Privacy & Data Protection
24th November 2025



YOUR CCTV'S GAZE MUST END AT THE BOUNDARY: INTERPRETING *NDERITU & ANOR. V. KARUNGO & ANOR.* AND ITS SIGNIFICANCE FOR DATA PROTECTION AND PRIVACY IN NIGERIA[1]

1. Introduction

We live in a society where Closed-Circuit Televisions ("**CCTVs**")[2] are now a common sight in residential homes, commercial and retail locations, office and industrial sites, places of worship, parks, schools, and public spaces. At one point in time, the Federal Government of Nigeria took a loan of $460 million to fund a CCTV project for the nation's capital, Abuja.[3] This practice draws strength and reasonableness from a blissful marriage between two needs: the need to secure and protect lives and the need to secure and protect properties. These needs are constitutionally embedded in the right to life and the right to acquire and own movable and immovable properties anywhere in Nigeria.[4] However, rights do not exist absolutely. One visible limit of a right is when its exercise impinges on or invades the precincts of another person's right.[5] This situation justifies a legal inquiry into the lawful and permissible range of a CCTV camera's view in relation to an individual's right to privacy.

---

1 **David Andy Essien, Associate, Cross-Departmental, S. P. A. Ajibade & Co., Abuja, Nigeria.**

2 A Closed-Circuit Television (CCTV) system, also commonly referred to as a "video surveillance system", includes an assemblage of security cameras linked to one or more monitors, usually television screens. The term, "Closed-Circuit", refers to the transmission of video footage exclusively limited to a private network, and accessible only to individuals who are authorized to view or monitor the content. See, Isarsoft, 'A Guide to CCTV Systems: What is CCTV?' (*Isarsoft*, 1 June 2024) <https://www.isarsoft.com/knowledge-hub/cctv> accessed 16 November 2025.

3 Itodo Daniel Sule, 'Reps to Probe $460m Abuja CCTV Project Amid Rising Insecurity' (*Daily Trust*, 23 October 2025) <https://dailytrust.com/reps-to-probe-460m-abuja-cctv-project-amid-rising-insecurity/> accessed 16 November 2025.

4 See, sections 33 and 43 of the *Constitution of the Federal Republic of Nigeria*, 1999 (as amended) ["*CFRN*"].

5 David Andy Essien, 'Reposts, Reshares, Retweets and Vile Comments on a Defamatory or Life-threatening Social Media Post: The Implications of the Harman v. Strydom's Case for Nigeria's

On 20th October 2025, the Office of the Data Protection Commissioner ("**ODPC**")[6] in the Republic of Kenya determined a complaint in the case of **Lilian Nyawira Nderitu & Anor. v. Josephat Karungo & Anor.,** ("**Nderitu's Case**"),[7] and decided that intrusive technological security measures in favour of one party cannot prevail or take precedence over the constitutional and statutory privacy rights of another party. The ODPC discountenanced the defence of "legitimate purposes" and resolved that an adjoining property is a private space, and continuous surveillance from a neighbouring property, even unintentionally, constitutes unauthorized processing of personal data. It counselled that the installation and operation of CCTVs must respect the privacy rights of others and the CCTV's field of view or range must remain confined within the legitimate boundaries of the owner's property.

In view of the evolving nature of data governance and the far-reaching adoption of technology in Nigeria, *Nderitu's Case* is a timely addition to the data accountability expectations from data controllers, data processors, and data administrators. Although this case was decided in line with Kenyan law, its reasoning accords with the privacy principles enshrined in section 37 of the *Constitution of the Federal Republic of Nigeria*, 1999 ("**CFRN**"), the *Nigerian Data Protection Act*, 2023 ("**NDPA**"), and the *General Application and Implementation Directive*, 2025 ("**GAID**").[8] This paper discusses the

---

Digital Landscape' (*SPA Ajibade & Co.*, 13 November 2025) at p. 1 <https://spaajibade.com/wp-content/uploads/2025/11/Reposts-reshares-retweets-and-vile-comments-on-a-defamatory.pdf> accessed 20 November 2025.

6 A summary of the legal framework enabling the ODPC to receive, hear, and determine complaints concerning data protection and privacy in Kenya, is as follows: (i) Section 5 of Kenya's *Data Protection Act*, 2019 ("*DPA*") established the ODPC and tasked it with several responsibilities including establishing the legal and institutional mechanism to protect data, and providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the *DPA*. (ii) Section 8(1)(f) of the *DPA* empowers the ODPC to receive and investigate any complaint by any person on infringements of the rights under the *DPA*. (iii) Section 56(1) of the *DPA* enables a data subject who is aggrieved by a decision of any person under the *DPA* to lodge a complaint with the Data Commissioner in accordance with the *DPA*.
These provisions are similar to its Nigerian equivalent concerning the Nigerian Data Protection Commission ("*NDPC*"). See, sections 5(g) and 6(f) of the *Nigerian Data Protection Act*, 2023 ("*NDPA*") and article 39 (4) – (13) of the *General Application and Implementation Directive*, 2025 ("*GAID*").

7 Unreported Determination in ODPC Complaint No. 0596 of 2025 delivered by the Office of the Data Protection Commissioner (ODPC), Republic of Kenya on 20th October 2025 (hereinafter referred to as "*Nderitu's Case*"). *Coram:* Immaculate Kassait, MBS (Data Commissioner). This can be accessed via this link: <https://www.odpc.go.ke/wp-content/uploads/2025/10/Lillian-Nyawira-and-another-vs-Josephat-Karungo-and-Another.pdf> accessed 16 November 2025.

8 See the transformative views of Honourable Justice A. B. Mohammed, JCA, in the celebrated case of *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors. v. National Identity Management Commission* (2021) LPELR – 55623 (CA), at pp. 20 – 21, paras. F – F, where he pontificated thus:

reasoning and doctrinal basis for the decision in *Nderitu's Case* and reflects its influence on Nigeria's data protection and privacy jurisprudence. Outside the legal implications, this paper mirrors a bigger policy challenge: how to fairly balance the legitimate use of technology by one party to secure lives and properties vis-à-vis the rights of others to the privacy of their homes, personal, and family life. In the end, this paper proffers lawful remedies to any person whose privacy rights are breached or likely to be breached by CCTV surveillance in Nigeria. Recommendations are made to the Nigerian Data Protection Commission ("**NDPC**"), and also to CCTV owners and operators in Nigeria on how best to operate their CCTVs without legal repercussions.

2. Facts of Nderitu & Anor. v. Karungo & Anor.

Nderitu and Mureithi ("**the Complainants**") lodged complaints with the ODPC against Karungo and Waweru ("**the Respondents**") alleging that the Respondents' CCTV cameras had been installed in a manner that intruded upon their private residence. The thrust of the case of the Complainants is that sometime in the year 2021, the Respondents installed CCTV cameras on their property and that the placement of the said cameras had deprived them of a quiet and safe living environment, thereby interfering with the peaceful enjoyment of their property. The Complainants contended that two of the camera's fields of view allegedly extended into their kitchen and the surrounding areas, capturing private and domestic activities within their home. They further contended that the continued surveillance had caused them considerable anxiety, stress, and emotional as well as psychological distress.

The Complainants stated that despite multiple attempts to resolve the matter amicably with the Respondents, including engagement through mutual contacts and legal representation, the issue remained unresolved. They further stated that they escalated the matter to the police and the area chief. However, the cameras have remained positioned in a manner that, in their opinion, continued to occasion a breach of their right to privacy. Consequently, the Complainants sought the following remedies:

i. Removal of the CCTV cameras and cessation of activities invading their privacy.

"*… **privacy to my mind can be said to mean the right to be free from public attention or the right not to have others intrude into one's private space uninvited or without one's approval**. It means to be able to stay away or apart from others without observation or intrusion. It also includes the protection of personal information from others. **The right to privacy is not limited to his home but extends to anything that is private and personal to him including communication and personal data***." (Emphasis added)

ii. General damages for anxiety, stress, and emotional and psychological distress caused by the alleged intrusion.

iii. Sanctions against the Respondents for breach of personal data privacy.

In response, the Respondents categorically denied the factual points made by the Complainants and maintained that their actions were lawful, necessary, and guided by legitimate security concerns. The Respondents contended that the CCTV was installed sometime in the year 2021 after an attempted burglary, following consultations with community elders and security representatives. They asserted that the installation was done in good faith to enhance household and neighbourhood safety, and not to infringe on anyone's privacy. The Respondents stated that the CCTV camera in question had already been adjusted before the formal complaint was received and that the adjustment was made on 14th July 2025, as a gesture of goodwill following a meeting with the area chief, Association Chairman, and another area member. Notwithstanding the foregoing, and without prejudice to their position, the Respondents stated that they were willing to co-operate with the Office of the Data Protection Commissioner should further engagement be necessary and that this goodwill offer did not amount to any admission of liability. Conclusively, the Respondents submitted that the CCTV adjustment was done voluntarily and in advance; that the installation served a legitimate security purpose; and that there is no evidence of unlawful data collection or intentional privacy breach.

By way of a rejoinder, the Complainants averred that the range of the CCTV camera mounted on the soffits (beneath the roof overhang on the First Floor of the Respondents' house near a glass window) was directly facing their premises and extended into their residence. During the meeting held at the Chief's office on 23rd April 2025, it was observed and confirmed that the specific camera captured parts of the Complainants' residence and there was evidence to this effect. The Complainants further contended that the same camera overreached other areas within their compound thereby violating their privacy. Again, they asserted that several moves were made by them to amicably resolve this issue but all to no avail and that this continued breach deprived them of their right to privacy and of the quiet and safe enjoyment of their home. By way of clarification, the Complainants stated that the camera in question is the one mounted at the soffits and not the one referred to in the Respondents' letter. They maintained that the overreach began soon after the installation of the cameras in the year 2021 and continued until 16th July 2025, when the cameras were finally removed. The Complainants acknowledged that security cameras play an important role in enhancing safety but that there was no justification

for violating their privacy in the name of security. In this wise, the Complainants maintained that the Respondents had a duty of care during installation to ensure that their actions did not cause harm or intrusion.

3. Determination by the Office of the Data Protection Commissioner (ODPC)

In determining this Complaint, the ODPC raised two issues, to wit: whether the Respondents fulfilled their obligations in accordance with Kenya's *Data Protection Act*, 2019 ("**DPA**"); and whether the Complainants are entitled to any remedies under the *DPA* and the attendant Regulations.

In resolving the first issue, the ODPC held that section 25 of the *DPA* obligates every data controller or processor to ensure that personal data is processed in line with the principles of privacy, fairness, purpose limitation, and accountability and that specifically, under sub-sections (c) and (d) of the said section 25, data should be collected for explicit and legitimate purposes and limited to what is necessary for those purposes. The ODPC noted that the Respondents relied on "legitimate interest" under section 30(1)(b)(vii) of the *DPA*, claiming that the CCTV was installed for security. While the ODPC acknowledged that security is a legitimate purpose, it held that such purpose must be pursued "*proportionately and within the confines of the law*."[9] It found that the Respondents did not demonstrate that "*they ensured the camera's range did not capture neighbouring property*" and that this failure "*breached the principles of privacy, lawfulness, fairness, and data minimisation*"[10] under section 25(a), (b) and (d) of the *DPA*.

The ODPC found that the Respondents admitted that the camera was later repositioned and that this admission demonstrates that its earlier range extended into the Complainants' property. Furthermore, the ODPC found that even though the adjustment was finally made, "*the prolonged period before the correction amounted to interference with the Complainants' privacy*."[11] The ODPC held that section 40(1) of the *DPA* grants data subjects the right to request rectification of any inaccurate or excessive processing without undue delay and that Regulation 10(4) of Kenya's *Data Protection (General) Regulations*, 2021 requires rectification within fourteen (14) days of such a request or written justification for delay. In reaching a conclusion on this issue, the ODPC determined as follows:

---

9 *Ibid*., at p. 7, para. 37.

10 *Ibid*.

11 *Ibid*., at p. 7, para. 38.

> **The Complainants made several rectification requests** between August 2024 and April 2025, both directly and through intermediaries. **The Respondents only acted in July 2025, almost a year later**. **This delay exceeded the statutory period** and violated the principles enshrined under section 25 of the Act.
> The Office also is cognizant of the fact that **the Respondents did not take adequate steps at the outset to ensure that the CCTV's field of view remained confined within their boundary**. The **Complainants' home is a private space, and continuous surveillance from a neighbouring property, even unintentionally, constitutes unauthorized processing of personal data** contrary to Sections 25(a), (b), (c), and (d) of the Data Protection Act, 2019. **In that regard, the Respondents did not fulfil their obligations in accordance with the Act**.[12] (Emphasis added)

In resolving the second issue, the ODPC found that the Respondents' actions and omission to act infringed the Complainants' right to privacy and violated the data protection principles under section 25 of the *DPA*. Relying on section 56 of the *DPA*[13] and Regulation 14(3) of the *Data Protection (Complaints Handling Procedure and Enforcement) Regulations*, 2021,[14] the ODPC found the Respondents liable and ordered the Respondents to pay to the Complainants the sum of Kenya Shillings Two Hundred Thousand (KES 200,000) as compensation for the infringement of their privacy rights under the *DPA*.

4. Policy and Regulatory Implications of Nderitu's Case on Nigeria's Data Protection and Privacy Landscape

Nigeria's data protection and privacy framework recognizes the right to privacy and embraces the legitimate use of technology for security. However, a gap exists in terms of policy and institutional balancing of these subsets – privacy rights and the use of technology for security. *Nderitu's Case* is the periscope that spots existing regulatory gaps in Nigeria's data governance and projects a roadmap for improvement. A handful of the policy and regulatory implications inherent in the said decision are discussed below.

i. Promoting the Culture of Surveillance Accountability:

---

12 *Ibid*., at p. 8, paras. 40 – 41.

13 Section 65(1) – (4) of the *DPA* provides that a person who suffers damage by reason of a contravention of a requirement of the Act is entitled to compensation for that damage from the data controller. The said section indicates that damage includes both financial loss and non-financial loss (which includes distress).

14 Regulation 14(3)(e) of Kenya's *Data Protection (Complaints Handling Procedure and Enforcement) Regulations*, 2021 provides that the Data Commissioner may make an order for compensation to the data subject and which compensation shall be paid by the Respondent.

In many offices and residential estates in Nigeria, CCTV cameras are positioned in various locations to capture random footages of passersby and adjoining property owners or residents with little or no oversight. The decision in *Nderitu's Case* can serve as a persuasive authority or standard to sanitize this practice and it can champion a new wave of progress in the data privacy and surveillance landscape by creating awareness on the regulation and ethical restraint surrounding the operation of CCTV cameras and processing of personal data of data subjects by individuals and organizations. Three significant standards or tests for appraising modern surveillance technology have been honed by this decision: legitimacy of purpose, spatial limitation, and proportionality of the intrusion.[15] *Nderitu's Case* authenticates the use of CCTV cameras for legitimate and range-controlled security purposes but deprecates any rangeless or snoopy monitoring of persons under the notion of "securing of lives and properties".

ii. **Possibility of Influencing Nigeria's Interpretive Jurisprudence on Technological Privacy and Surveillance:**

Commendable progress has been made by Nigerian courts in expanding the scope of privacy rights to meet the ever-growing modern realities even though our jurisprudence is yet to be tested directly in the context of private CCTV surveillance. In the case of **Emerging Markets Telecommunications Services Limited v. Barr. Godfrey Nya Eneye**,[16] it was decided by the Nigerian Court of Appeal that unauthorized use or disclosure of personal data amounts to an evisceration of the constitutional right to privacy in Nigeria. In the same vein, the Court of Appeal in the case of **Incorporated Trustees of Digital Rights Lawyers Initiative & Ors. v. National Identity Management Commission**,[17] declared that right to privacy guaranteed under section 37 of the *CFRN*, "*extends to anything that is private and personal, including personal communication and personal data*."[18] Though a foreign decision,[19] *Nderitu's*

---

15 This "proportionality" reasoning espoused in *Nderitu's Case* is in harmony with the data protection and privacy safeguards of data minimization, fairness, accountability, transparency, oversight and lawfulness as contained in sections 25, 26, 27, 29, 34, 35, 36 and 37 of the *NDPA*.

16 (2018) LPELR – 46193 (CA) at p. 29, paras. A – D.

17 (2021) LPELR – 55623 (CA).

18 *Ibid*., at p. 32, paras. D – E, per Honourable Justice A. B. Mohammed, JCA.

19 It is hornbook law that decisions based on foreign statutes and Constitutions with identical provisions as the Nigerian statutes or Constitution carry some measure of weight and persuasive effect. See the case of *Attorney-General, Rivers State v. Attorney-General, Akwa Ibom State & Anor.* (2011) 8 NWLR (Pt. 1248) 31 (SC) at p. 177, paras. D – F.

Case could spur the NDPC and Nigerian Courts to give a purposive and expansive constitutional and statutory interpretation of data protection, CCTV surveillance, and privacy rights to the effect that: (a) CCTV surveillance constitutes data processing under the *NDPA*;[20] (b) Owners and operators of CCTV cameras are data controllers; (c) Surveillance beyond the precinct of one's property amounts to an unlawful intrusion under section 37 of the *CFRN*, the *NDPA*, and the *GAID*; and (d) Affected persons can seek declaratory, injunctive, and even compensatory reliefs against such impermissible intrusion.

iii. **Shedding Light on CCTV-specific Regulatory Gap:**

While providing a broad framework for data processing in Nigeria, the *NDPA* does not contain sector-specific provisions for CCTV and other visual surveillance technologies in private and public contexts. The NDPC, as the supervisory authority in terms of compliance,[21] is yet to issue a specific guideline or regulatory framework for CCTV use. As things stand, there is no clear-cut regulation or prescription on signage requirements, spatial limits, operational limits, data retention standards, and CCTV policy. This gap leaves the regulation of CCTVs open-ended and at the mercies of the generic data privacy expectations. In this wise, *Nderitu's Case* redirects the focus of policy makers in Nigeria to the need to issue a CCTV-specific subsidiary legislation for spatial delimitation of the gaze of CCTVs and to ensure improved transparency, compliance, and enforcement.

iv. **Enforcement Constraints and Ignorance on Procedure for Redress:**

The data protection and privacy enforcement mechanism in Nigeria appears weak and underutilized. Though empowered by the *NDPA* to investigate violations,[22] the NDPC faces numerous constraints, including the challenge of technical capacity and limited personnel to monitor thousands of decentralized surveillance systems; limited funding to achieve this purpose; weak penalties for violations; and the reality of dealing with the significant gap between data protection laws and their practical implementation. Furthermore, the affected parties, in most cases, are not aware of their right to seek redress under section

---

20 This would be possible because section 65 of the *NDPA* gives an expansive definition of "*personal data*" to accommodate information that identifies or can identify an individual, directly or indirectly, including images or video recordings. This leads to the ineluctable conclusion that footage captured by CCTV cameras qualifies as "personal data" where "identifiable persons" appear therein.

21 See, section 5 of the *NDPA*.

22 See, sections 5(g) and 6(f) of the *NDPA;* and article 39 (4) – (13) of the *GAID*.

37 of the *CFRN* or under the complaint procedure provided for in the *NDPA* and the *GAID*. This frustrates the progressive move towards accountability and privacy literacy in Nigeria.

v. **Evidentiary Challenges Faced by Complainants and Litigants:**
The burden of proving that a particular CCTV camera captured unauthorized footage or that such footage was stored or disseminated unlawfully is not a walk in the park. It is an exercise that requires basic technological literacy and some form of expertise, which many complainants or litigants may not possess at the outset. This raises the need for privacy protection to be further simplified in terms of its reporting, procedure for investigation, and evidence-gathering process.

5. Legal remedies Available to any Person whose Privacy Rights are Breached or Likely to be Breached by CCTV Surveillance

The following options are open to a person whose privacy rights are breached or likely to be breached by CCTV surveillance:

i. **Instructing or briefing a Lawyer to issue a Data Subject's Standard Notice to Address Grievance ("SNAG") to the CCTV Owner or Operator:**
SNAG is an innovation by the *GAID* and it is a structured way for aggrieved individuals to request internal remediation from a data controller or processor for a perceived violation of their data privacy rights.[23] Through the use of a SNAG, an affected person or his/her representative can formally raise data privacy complaints with a CCTV owner or operator before escalating same to the NDPC. However, issuing a SNAG is not a precondition for lodging a direct complaint with the NDPC or for pursuing legal action.

ii. **Lodging a Complaint with the NDPC:**
Any aggrieved person can submit a petition to the NDPC about data privacy violation by a CCTV owner or operator and this breach can arise where, for example, a CCTV camera's gaze exceeds the boundary of its owner or operator's rights.[24] The NDPC can fine erring CCTV owners or operators, order them to adjust the gaze of their CCTV camera(s), and also order them to cease further unlawful data processing.[25]

iii. **Action for Breach of Data Privacy:**

---

23 See, article 40 and schedule 9 of the *GAID*.
24 See, sections 34(1)(vi) and 46 of the *NDPA;* and article 39 of the *GAID*.
25 See, section 48 of the *NDPA*.

The unlawful collection of a data subject's footage without his/her express consent and/or the extension of the gaze of a CCTV camera beyond the fence of a property could lead to a breach of a data subject's constitutional right to privacy contained in section 37 of the *CFRN* and the prescriptions of sections 24, 25 and 26 of the *NDPA*. This can ground a civil suit for breach of data privacy. Additionally, such a practice violates the *GAID* which provides that personal data must be collected and processed in a lawful and fair manner[26] and that data subjects have the right to object to the processing, request deletion, and seek redress for abuse.[27]

iv. **Enforcement of the Fundamental Human Right to Privacy:**

An affected person can file an application in court for the enforcement of his/her Fundamental Human Right to Privacy which has been breached, is being breached, or is likely[28] to be infringed by a CCTV owner or operator.[29] The need for this option arises where the CCTV owner or operator positions the gaze of the CCTV camera(s) beyond his property boundary to capture footage of the private and family life of an affected person or threatens to do so.[30] Declaratory and injunctive reliefs can be sought restraining the CCTV owner or operator from fixing or further fixing the gaze of the CCTV cameras to exceed the spatial limitation of his property.

6. Recommendations

In line with the policy and regulatory implications discussed above, a number of recommendations are necessary to chart the path of progress for the NDPC, other relevant agencies of government, and CCTV owners and operators in Nigeria. These are highlighted in the succeeding subsections.

6.1 Recommendations for the NDPC and Relevant Agencies:

---

26 See, articles 15, 16, 20, 21, 22, 23, 24, 25 and 26 of the *GAID*.

27 See, articles 38 and 40 of the *GAID*.

28 See the case of *Ezeaduakwa v. Maduka* (1997) 8 NWLR (Pt. 518) 635 (CA) at pp. 660 – 661, para. A, where the Court of Appeal aptly confirmed this point, thus: *"… the Applicant can move to Court to seek for redress* ***immediately he senses some moves on the part of the Respondent*** *to contravene his Fundamental Rights…."* (Emphasis added)

29 See, sections 37 and 46(1) of the *CFRN*; and Order II Rule 1 of the *Fundamental Rights (Enforcement Procedure) Rules*, 2009.

30 See the case of *Chijuka v. Maduewesi* (2011) ALL FWLR (Pt. 586) 517 (CA), where Honourable Justice Danjuma, JCA, relying on section 46(1) of the *CFRN*, held: *"The said section envisages a situation where* ***a threatened breach or violation of one's fundamental right exists. The breach may be in future, as it may not have occurred but merely in sight or feared***." (Emphasis added)

In Nigeria, the *NDPA* has established the legal structure for data protection and privacy but the institutional standards for CCTV deployment leaves much to be desired in terms of compliance and enforcement. To remedy these lapses and bring Nigeria's data protection and privacy regime in line with global best practice, the following policy recommendations are made:

i. **Making CCTV-specific Subsidiary Legislations:**
The NDPC, as the specific data protection regulator in Nigeria, should issue a guideline or regulation for the practice of Visual Surveillance Systems. This subsidiary legislation will prescribe the signage requirements, spatial limits, operational limits, data retention standards, CCTV policy requirements, and reliefs for unlawful capturing by a data controller. This would be something similar to the United Kingdom's *Surveillance Camera Code of Practice*, 2013 and would be a guiding light to individuals and organizations in Nigeria.

ii. **Mandatory Registration for Data Controllers Using Large-Scale Systems:**
Residential and commercial estates, shopping malls, corporate bodies, educational institutions, and other organizations using multiple CCTV units should be mandated to register their surveillance systems with the NDPC, including range or coverage area, data retention periods, and the purpose in which the information is obtained.

iii. **Technical and Ethical Guidelines for CCTV Vendors and Installers in Nigeria:**
To further sanitize the CCTV landscape in Nigeria, the NDPC should certify or accredit CCTV vendors and installers to ensure that devices are configured based on privacy by design which will limit the range and angle of capture to lawful parameters.

iv. **Public Awareness Campaigns:**
Even with the enactment of the *NDPA*, privacy literacy is still at its infancy in Nigeria. There is need for sensitization campaigns to be held in collaboration with Non-governmental Organizations, professional bodies, and relevant government agencies to bring privacy education around CCTV deployment and limits to the physical and virtual doorstep of Nigerians.

6.2 **Recommendations to CCTV Owners and Operators:**
It is axiomatic that prevention is better than cure. In this wise, the following recommendations could save a CCTV owner or operator from sanction and/or liability under Nigeria's data protection and privacy regime:

i. **Conduct a Data Privacy Impact Assessment ("DPIA"):** Where high-risk data processing is to be carried out by CCTV cameras, the owner or operator of the said device must ensure that a DPIA is carried out in consultation with the *NDPC* prior to processing.[31]

ii. **Spatial Limitation:** Regularly audit and adjust the sight lines, field view, or range of your CCTV cameras and ensure that the gaze ends at your boundary. The scope of surveillance must be limited to areas under the lawful control of the data controller or CCTV owner/operator. This is to ensure spatial limitation.

iii. **Rectification of the CCTV Gaze and Prompt Resolution of Complaints:** Respond promptly and resolve the complaint if a concern is raised about the range or gaze of your CCTV cameras.

iv. **Notification of Data Subjects and Transparency:** Ensure that a clear notice is posted where the cameras are installed with barcodes/hyperlinks, informing data subjects about the CCTV usage and data subject rights, and providing contact details for inquiries. This is to ensure transparency and secure informed consent where appropriate.

v. **Legitimate Purpose:** Ensure that the footage captured can only be used for the legitimate, specific, and necessary purpose for which it was collected, which is for personal or property security, and the safety of third parties. This is to ensure purpose limitation of the data collected.

vi. **Data Minimization and Proportionality:** Ensure that only data that is necessary for the stated purpose is processed. This is to ensure data minimization and proportionality.

vii. **Communication of Purpose Specification:** Ensure that the purpose of using CCTV is communicated to the data subjects. This is to ensure purpose specification.

viii. **Right to Access Footage and Right to Request Erasure or Correction:** Ensure that data subjects have the right to access their own footage and that requests for erasure or correction are handled in line with the law.

ix. **Retention of Footage:** Ensure that footage captured is retained for the period necessary to fulfil the purpose it was collected and as required under the law. Data and information obtained via the CCTV device is not personal property that should be kept *ad infinitum*.

[31] See, section 28 of the *NDPA*.

x. **Restrict Third Party Access to and Unauthorized Distribution of Footage:** Ensure that there is restricted access to the footage and measures are put in place to prevent unauthorized sharing, for example, on social media platforms.

xi. **CCTV Policy:** Business owners, commercial offices, and organizations using CCTV for security purposes should endeavour to have a CCTV policy. This policy will set out how the CCTV cameras are to be managed, operated, and used by the organization while ensuring enhanced operational efficiency and user or operator accountability.

7. Conclusion

Legitimate security objectives can co-exist with privacy rights, provided that the pursuit of security respects and stays within the boundaries of privacy. *Nderitu's Case* reviewed in this piece serves as a persuasive template for balancing technology, data ethics and human rights, and exultantly affirms the position that private surveillance without spatial limitation is an interference on the right to privacy. Whichever way the decision in *Nderitu's Case* is considered, it remains an apodictic statement of the law on data protection and privacy which should be embraced beyond the legal and territorial shores of Kenya. It is a clarion call for every individual, adjoining property owner or occupier, business owner, government agency, property manager and/or home owner in Nigeria to move from reactive enforcement of data protection and privacy laws to a preventive governance.

Since there is a global consensus that law must grow with the growth of the society, Nigeria's data protection and privacy landscape could benefit from the interpretive jurisprudence in ground-breaking foreign decisions like *Nderitu's Case*. The principles of legitimate purpose, spatial limitation, and proportionality applied in *Nderitu's Case* would help delineate the boundary between permissible use of technology for security in Nigeria and the impermissible invasion of the privacy of a person by a CCTV's gaze.

For further information on this article and the area of law,
Please contact David Andy Essien
at S. P. A. Ajibade & Co., Lagos by
Telephone (+234 8145942221; +234.811890 3060; +234.8064373384)
Mobile (+2349022470375, + 2348180247252)
Email: dessien@spaajibade.com
www.spaajibade.com