

KENYA / JUDGMENT

Matey v Safaricom PLC

[2026] KEHC 13624 (KLR)

[2026] KEHC 13624 (KLR)

COURT

High Court

BEFORE

D Mburu

CASE / FILE NUMBER

Constitutional Miscellaneous Application E043 of
2026

Source: new.kenyalaw.org · Research copy typeset by Esheria. Not court-issued or certified.

Matey v Safaricom PLC (Constitutional Miscellaneous Application E043 of 2026) [2026] KEHC 13624 (KLR) (Constitutional and Human Rights) (18 September 2026) (Ruling) Neutral citation:

[2026] KEHC 13624 (KLR) Republic of Kenya In the High Court at Nairobi (Milimani Law Courts) Constitutional and Human Rights Constitutional Miscellaneous Application E043 of 2026 D Mburu, J September 18, 2026 Between Naomi Jepkemboi Matey Applicant and Safaricom Plc Respondent

Ruling

Introduction

1. Before the Court for determination is the Notice of Motion Application dated 27 th July, 2026 brought under Order 51 of the Civil Procedure Rules. The application is supported by the Affidavit of, Naomi Jepkemboi Matey, the applicant, sworn on even date. 2. The application seeks the following orders: 1. That this Court do issue an order compelling the Respondent to furnish the Applicant with particulars of all requests made by any person or institution seeking access to or disclosure of information relating to the communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 796 xxx xxx and +254 714 xxx xxx. 2. That this Court do issue an order compelling the Respondent to provide details of any monitoring, surveillance, querying or access to the communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 796 xxx xxx and +254 714 xxx xxx between March 2024 and January 2025. 3. That this Court do issue an order compelling the Respondent to disclose the identity of any person or institution that sought or obtained access to the communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 796 xxx xxx and +254 714 xxx xxx

between March 2024 and January 2025. 4. that this Court do issue an order compelling the Respondent to furnish the Applicant with certified copies of all logs and records relating to access, monitoring, surveillance or querying of communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 796 xxx xxx and +254 714 xxx xxx between March 2024 and January 2025. 5. That costs be provided for. 3. Through her supporting affidavit, the applicant asserts that she is the holder and registered user of mobile numbers +254 xxx xxx and +254 714 xxx xxx (hereinafter referred to as the "mobile numbers") with the Respondent, a telecommunications service provider and the custodian of communications records, telecommunications data, financial transactions and M-Pesa account information relating to the mobile numbers. 4. The applicant avers that she has recently learned and has reasonable grounds to believe that her communications, telecommunications data, financial transactions and M-Pesa account activity linked to the mobile numbers may have been unlawfully requested, accessed, monitored, queried, disclosed or otherwise interfered with by certain persons or institutions between March 2024 and January 2025. 5. Since the Applicant is unable to ascertain the persons involved, the nature of the access and the legal basis without obtaining the relevant records from the Respondent, she requested the Respondent to furnish information and records relating to the same vide a letter dated 2 nd June 2026 , to which the Respondent vide a letter dated 4 th June 2026, refused to furnish the information, stating that disclosure would only be made upon receipt of a court order, even though some information is at risk of falling outside its data retention timelines. 6. With the Response from the Respondent, the Applicant asserts that there is no substantive opposition to the disclosure sought and that information sought is necessary to enable her establish whether her communications and financial information were interfered with, and by whom. That without the information, she is unable to effectively exercise and protect her constitutional rights to dignity, privacy and access to information. 7. The Respondent filed a replying affidavit sworn on 29 th July, 2026 by one Mercelynne Awuor Okelo, the Principal Officer of the Respondent's fraud department. 8. She deposes that in providing the telecommunications services, the Respondent processes and safeguards customer information in accordance with the Constitution , the Data Protection Act, 2019 , the Kenya Information and Communications Act and all applicable regulatory obligations and is committed to protecting the integrity, confidentiality and security of subscriber information and has in place policies, internal controls and technical safeguards designed to protect customer information from unauthorized access and misuse. She admits that the applicant is a subscriber of their services. 9. The Respondent acknowledges receipt of the Applicant's letter dated 2 nd June 2026 requesting disclosure of various categories of information relating to the Applicant's mobile numbers on the basis that she believed her communications and M-Pesa information had been unlawfully accessed between March 2024 and January 2025, but states that contrary to the repeated assertions contained in the Supporting Affidavit, the Respondent did not refuse the Applicant's request, that they expressly advised the Applicant of the appropriate provisions through which the request could be assessed and considered, including the lodging of a formal request through the

Respondent's Headquarters, following which the Respondent would advise on the applicable requirements and documentation necessary to facilitate the request. 10. She deposes that the Applicant has therefore materially mischaracterized the Respondent's response by describing it as a refusal as they neither declined to assist the Applicant nor rejected her request. Rather, she explained that any disclosure would necessarily be undertaken within the framework of the applicable legal and regulatory requirements governing subscriber information but more importantly, the Applicant never visited and lodged a formal complaint with the Respondent as advised nor provided any particulars explaining the basis of her allegations to date. 11. That the Applicant's letter dated 2 nd June 2026 sought disclosure of information. It did not constitute an investigative complaint capable of being acted upon by the Respondent's operational teams and that normally, where a subscriber alleges unauthorized access to their account or personal information, the Respondent's established procedure is to receive a formal complaint setting out the factual basis of the allegation together with such supporting documentation as may be available, including the dates of the alleged incident, the specific activity complained of and any other material capable of assisting in identifying the alleged compromise. 12. The Respondent states that those particulars enable the Respondent to define the scope of the inquiry and undertake a focused investigation. And that despite alleging unlawful access to her communications and M-Pesa information over an extended period, the Applicant has not annexed to her Supporting Affidavit any documentary material capable of identifying the alleged unauthorized access or assisting the Respondent in narrowing the scope of any investigation. They therefore state that the Applicant therefore approached the court before exhausting the very process that would have enabled the Respondent to ascertain whether any unauthorized access had occurred and, if so, whether any substantive information exists. 13. The Respondent denies that it does not undertake surveillance or monitoring of subscriber communications in the manner alleged by the Applicant, nor does it maintain records of "surveillance", "monitoring" or "querying" in the broad terms framed in the Application, because such records are neither generated nor maintained in the ordinary course of the Respondent's business. 14. The Respondent states that they advised the Applicant that available information would be pursuant to a court order however the Respondent is limited to what is actively in their possession and they further expressly informed the Applicant, prior to the commencement of these proceedings, that given the period identified by the Applicant, certain information sought might fall outside the applicable retention timelines, this was done to manage the Applicant's expectations regarding the possible availability of historical records. 15. The Respondent finalizes by stating that granting the orders sought in their present form would expose the Respondent to the risk of being directed to produce information that may not exist, may not have been generated, may not be retained or may not fall within the Respondent's custody or control, thereby rendering compliance with such orders impracticable through no fault of the Respondent. They however remain ready and willing to assist the Applicant within the confines of the law. However, to facilitate any meaningful investigation and enable the Respondent to identify what information, if any, exists and is lawfully disclosable, the

Applicant must first provide sufficient particulars together with any supporting documentation forming the basis of her allegations, thereby ensuring compliance with any orders that this Court may issue. 16. The Application proceeded for inter-partes hearing on 31 st July, 2026 where parties restated their positions as per their respective affidavits.

Analysis and Determination

14. Having considered the application, affidavits and submissions by both parties, the sole issue for determination is: A. Whether the Applicant has Established Sufficient Basis for the Court to Compel the Respondent to Ddisclose the Information Sought. 17. Of importance to note is that the Respondents in their letter dated 4 th June 2026, expressly stated that disclosure would only be made upon receipt of a court order even though some information is at risk of falling outside its data retention timelines. 18. In their response they state that the Applicant ought to have exhausted the processes laid down before coming to this court. This process is not laid out in their affidavit or the letter of 4 th June, 2026. What is contained thereon is advice to lodge an official request, whereby they Applicant will then be informed of the requirements and the appropriate process including any documentation. 19. That this process is shrouded in mystery explains why the Applicant opted to approach this court for the Court Orders as advised, for her to be able to access the information she requires. 20. Having said that, the application principally invokes the constitutional rights to privacy under Article 31 and access to information under Article 35 of the Constitution . While Article 35 guarantees every citizen access to information held by another person where required for the exercise or protection of a right, such access is not absolute and must be balanced against statutory obligations governing confidential subscriber information. 21. Article 35 provides: (1). Every citizen has the right of access to- a. Information held by the State; and b. Information held by another person and required for the exercise or protection of any right or fundamental freedom. 22. There is no dispute that the right to information is at the core of the exercise and enjoyment of all other rights by citizens and is a right expressly recognized in the Constitution . The essence of the right of access to information has been explained in many decisions. 23. In *Brummer v Minister for Social Development* (CCT 25/09) [2009] ZACC 21; the Constitutional Court of South Africa stated that: “ access to information is fundamental to the realization of the rights guaranteed in the Bill of Rights. For example, access to information is crucial to the right to freedom of expression which includes freedom of the press and other media and freedom to receive or impart information or ideas.” 24. Back at home, in *Nairobi Law Monthly Company Limited Kenya Electricity Generating Company & 2 others* the court stated: [56] ...State organs or public entities ... have a constitutional obligation to provide information to citizens as of right under the provisions of Article 35(1)(a)....they cannot escape the constitutional requirement that they provide access to such information as they hold to citizens. 25. Similarly, in *Katiba Institute v President’s Delivery Unit*, the court observed that the right to access information is a foundational human right upon which other rights must flow. And for citizens to protect their other rights, the right to access information becomes critical for any meaningful and

effective participation in the democratic governance of their country. 26. The court went on to state: “ (29) The importance of this right was fully appreciated by the drafters of our Constitution and they dutifully included Article 35 to make this right attainable as the foundation for an open, responsive, accountable and democratic government and its institutions. The Constitution , therefore, grants citizens’ access to information as a constitutional right and only the same Constitution can limit that access.” 27. To actualize article 35, Parliament enacted Access to Information Act in 2016 whose section 4 provides for accessing information. The section repeats the words in article 35 providing: 1. Subject to this Act and any other written law, every citizen has the right of access to information held by— (a) the State; and b) another person and where that information is required for the exercise or protection of any right or fundamental freedom. 2. Subject to this Act, every citizen's right to access information is not affected by— a) any reason the person gives for seeking access; or b) the public entity's belief as to what are the person's reasons for seeking access. 3) Access to information held by a public entity or a private body shall be provided expeditiously at a reasonable cost. 16. The Respondent is a public entity hence falls under section 3 as stated above. The Applicant sought information which has not been provided by the Respondent because of the need for a court order. For the petitioners to access information under article 35(1)(b), the information had to be for purposes of exercising or protecting a right or fundamental freedom in the Bill of Rights. The Applicant has stated clearly as much, that she believes there has been illegal access, monitoring and disclosure of her information without her consent, she wishes to get the information to protect herself against the intruders. 16. On the other hand, Section 5 of the Act further provides that a public entity should facilitate access to information held by it. Under section 8, a citizen who wants to access information should do so in writing with sufficient details and particulars to enable the public officer understand what information is being requested. The Act is also sufficiently clear that the information should be given without delay and at no fee, notwithstanding why the citizen wants to access information. Section 9 makes states that a decision on the request to access information should be made and communicated within 21 days. The communication should include whether the public entity has the information and whether it will provide access to the information. 17. Section 25 (a), (b) and (c) of the Data Protection Act provides that; “ Every data controller or data processor shall ensure that personal data is — a. processed in accordance with the right to privacy of the data subject; b. processed lawfully, fairly and in a transparent manner in relation to any data subject; (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;” 18. Section 26 of the Data Protection Act provides that; A data subject has a right— (a) to be informed of the use to which their personal data is to be put; (b) to access their personal data in custody of data controller or data processor; (c) to object to the processing of all or part of their personal data; (d) to correction of false or misleading data; and (e) to deletion of false or misleading data about them.’ 20. It is not disputed that the Applicant is the registered subscriber of the two mobile numbers. Equally undisputed is that she requested information from the Respondent through her letter dated 2 nd June 2026. The Respondent's response did not deny the

possibility of disclosure; rather, it indicated that disclosure would be undertaken within the applicable legal framework and upon satisfaction of the necessary requirements, including a court order where appropriate. The Court also notes that the Respondent expressly indicated that disclosure could be made pursuant to a court order. Having taken that position, the Respondent cannot simultaneously rely solely on procedural objections to defeat a judicial request for disclosure where the information sought relates to the Applicant's own personal data. 21. The Respondent's principal objection is that the Applicant failed to lodge a formal investigative complaint and failed to provide sufficient particulars to facilitate an internal inquiry. That argument has merit to the extent that a telecommunications provider cannot reasonably investigate vague allegations of unauthorized access spanning several months without identifiable incidents or dates. However, the present application is distinguishable from an internal fraud investigation. The Applicant does not seek the Respondent to determine liability or conduct disciplinary proceedings; she seeks disclosure of records relating to access to her own information. 22. The Court is persuaded that if access logs, audit trails, requests from third parties or disclosure records exist within the Respondent's custody and relate to the Applicant's own subscriber accounts, such information falls within the scope of information capable of disclosure subject to the Constitution, the Data Protection Act and any lawful limitations protecting third-party interests or ongoing investigations. 23. At the same time, the Court cannot compel production of records that do not exist or were never generated. Courts issue orders requiring production of documents within a party's possession, custody or control they do not compel the creation of documents or records that have lawfully been deleted pursuant to applicable retention policies. 24. Consequently, the Court finds merit in the application dated 27th July, 2026 and grants the following orders: a. The Respondent shall within 21 days from the date of this ruling, provide the Applicant with certified copies of subscriber details, particulars of all requests made by any person or institution seeking access to or disclosure of information relating to the communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 xxx xxx 796 and +254 714 xxx xxx between March 2024 and January 2025 as sought. b. The Respondent shall disclose all available access logs, audit records or disclosure records in its possession, custody or control relating to the Applicant linked to mobile numbers +254 xxx xxx and +254 714 xxx xxx between March 2024 and January 2025. c. The Respondent shall within 21 days, furnish the Applicant with certified copies of all logs and records relating to access, monitoring, surveillance or querying of communications, telecommunications data, financial transactions or M-Pesa account information linked to mobile numbers +254 796 xxx xxx and +254 714 xxx xxx between March 2024 and January 2025. d. Each party shall bear its own costs of the application. DATED, SIGNED AND DELIVERED VIRTUALLY AT NAIROBI THIS 18TH DAY OF SEPTEMBER, 2026. DAVID MBURU JUDGE

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://new.kenyalaw.org/akn/ke/judgment/kehc/2026/13624>

CASE PAGE <https://chat.esheria.ai/case-law/kenya/matey-v-safaricom-plc-2026>

Prepared on 29 October 2026 · Esheria