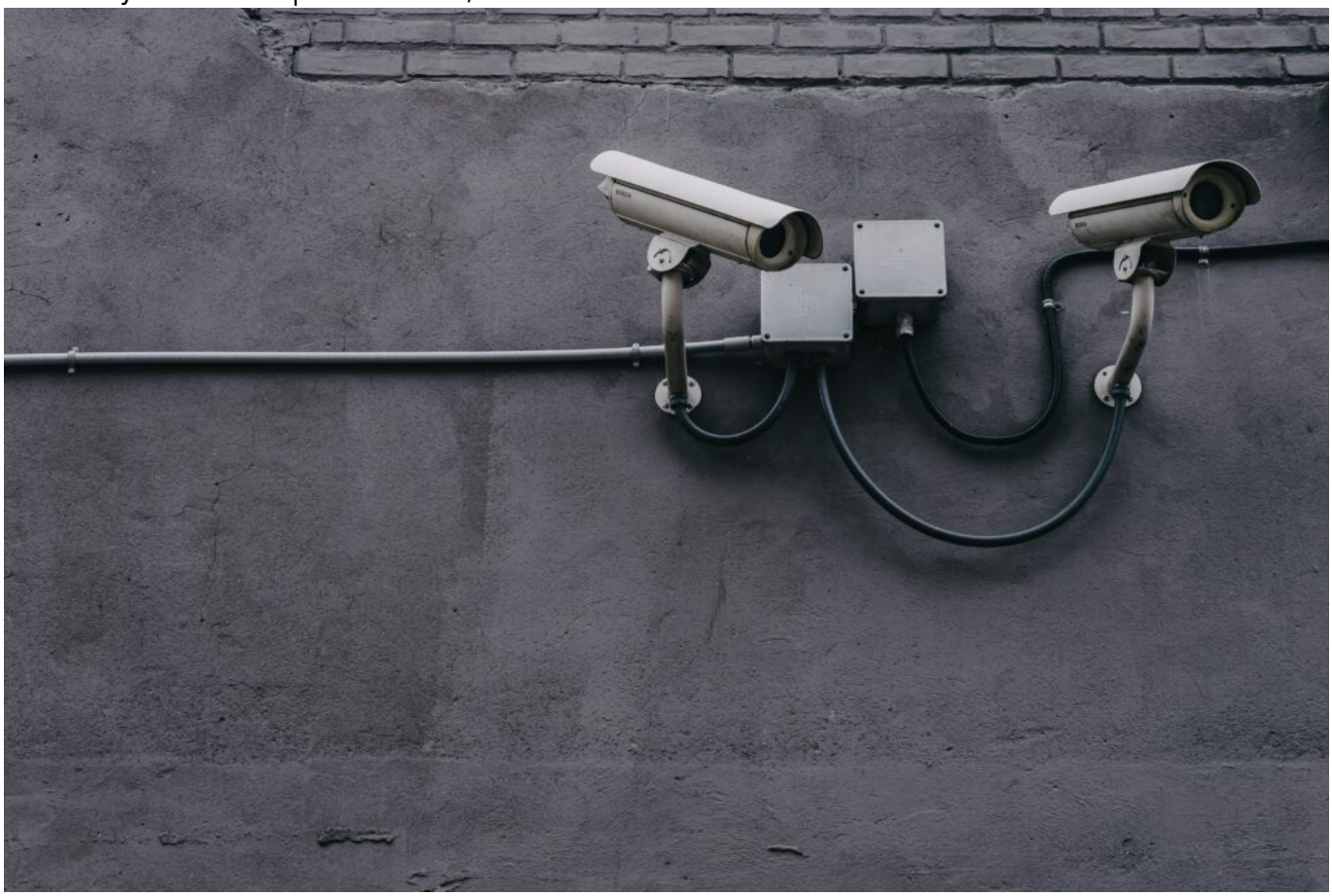
WORKPLACE MONITORING AND SURVEILLANCE: CAN EMPLOYERS MONITOR EMPLOYEES' ACTIVITIES?

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA
written by Sadia Rizvi | December 1, 2022



Workplace productivity and information security is a concern for many employers in South Africa. Employers have the burden of protecting sensitive business information to mitigate against risks such as data breaches and expensive litigation. Therefore, many employers are questioning whether they can monitor employees' activity. The availability of technology means that it is now possible for employers to monitor employees' emails, internet and social media usage, as well as telephone usage. Whilst guarding against these risks, employers are also required to balance its business interests the company with the reasonable expectations of privacy of the employees.

Legislation: Can employers monitor employees?

In terms of the Regulation of Interception of Communication and Provision of Communication-Related Information Act, 70 of 2002 ("**RICA**"), employers are entitled to intercept[1] or monitor[2] the communications of employees in the working environment. However, employers may only intercept communications if they are a party to the communications,[3] on the basis of consent,[4] or in connection with the carrying on of business.[5]

In terms of section 6, RICA provides that employers will be justified in monitoring email communications if they are able to prove the communication was intercepted in the course of the carrying on of any business; if that communication relates to that business, or which otherwise takes place in the course of the carrying on of that business. Furthermore, the interception must be

effected by, or with the express or implied consent of the system controller,[6] for the purposes of monitoring or keeping a record of indirect communications; in order to establish the existence of facts if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and if the system controller has made all reasonable efforts to inform in advance a person who intends to use the telecommunication system concerned that indirect communications transmitted by means thereof may be intercepted.

Therefore, considering the requirements of RICA, employers are entitled to monitor employee's activities if adequate notice is given to the employee. Adequate notice can include clauses in employees' employment contracts or in a workplace policy which allows for the employer to monitor and intercept communications on devices and email accounts. Usually, this clause or policy normally states that employers reserve the right to monitor and intercept communications on work devices and accounts to ensure that they are being used for work-related purposes only.

On the other hand, the Protection of Personal Information Act, 4 of 2013, ("**POPIA**") protects the privacy rights of employees. In terms of POPIA, when an employer processes the information of an employee (who is the data subject), the employer must process that information in compliance with POPIA. The employer must, therefore base the reason for processing on one of the grounds of justification in the Act.[7] The grounds of justification are consent, performance of a contract, an obligation imposed by law, legitimate interest of the data subject, performance of a public law duty, legitimate interest of the responsible party or a third party. It is very important that an appropriate ground of justification is used.

If such a clause is included in the employment contract or in a clearly communicated workplace policy, an employer can rely on "legitimate interest of the responsible party" as the ground of justification to access employee's work emails, because the employee is notified of the reason and the purpose of the processing. Such a reason must be legitimate, an example would be where an organisation is required to meet its auditing obligations.

In the absence of such a clause or policy, the employer must obtain informed, express and voluntary consent to monitor employees. This would then make the processing compliant with the provisions of POPIA.

Conclusion

What are the employer and employees rights in regards to surveillance? The privacy rights of the employee and the business requirements of the employer must be carefully balanced in order to achieve its goals. In essence, the employer must adhere to the data minimisation principle under POPIA: Personal information that a party processes must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.[8]

We suggest that employers also conduct a project specific Personal Information Impact Assessment to mitigate any data privacy risks.

Contact us if you require assistance in drafting an email, cellphone, and internet usage policy for your organisation.

Co-authors – Sadia Rizvi & Lucinda Botes

[1] “Intercept” under RICA means the acquiring of the contents of any communication through any means in order to make the contents of the communication available to another person other than the intended recipient of that communication. It includes acquisition through aural means, through an interception device, viewing, examination, inspection or diversion of the contents of the communication.

[2] “Monitor” under RICA includes to listen to or record communications by means of a monitoring device. “Monitoring device” means any electronic, mechanical or other instrument, device, equipment or apparatus which can be used to listen to or record any communications.

[3] Section 4 of RICA.

[4] Section 5 of RICA.

[5] Section 6 of RICA.

[6] System controller in relation to a private body means a natural person that is duly authorised to act as a system controller. In respect of a public body, it means the head of a department, Director-General, executive director, municipal manager, or equivalent officer of that public body.

[7] Section 11 of POPIA.

[8] Section 10 of POPIA.