during work hours. As a result, many employers across the globe are increasingly turning to employee monitoring technology to replace the physical employee oversight once enjoyed in the office.

Our IT friends tell us that employers have been monitoring employees in the workplace for a long time through CCTV, biometric clock-in systems, and internet and telephone use, for example. Recent developments have seen employers turn to the latest technology to monitor employees, now in the home setting. The increasing suite of surveillance technology available to employers offers everything from allowing employers to view login times, measure keystrokes, track live locations, monitor and track internet, email and video, and take screenshots of employees’ desktop throughout the day.

Of course, employers have many legitimate reasons for monitoring employee activity, including managing productivity, securing information in modern networked enterprises, enforcing company policies, controlling quality, protecting employees’ safety, and securing business assets. However, the decision to monitor employees in this way is not without ethical and legal complexities.

Be wary of recorded conversations

11 Jun 2019

Justification

In South Africa, the monitoring and interception of communications is governed by the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (RICA Act). The default position in terms of the Act is that all workplace monitoring and interception is prohibited, unless it falls within one of the exceptions left open at Chapter 2 of the Act. Thus, employee monitoring is permitted:

- where the employee consents or where their consent can be reasonably implied;
- where the interception occurs in connection with carrying on of business (the business exception); or
- where interception is carried out by a person who is a party to the same communication.

Often the decision that an employer must make is whether to base their approach on prior written consent in terms of section 5, or the business exception at section 6 where written consent is not required, or a combination of both. Most employers ensure they have the prior written consent, which may be obtained in employment contracts. Those agreements may also include reference to the processing of personal information and interception of communication.

For those situations where something falls through the cracks - where the employer has written consent for some, but not all reasons for intercepting and monitoring, or where the employee has not secured consent from all staff members - the employer may have recourse to the business exception at section 6. This provision acts as a catch-all exception for employee monitoring that occurs in connection with the carrying on of a business. It does not require written consent, and is sufficient to justify the monitoring and interception of communication in connection with business operations.

Once employee communication has been intercepted, employers can expect that the data they obtained will invariably be subject to the protection of both the Protection of Personal Information Act (POPIA) and the Constitution, both of which must be fully considered when planning to monitor employees in a home setting.

The implementation of the substantive data protection and privacy provisions of PoPIA during 2020 ensured that data subjects in South Africa now have an array of additional data privacy rights. It brought with it the creation of new civil remedies, empowering data subjects to bring claims against employers for their personal information on a strict liability basis. With only a few months left of the PoPIA's grace period, it is in the employer's interest to ensure full compliance. Thus, from a PoPI compliance perspective, employers must be prepare to:

- implement a monitoring policy for employees, with the aim of informing them of the types of monitoring (for eg. covert, on-going, once-off, or occasional);

- implement the use of appropriately worded consent forms, which the employer would sign whenever consent is required. Specific reasons for the processing must be provided (for eg. where employee monitoring will take place as a result of a new work from home policy).
- inform employees of the methods of monitoring and the circumstances under which it will be conducted (typically to investigate allegations for misconduct);
- implement measures to ensure the confidentiality of the data, and that the processing complies with the PoPIA;
- implement employer's communication and awareness training programmes for existing and new employees; and at the induction of new employees.

15% of South Africans prefer to wear their birthday suit when WFH

9 Dec 2020

The boundaries between our professional and personal spaces were already rather blurry before WFH became a thing, and those lines have only become less visible. The new normal has already resulted in a shift in employee-employer relations, with staff having to work around additional childcare obligations, at-home distractions, grief and other straining factors - each requiring a more empathetic approach from employers.

Mind your monitoring

Thus, it's best to tread prudently; if the employer's aim is simply to assure productivity within the workplace, then it might be enough to simply use software that analyses the amount of time spent on a given website or programme to ensure that staff are working instead of playing. To the extent that the monitoring technology doesn't capture any personal data like passwords and banking details, and only tracks the employee during working hours, there should be no infringement on data privacy rights.

Data gathered from employee monitoring programmes could be useful in managing employee underperformance, and identifying and remedying employee misconduct, especially when physical oversight and supervision is not possible. In order to ensure a sound employee relations environment, it is critical to have a clear plan on managing employee concerns about unwarranted infringements of privacy, abuse of personal data and consequence management.

ABOUT THE AUTHOR

Keketso Kgomosotho, Candidate Attorney, overseen by Johan Botes, Partner and Head of the Employment & Compensation Practice, Baker McKenzie, Johannesburg