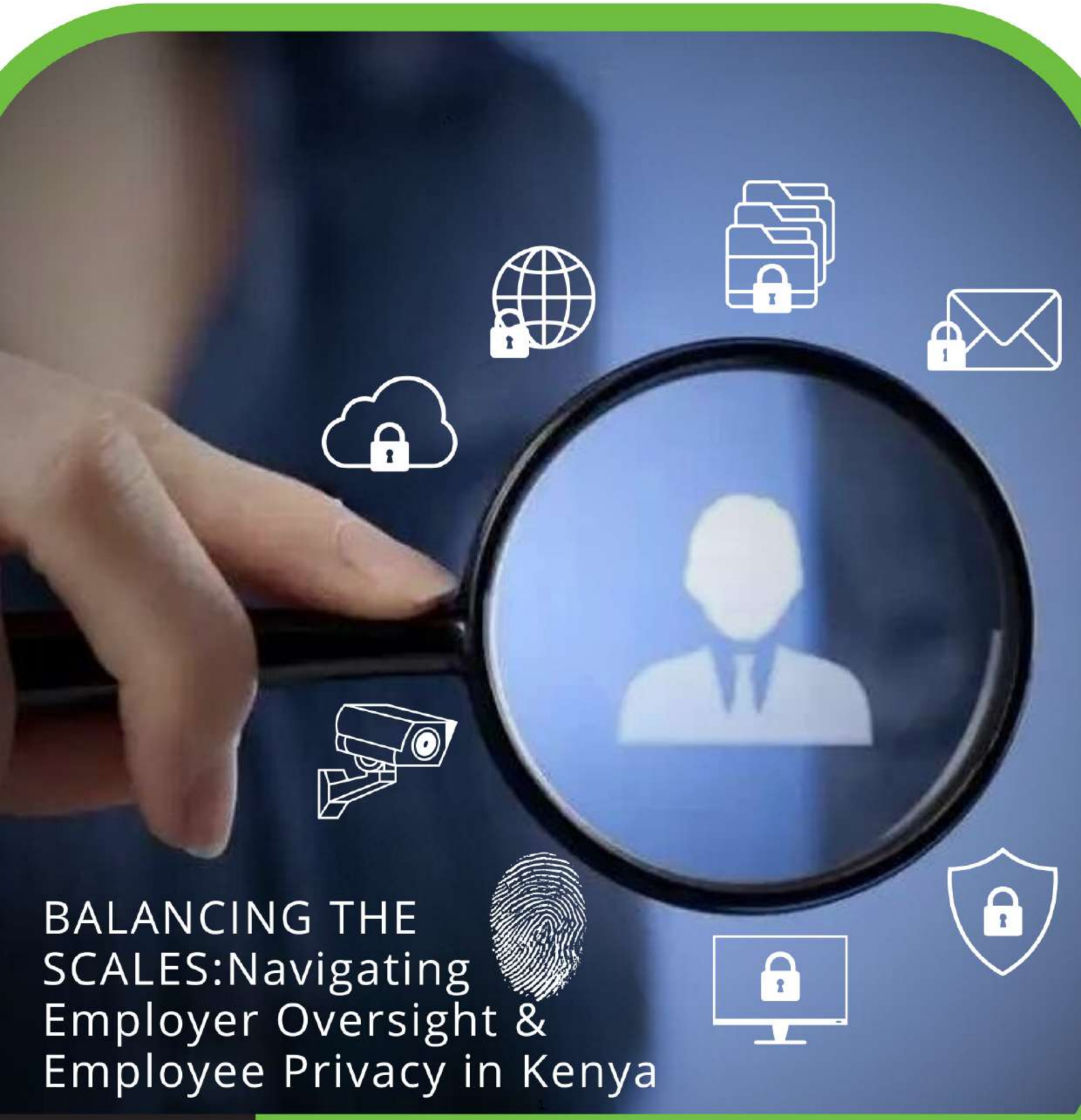
ANDREW & STEVE ADVOCATES

LEGAL ALERT

Vol.18 | March 2025

BEVERLY MABANGO /// ASSOCIATE
NELLY MAINA /// LAWYER
LITIGATION DEPARTMENT



BALANCING THE SCALES:Navigating Employer Oversight & Employee Privacy in Kenya

BALANCING THE SCALES

"Protecting privacy is necessary if an individual is to lead an autonomous, independent life, enjoy mental happiness, develop a variety of diverse interpersonal relationships, formulate unique ideas, opinions, beliefs and ways of living and participate in a democratic, pluralistic society. The importance of privacy to the individual and society certainly justifies the conclusion that it is a fundamental social value and should be vigorously protected in law. Each intrusion upon private life is demeaning not only to the dignity and spirit of the individual but also to the integrity of the society of which the individual is part."

Beate Rossler in his book – The Value of Privacy (Polity Press, 2005)

INTRODUCTION

Despite the entitlement to privacy as prescribed in our **Constitution** as well as the **Data Protection Act**, nevertheless, employers wield tools such as email surveillance, CCTV, biometrics, and social media checks to boost productivity and security for their businesses, which often clash with employees' constitutional right to privacy. Recent judicial decisions reveal how fragile the equilibrium is; between the promise of privacy and employer oversight, thereby sparking a legal tug of war. This article explores these limits, drawing lessons from three landmark decisions and proffering a path forward.

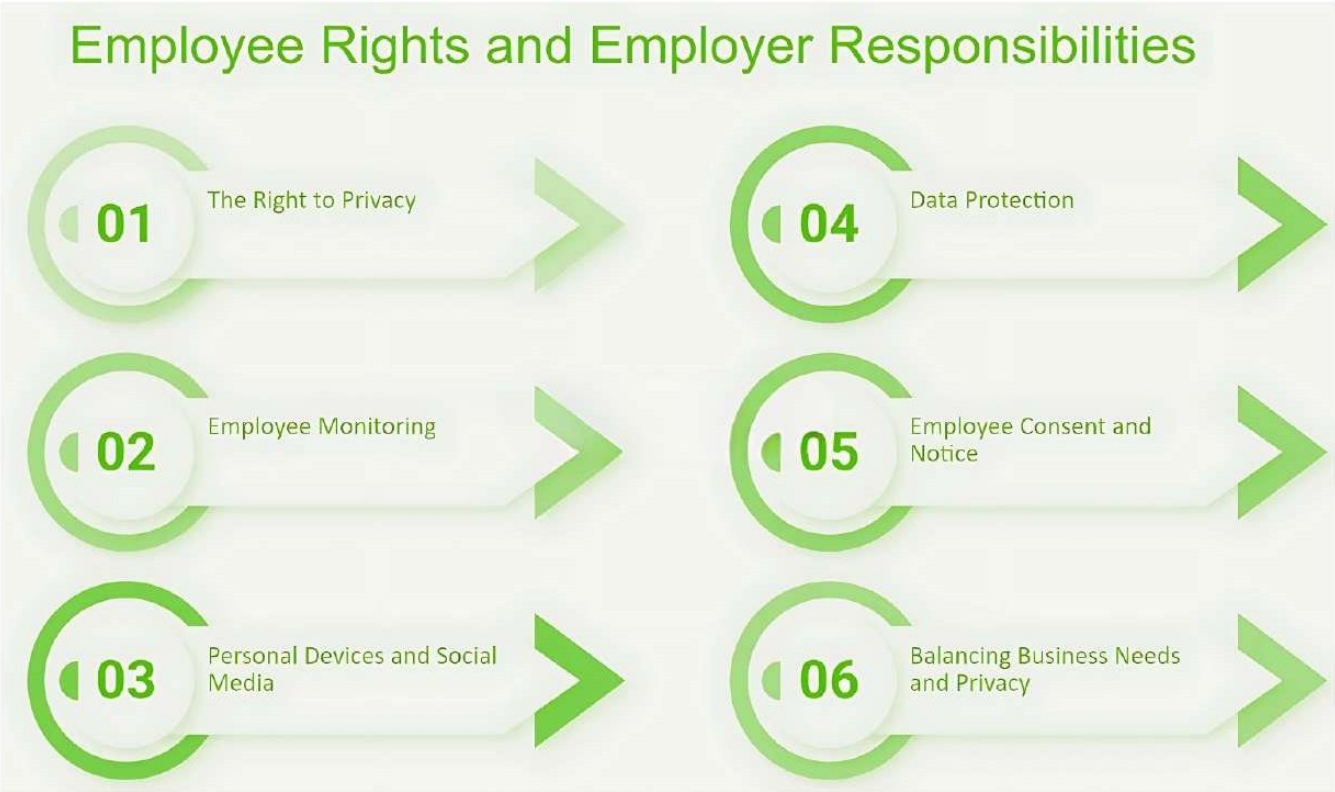
Legal Framework

Article 31 of the **Constitution** shields individuals from unwarranted data intrusions, a right that extends to workplaces. Specifically, every person has the right to privacy, which includes the right not to have their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.

Additionally, Article 41 of the **Constitution** postulates that every person has the right to fair labour practices, including inter alia, the right to reasonable working conditions.

Statutorily, the **Data Protection Act**, tightens this protection, requiring employers—in their capacity as data processors and/or controllers—to process personal data lawfully and consensually, and only for clear purposes. Moreover, high-risk monitoring demands for a data impact assessment to be conducted and enforced by the Office of the Data Protection Commissioner (ODPC).

Even so, pursuant to Article 24 of the **Constitution**, the right to privacy is not an absolute right. It can be lawfully limited but only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. This is done while taking into account factors such as the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others and the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose.



Case Studies

a. ***Emails and Devices:*** *The Musa Lesson*

When does checking an employee's messages cross the line, if at all? In **Musa & another v Makini Schools Limited [2025] KEELRC 17 (KLR),** a teacher's WhatsApp chats on a school laptop sparked his dismissal.

Japher Nanjira Musa, an IRE teacher with 18 years at Makini Schools Limited and a shop steward for the Hospital Workers union, was summarily dismissed on 13th October 2022, for alleged gross misconduct following an investigation into defamatory
blog posts by Cyprian Nyakundi. The investigation, sparked by Silas Wafula's admission and WhatsApp messages accessed from his work laptop, implicated Musa, leading to his suspension and a disciplinary hearing he claimed was unfair—citing biased panel composition, inadequate preparation time, and reliance on illegally obtained evidence.

The Court addressed the issue of Musa's privacy in relation to the WhatsApp messages accessed by Makini Schools from Silas Wafula's company-issued laptop, which formed a key part of the evidence against him. The Claimants argued that this access violated Musa's right to privacy, asserting that the personal WhatsApp conversations were illegally obtained and inadmissible under the **Evidence Act**. They contended that, unlike a work email, his personal WhatsApp account did not constitute Respondent property, even if accessed via a work device, and that such intrusion breached his constitutional rights.

The Court, however, rejected this privacy claim, ruling that the WhatsApp messages were not held by Musa personally but were retrieved from the company's laptop, thus not constituting an unwarranted invasion of his privacy. Citing Section 6(1)(d) of the **Access to Information Act**, which limits access to information when it invades privacy unjustifiably, the court found no violation here, as the data was on employer property.

The court balanced Musa's privacy against the employer's right to manage its business, concluding that accessing the messages was proportionate to the allegations and did not infringe his rights, given their location on a work device rather than a personal gadget.

b. ***Beyond the Office:*** *The Mwangi and Cyrus Warnings*

In **Mwangi v ABSA Bank Kenya PLC [2024] KEELRC 2399 (KLR) (1 October 2024),** a bank hired a private investigator to tail a suspended branch manager—tracking him to pubs and restaurants.

Thomas Macharia Mwangi, a senior branch manager at ABSA Bank Kenya PLC's Nkrumah Road branch in Mombasa, was terminated on May 26, 2023, following a disciplinary process initiated by a suspension on March 17, 2023, for irregular and unauthorized overdraft facilities granted to customers DM Kanyi and Safinah Petroleum Limited. Mwangi claimed unfair termination, alleging procedural flaws, a premeditated dismissal evidenced by the bank advertising his position before his appeal, and a witch hunt for raising concerns about senior staff. He also accused the bank of breaching his privacy under Article 31 of the **Constitution** by

hiring a private investigator to probe his personal life during suspension, tracking him in public spaces, and circulating damaging reports, seeking damages for defamation.

The Court ruled that Mwangi's termination was substantively and procedurally fair under Sections 35, 41, 43, and 45 of the **Employment Act**, citing his failure to manage loan accounts properly, including a Ksh 500,000 deposit into DM Kanyi's account and unprocedural excesses for Safinah, breaching bank policies and exposing ABSA to financial risk.

However, it found the bank's use of a private investigator to monitor Mwangi's private life unjustified and a violation of his Article 31 privacy rights, as no workplace-related basis was provided, awarding Ksh 5 million in general damages to Mwangi.

Contrast the aforementioned with **Cyrus Mwaniki Ndungu v Moja Expressway Company (ODPC Complaint 0264 of 2024),** where the ODPC tackled an ex-toll attendant's image used in promotional videos nearly a year after resignation.

Cyrus Mwaniki Ndungu filed a complaint with the ODPC on February 16, 2024, alleging that Moja Expressway Company unlawfully used his image in promotional videos on social media nearly a year after his resignation on November 28, 2022, without his consent. Ndungu, employed as a toll attendant and sales personnel from July 5, 2022, claimed the video, posted on 5th October 2023, depicted him as still working for the company, violating his privacy rights under Article 31 of the **Constitution** and the **Data Protection Act**.

Following a demand letter on December 7, 2023, the Respondent deleted the video on December 10, 2023, but offered no apology or explanation. Ndungu sought a declaration of rights violation, an administrative fine, and Kshs. 3 million in compensation. The Respondent admitted to using the video, claiming it was an operational tool created with Ndungu's oral consent during employment for explaining Electronic Toll Collection (ETC) services, not commercial promotion, and relied on his contract as the lawful basis, asserting they deleted it upon his objection.

The ODPC investigated and determined three issues: (1) consent for further processing (post contractual engagement), (2) rights violation, and (3) remedies. It found that while Ndungu's initial participation in the video was part of his job, the Respondent failed to obtain express consent under Sections 30 and 32 of the **Data Protection Act** to use his image post-resignation, rendering the use unlawful, especially for commercial purposes (influencing ETC subscriptions) under Section 37 and Regulation 14 of the **Data Protection (General) Regulations**.

Although the Respondent deleted the video within 3 days of Ndungu's demand, complying with erasure rights under Section 40, the prior unauthorized use breached his data protection rights. Balancing the violation's duration and the Respondent's mitigation (deletion and policy review), the ODPC ordered Kshs. 500,000 in compensation for Ndungu, directed the Respondent to ensure proper consent practices, and upheld their liability, with an appeal option to the High Court within 30 days.

Analysis

Kenya's legal framework on workplace privacy is a dynamic battleground, with *Musa*, *Mwangi*, and *Cyrus* revealing a spectrum of judicial and regulatory responses. On one hand, the Court carved out a pragmatic boundary: employer-owned devices are fair game for monitoring when tied to legitimate business needs, like investigating misconduct. On the other hand, the Court drew a sharper line. While upholding an employee's termination for fiduciary lapses, the court castigated ABSA's off-duty surveillance via a private investigator as an unjustifiable overreach. The absence of a workplace nexus for tracking Mwangi to pubs and restaurants violated Article 31, earning him Kshs. 5 million in damages. This pivot highlights a critical threshold: employer oversight must tether to job-related conduct, not personal whims.

Meanwhile, Moja Expressway's post-employment use of Cyrus's image for commercial gain—without renewed consent—breached his rights as under the **Data Protection Act**. The Kshs. 500,000 penalties, tempered by swift mitigation, reflects a nuanced stance: violations sting, but responsiveness matters.

A snapshot of this triad suggests a judiciary and regulator wrestling with context—workplace tools versus personal spaces, active employment versus post-exit rights—while striving to align constitutional and statutory protections with employer interests.

Reconciling employer oversight with privacy demands a practical approach. First, transparency is non-negotiable: employers must codify monitoring policies—scope, tools, and limits—mirroring *Musa's* implicit nod to notice. Second, consent must evolve beyond oral ambiguity (*Cyrus's* lesson) to written, specific agreements, renewable post-employment for ongoing data use. Third, proportionality, as in *Musa* and *Mwangi*, requires employers to link surveillance to clear risks—financial loss, misconduct—not speculative curiosity. Fourth, off-duty monitoring needs a high bar: *Mwangi's* rebuke signals that absent a direct job nexus, it's a legal minefield. Finally, pre-emptive risk assessments, inspired by the Data Protection Act's Section 31, should be routine for invasive tools like biometrics or trackers, echoing global best practices. Employers can operationalize this through tiered strategies: notify staff of device monitoring at onboarding, secure opt-in consent for marketing uses, and audit data retention post-exit.

CONCLUSION

In Kenya's evolving legal landscape, balancing employer oversight and employee privacy remains a delicate endeavour. While employers have a legitimate interest in ensuring productivity, safeguarding assets, and maintaining workplace discipline, these interests must be pursued within the boundaries of employees' constitutional rights to privacy and dignity. A proactive approach that includes clear policies, transparent communication, and lawful

data management practices is essential. Employers should regularly review their monitoring practices to ensure compliance with the **Data Protection Act** and related labour laws. Likewise, employees should be aware of their rights and avenues for recourse in case of infringement. Ultimately, fostering a culture of

trust, respect, and compliance benefits both parties, contributing to a more productive and legally sound work environment.