Volume 4 / Issue 8/ August 2026
ISSN:2584-2706
International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.67317/IJMSRT26AUG176

Operationalizing Data Protection in Satellite Earth Observation Workflows: A Three-Segment Privacy Architecture under the Nigeria Data Protection Framework

*Tubolayefa Warekuromor
Head, Mission Planning Division, National Space Research and Development Agency

*Corresponding Author

Abstract
High-resolution Earth Observation (EO) platforms routinely capture spatial Data capable of identifying individual structures and human activities, creating tension between open-Data mandates and privacy rights. While international agencies align with frameworks like the General Data Protection Regulation (GDPR), mechanisms for embedding privacy into national satellite workflows remain underdeveloped. This paper examines the misalignment between Nigeria's Data Protection Act (NDPA) 2023 and EO operations, particularly in rapid disaster response. Using statutory analysis and synthesis of geospatial privacy and GeoAI literature, we evaluate risks across upstream, midstream, and downstream segments of Earth Observation. To overcome manual compliance latency, we propose the Data Protection for Earth Observation Data (DP-EO Data) Architecture, a Privacy-by-Design framework that integrates geographic zoning at sensor-tasking, end-to-end encrypted telemetry, and automated GeoAI spatial anonymization with tiered role-based access control. This architecture operationalizes the NDPA 2023 across the EO value chain, transforming legal obligations into technical safeguards for responsible satellite Data use in national contexts. It enables Nigeria to reconcile Data sovereignty with multilateral commitments under the United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) and the Committee on the Peaceful Uses of Outer Space (UN COPUOS), ensuring responsible use of satellite Data without compromising spatial personal information. The DP-EO Data Architecture offers a transferable model for African space programs seeking to innovate responsibly within domestic legal frameworks.

Keywords: Earth Observation; Geospatial Privacy; Data Governance; Space Policy; Nigeria Data Protection Act; DP-EO Data Architecture; GeoAI; UN-SPIDER; UN COPUOS.

List of Acronyms
AES-256: Advanced Encryption Standard with 256-bit key
API: Application Programming Interface
CNN: Convolutional Neural Network
DP: Differential Privacy
DP-SGD: Differentially Private Stochastic Gradient Descent
DPIAs: Data Protection Impact Assessments
DSA: Data Sharing Agreement
ECOWAS: Economic Community of West African States
EDPB: European Data Protection Board

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

EO: Earth Observation
GAID: General Application and Implementation Directive
GDPR: General Data Protection Regulation
GeoAI: Geospatial Artificial Intelligence
NDPA: Nigeria Data Protection Act
NDPC: Nigeria Data Protection Commission
PII: Personally Identifiable Information
RBAC: Role-Based Access Control
UN COPUOS: United Nations Committee on the Peaceful Uses of Outer Space
UN-GGIM: United Nations Committee of Experts on Global Geospatial Information Management
UN-SPIDER: United Nations Platform for Space-based Information for Disaster Management and Emergency Response
NEMA: National Emergency Management Agency (Nigeria)
OECD: Organisation for Economic Co-operation and Development
POPIA: Protection of Personal Information Act (South Africa)
WGIC: World Geospatial Industry Council

1. Introduction

1.1 Spatial Exposure and Privacy in High-Resolution Remote Sensing

Historically, space sensors operated at coarse spatial resolutions designed for macro-level environmental monitoring, where individual human activity was inherently unresolvable (Kitchin, 2022). Contemporary commercial and sovereign orbital assets, however, routinely capture imagery at high and fine spatial resolutions (ranging from sub-meter to 3-meter ground sample distances). At these scales, remote sensing Data intersects with individual privacy by resolving distinct residential footprints, vehicle arrangements, informal settlements and private property boundaries (McAmis et al., 2024).

When fine-scale satellite imagery is combined with spatial coordinate reference systems or cadastral Databases, environmental telemetry transitions into spatial personal information and Personally Identifiable Information (PII) (Zandbergen, 2014). This capability creates spatial exposure. Spatial exposure is the unconsented capture and potential dissemination of fine-scale spatial features that reveal individual routines or structural vulnerabilities. A 2024 public-perception survey conducted in the United States found that most respondents were unaware that direct-to-consumer commercial satellite imagery at sub-meter resolutions that were fine enough to resolve individual vehicles and building features existed at all, and once informed, expressed discomfort with current capabilities (McAmis et al., 2024). This lack of awareness and unease reflects broader concerns about transparency and oversight in emerging technologies, where public trust is increasingly tied to clear governance and accountability in Data use (Organisation for Economic Co-operation and Development [OECD], 2026).

In response to rapidly advancing sensor capabilities, international legal frameworks have increasingly recognized location Data and high-resolution imagery as potential personal information. Article 4(1) of the European Union's General Data Protection Regulation (GDPR) explicitly defines location Data as personal Data when it can identify an individual, requiring Data controllers to apply principles like Data minimization and purpose limitation (European Union - GDPR, 2016). Multilateral bodies, including the United Nations Committee of Experts on Global Geospatial Information Management (UN-GGIM), have echoed these concerns, advocating for ethical governance and the integration of privacy safeguards into geospatial systems though these remain advisory rather than binding (WGIC, 2020).

Despite these policy directives, operationalizing compliance across the global space sector remains complex. Legacy satellite Data distribution systems, such as those governing major open-Data repositories, were not originally engineered to support real-time, automated redaction of sensitive spatial personal information. As a consequence, space programs face a critical challenge to balance the maintenance of rapid, open Data flow which is essential for scientific and humanitarian purposes while upholding statutory obligations to protect individuals and Data subjects from unauthorized spatial exposure.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

1.2 The Nigerian Context, Multilateral Leadership, and Research Aims

There is a growing imperative to harmonize expanding orbital capabilities with robust domestic digital governance in both emerging and developed economies. Nigeria has advanced its digital governance framework by enacting the Nigeria Data Protection Act (NDPA) in 2023. This law was signed into effect by President Bola Ahmed Tinubu on June 12, 2023, and published in the Federal Republic of Nigeria Official Gazette No. 119, Vol. 110, on July 1, 2023 (Federal Republic of Nigeria, 2023). The NDPA established the Nigeria Data Protection Commission (NDPC) as the independent regulatory body responsible for enforcing Data protection standards across the country.

In the space sector, Nigeria operates as a regional leader through the National Space Research and Development Agency (NASRDA), established under the NASRDA Act 2010. The country also features the Defence Space Administration (DSA) for military operations, Nigeria Communications Satellite Limited (NigComSat) for satellite communications, and a growing number of private sector participants. Strategic oversight is provided by the National Space Council, chaired by the President, with the Vice President serving as Vice Chairman and the Director General of NASRDA acting as Secretary, ensuring coordinated governance across civilian, security, and commercial space activities (James et al., 2014).

Among other functions, NASRDA is mandated to apply space science and technology, including Earth Observation (EO) Data and geospatial intelligence, to benefit society broadly, including supporting disaster response both locally and internationally. NASRDA produces flood and drought impact maps in collaboration with the National Emergency Management Agency (NEMA) and other partners in the Emergency Operations Centre (EOC) during floods and major disasters. Beyond domestic governance, Nigeria's space program engages with international multilateral frameworks. NASRDA hosts the regional support office for the United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) (United Nations Platform for Space-based Information for Disaster Management and Emergency Response [UN-SPIDER], n.d.), contributes technical expertise to the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS), and participates in international emergency Data-sharing mechanisms such as the International Charter: Space and Major Disasters. Across all of these efforts, adapting Data access, utilization, and dissemination protocols to comply with domestic and international frameworks, while embedding spatial privacy in line with the NDPA into national satellite workflows is key.

To understand how other Data protection frameworks have addressed alignment with spatial Data systems, this study also examined Kenya’s Data Protection Act, 2019, and South Africa’s Protection of Personal Information Act, 2013. The goal was to determine whether either law provides a lawful basis for processing personal Data during emergencies that is comparable to the vital-interest basis in Nigeria’s Data Protection Act (NDPA). This basis is essential, as it supports the DP-EO Data architecture proposed in this paper—specifically, the automated override proposed in this paper and the justification for cross-border Data sharing. However, as a synopsis, Kenya’s provision is nearly identical in wording and scope to NDPA's while South Africa’s is not. Neither jurisdiction, to this author's knowledge, has yet produced a published, EO-specific operational framework of the kind proposed here. This paper therefore positions the Nigerian case not as a uniquely generalizable template for all emerging space nations, but as a concrete instance from which comparable African jurisdictions (with a similarly available emergency-processing basis) may adapt elements of the approach. It does not present the DP-EO Data architecture as a legal or policy document, but rather as a set of recommendations grounded in academic research.

During sudden-onset environmental emergencies - such as seasonal riverine flooding across West Africa, which is a recurring and almost annual scenario in Nigeria - rapid dissemination of high-resolution EO Data is required to support disaster response under multilateral mechanisms such as UN-SPIDER and the International Charter: Space and Major Disasters (UN-SPIDER, n.d.). While the NDPA provides bases for processing personal Data to protect vital interests, such processing must remain legally proportionate and time-bounded. Currently, legacy approaches to privacy compliance rely heavily on manual human inspection and redaction, which plausibly introduces delays into emergency distribution pipelines, although the magnitude of that delay has not, to this author's knowledge, been empirically measured for this specific workflow.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

This paper bridges the gap between statutory mandates and technical execution. By clarifying the boundaries of spatial personal information under the NDPA, navigating multilateral Data-sharing obligations, and synthesizing advances in GeoAI and privacy-enhancing technologies, the study proposes a conceptual three-segment privacy architecture. This framework offers a blueprint for national space programs to embed automated Privacy-by-Design controls into their operational ecosystems.

2. Methodology

This study employs an integrative research design that combines legal-regulatory analysis with a targeted synthesis of technical literature to develop a conceptual privacy architecture for Earth observation (EO) Data workflows in national disaster response. The research objective is to reconcile statutory Data protection obligations, particularly under Nigeria's Data Protection Act (NDPA) 2023, with the operational demands of rapid, high-resolution satellite Data dissemination during emergencies. Given this focus on structural alignment between law and technology, the methodology is theoretical and conceptual, prioritizing framework development over empirical measurement or software implementation (Hildebrandt, 2015; Nissenbaum, 2010).

The research proceeded through three structured phases.

2.1 Statutory and Legal Analysis

The first phase established the statutory boundaries governing the processing of spatial personal information. A systematic legal review was conducted of the Nigeria Data Protection Act (NDPA) 2023 and its General Application and Implementation Directive (GAID) 2025, with particular attention to:

- The definition of personal Data (Section 65),
- Lawful bases for processing to protect vital interests during emergencies (Section 25(1)(b)(iii), reiterated for sensitive Data in Section 30(1)(c)), and
- Regulatory constraints on cross-border Data transfers (Sections 41–43).

These provisions were evaluated in light of Nigeria's international and regional obligations, including guidelines from the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS), operational mandates of UN-SPIDER, and the ECOWAS Policy for Disaster Risk Reduction. The latter, developed following the establishment of a Technical Committee on Disaster Management by the ECOWAS Council of Ministers in 2003, provides the regional framework for cross-border emergency coordination among member states, including Nigeria (ECOWAS, 2003). This comparative legal analysis ensures that the proposed DP-EO Data architecture is not only nationally compliant but also interoperable with multilateral disaster response mechanisms.

2.2 Targeted Literature Synthesis

The second phase evaluated the technical feasibility of automating privacy compliance. This phase was a targeted, non-exhaustive synthesis rather than a pre-registered systematic review. Relevant peer-reviewed literature on geospatial privacy, Geospatial Artificial Intelligence (GeoAI), differential privacy applied to raster imagery, and satellite edge computing was identified through iterative keyword search across major computer science and geospatial science venues (including ACM SIGSPATIAL, IEEE Transactions on Geoscience and Remote Sensing, and the MDPI Remote Sensing and Electronics journals).

A small number of preprints are also cited where they are the only available source on a fast-moving technical point (for example, differential privacy survey work); each is flagged as a preprint at first citation so the reader can weigh it accordingly, and none is relied upon for a load-bearing legal or empirical claim. No formal inclusion or exclusion protocol, search-string log, or PRISMA-style screening count was maintained, and the resulting synthesis should be read as a curated conceptual review rather than a systematic one.

The review draws on foundational frameworks such as Cavoukian's (2009) Privacy-by-Design principles and Jabareen's (2009) approach to conceptual framework development, to ensure theoretical coherence and normative grounding.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

2.3 Conceptual Framework Development

In the final phase, the legal constraints identified in Phase 1 were synthesized with the technological capabilities extracted from the literature review in Phase 2. Guided by Privacy-by-Design principles, the standard EO value chain was segmented into three operational phases:

- upstream (mission planning),
- midstream (telemetry and transmission), and
- downstream (ground processing).

Technical privacy controls, such as onboard Data anonymization, edge-based redaction, and access-tiered dissemination protocols, were systematically mapped to these segments to construct a theoretical privacy architecture. The framework was then evaluated through an illustrative disaster-response scenario, following the case-based reasoning approach advocated by Carroll (2000), to assess its operational viability and alignment with real-world workflows.

3. Statutory and Regulatory Context

3.1 Spatial Personal Information under the Nigeria Data Protection Act (NDPA) 2023

Section 65 of the NDPA 2023 defines personal Data as information relating to an individual who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location Data, an online identifier, or one or more factors specific to that individual's physical, physiological, genetic, psychological, cultural, social, or economic identity (Federal Republic of Nigeria, 2023). In satellite remote sensing, a raw raster grid does not explicitly list personal names. However, high-resolution and fine-scale spatial coordinates allow external parties to indirectly identify individuals and extract personal information by cross-referencing physical structures with national land registries or census maps (Zandbergen, 2014; Kounadi & Resch, 2024, preprint).

The GAID,p- 2025 operationalizes the NDPA by prescribing circumstances - including evaluation, scoring, and profiling activities - under which a Data controller must conduct and file a Data Protection Impact Assessment (DPIA) with the NDPC. For an Earth observation (EO) scientist or systems architect, this provides practical design input that transforms compliance from a procedural obligation into an engineering requirement. It establishes a clear threshold for integrating a DPIA-style risk assessment into mission planning workflow, specifically whenever sensor tasking can resolve individual property boundaries. When framed as a forward-looking specification, it becomes a criterion to design against - one embedded in the DP-EO Data architecture presented in this paper from the upstream segment onward - rather than a retrospective evaluation of any existing programme’s current practice.

3.2 Bases for Processing Personal Data during Emergencies

Section 25(1)(b)(iii) of the NDPA provides a lawful basis allowing Data controllers to process personal Data without consent when necessary "to protect the vital interest of the Data subject or another person," a basis reiterated for sensitive personal Data at Section 30(1)(c). In environmental disasters, this provision justifies processing satellite Data over impacted residential areas. Notably, Section 31 of the NDPA, often mistaken for a general emergency exemption, actually addresses the processing of personal Data concerning children or persons lacking legal capacity. It does not apply to the vital-interest basis discussed in this paper.

When designing the architecture proposed in this paper, invoking the vital-interest basis is a starting point rather than a blanket permission. The European Data Protection Board (EDPB) clarifies that comparable derogations do not suspend Data protection principles entirely (EDPB, 2018), and this paper adopts that interpretation as the more cautious - and therefore more defensible - design baseline. This translates into two concrete engineering constraints, not abstract legal tests: necessity and proportionality. In practice, this means unredacted high-resolution Data containing personal information should be geographically bounded to the active disaster zone and time-bounded to the duration of the threat. These constraints are programmatically enforced by the automated statutory override mechanism in the DP-EO Data architecture (specifically prescribed in the documentation for the Upstream segment) and not left to manual judgment after the fact. This embeds compliance into

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

the system architecture, aligning with the GDPR's principle of "Data protection by design and by default" (GDPR Article 25).

One open design question worth naming rather than quietly working around involves the Data subject's side of this exchange. Section 27 of the NDPA requires controllers to inform Data subjects of the purpose and basis of processing, but Section 27(2)(b) exempts a controller from this duty where provision of such information "is impossible or would involve a disproportionate effort or expense". This exemption plausibly applies when satellite imagery captures an entire disaster-affected population, rather than specific, identifiable individuals. Arguably, this reflects a deliberate policy trade-off, not an oversight. Requiring individual notice at population scale during an active emergency would be operationally impractical, and embedding such a requirement into disaster-response workflows could delay the very time-critical actions the vital-interest basis is meant to enable.

Section 36, however, preserves the rights of Data object once identified, and Section 34 maintains rights of access and erasure more generally. Yet the statute, like all comparable laws reviewed in this paper, does not address how a resident of an imaged settlement would learn that imagery was captured at all. This is not a defect in the NDPA or any single agency's implementation arrangements. It is a broader systemic gap for EO-based emergency-response architectures and this research identifies that as a direction future work across the EO ecosystem presented in this paper.

3.3 Reconciling Cross-Border Telemetry with Multilateral Frameworks

Sections 41–43 of the NDPA impose strict controls on the transfer of personal Data outside Nigeria. A critical legal ambiguity arises when satellite operators downlink raw, unencrypted telemetry containing spatial personal information through foreign ground stations, or when sovereign agencies fulfil mandatory international Data-sharing obligations under frameworks such as the International Charter: Space and Major Disasters or UN-SPIDER protocols. NASRDA exemplifies this regional coordination role. It has hosted the UN-SPIDER Regional Support Office since 2008 and maintains an established working relationship with the ECOWAS Commission on disaster-management cooperation (United Nations Platform for Space-based Information for Disaster Management and Emergency Response [UN-SPIDER], n.d.). A statute silent on how this kind of routine cross-border coordination should be reconciled with the NDPA's transfer restrictions leaves the practical resolution to engineers, scientists and compliance officers handling each case individually, rather than settling the question in advance.

To address this, the proposed DP-EO Data architecture treats humanitarian and emergency-response Data sharing as legally permissible under Section 25(1)(b)(iii) (vital interest) and the Section 41–43 adequacy and derogation mechanisms, provided that the technical safeguards in prescribed in the DP-EO Data architecture (specifically for in the documentation of the mid-stream segment) are embedded before transmission. The legal basis and engineering controls are treated as a single, jointly-satisfied requirement and not two separate compliance boxes to tick. This approach aligns with the GDPR's principle of "Data protection by design and by default," which mandates that privacy safeguards be integrated at the earliest stage of system development (GDPR Article 25).

3.4 A Comparison of Emergency Processing Bases in Kenya and South Africa

This paper positions the NDPA-anchored architecture as potentially adaptable to other African jurisdictions. It is therefore worth examining whether Kenya and South Africa offer a comparably clear emergency-processing basis, rather than merely asserting interoperability by naming statutes.

Kenya's Data Protection Act, 2019 (No. 24 of 2019) provides a close match. Section 30(1)(b)(iii) permits processing without consent where necessary "to protect the vital interests of the Data subject or another natural person" - wording that is, apart from minor phrasing, functionally identical to NDPA Section 25(1)(b)(iii). The DP-EO Data architecture proposed in this study could plausibly be adapted to Kenya's legal framework, with statutory citations in Table 1 substituted almost directly, subject to the same institutional and hardware constraints noted throughout.

South Africa's Protection of Personal Information Act, 2013 (POPIA), however, diverges in a way that warrants explicit attention. POPIA's Section 11(1) lawful-processing grounds do not include a distinct "vital interests" basis in the GDPR, NDPA, or Kenya sense. The closest equivalent, Section 11(1)(d), permits processing that "protects a legitimate interest of the Data subject"—a broader, less clearly emergency-specific standard. In practice, this ground is more commonly invoked for purposes

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

such as locating a beneficiary or confirming eligibility for social services (Information Regulator of South Africa, 2022; Bygrave, 2021), rather than for life-safety disaster response. No public enforcement action or advisory opinion has yet applied Section 11(1)(d) to emergency EO Data processing, suggesting it is not the intended or accepted legal basis for such use.

A POPIA-based adaptation of this DP-EO Data architecture would therefore need to establish, as a threshold matter this paper does not resolve, whether disaster-response satellite processing over an affected population fits within Section 11(1)(d)'s legitimate-interest ground or would instead need to rely on the public-law-duty ground at Section 11(1)(e) for public-body responders. This is a genuine point of legal divergence, not a minor drafting difference, and it means the DP-EO Data architecture is more directly adaptable to Kenya statute than to South Africa without further legal analysis specific to POPIA.

4. Synthesis of Literature on Spatial Privacy and GeoAI

The synthesis of contemporary literature on automating spatial privacy in Earth Observation (EO) workflows reveals three distinct thematic approaches: mathematical privacy, deep learning-based masking, and privacy-preserving foundation models. This section evaluates their technical trade-offs, empirical validation, and readiness for operational deployment in African EO systems.

4.1 Trade-offs in Mathematical Privacy (Differential Privacy)

A significant subset of the literature evaluates Differential Privacy (DP) as a mechanism for spatial anonymization. DP provides a formal mathematical framework that bounds privacy risk by injecting calibrated noise (Laplacian or Gaussian) into spatial coordinates or pixel values (Dwork & Roth, 2014). In theory, DP ensures that the presence or absence of any individual's Data does not significantly affect the output, providing a provable privacy guarantee. However, applying DP directly to high-resolution satellite imagery using conventional methods - such as static noise levels and fixed clipping thresholds in Differentially Private Stochastic Gradient Descent (DP-SGD) - results in slow convergence and material degradation of classification utility (Yang et al., 2025). The high dimensionality and spatial correlation of EO Data exacerbate this issue, making naive DP-SGD impractical for real-world applications.

Recent work proposing adaptive, layer-wise noise scaling for satellite image recognition has demonstrated meaningfully improved accuracy and convergence relative to static-noise DP-SGD, narrowing but not eliminating the privacy-utility gap for this Data type (Yang et al., 2025). By modulating noise intensity based on the sensitivity of each network layer, these methods improve convergence and classification accuracy while maintaining privacy guarantees. While this narrows the privacy-utility gap, it does not eliminate it, particularly for fine-grained land cover classification. Thus, DP remains a promising but constrained tool for EO, best suited for aggregated or low-resolution outputs rather than pixel-level analysis.

4.2 Deep Learning and GeoAI for Spatial Masking

To overcome the utility loss inherent in naively applied DP, research has pivoted toward Geospatial Artificial Intelligence (GeoAI). Studies demonstrate that Convolutional Neural Networks (CNNs) can be trained to segment and mask sensitive spatial features containing personal information - such as residential roof footprints - while leaving surrounding environmental pixels comparatively untouched (Janowicz et al., 2020; Cannas et al., 2023). This approach offers higher utility than DP, as it avoids global noise injection and instead applies targeted obfuscation. However, it is not without limitations. Segmentation accuracy depends heavily on training Data, and models trained on formal, grid-like urban layouts may fail to detect atypical or irregular structures - a significant concern in informal settlements or rural areas (Cannas et al., 2023). This creates a residual privacy risk, where unmasked structures remain identifiable.

Moreover, while CNN-based masking is technically feasible, it is not yet production-validated at scale. Most studies remain in the experimental or proof-of-concept phase, with limited deployment in operational EO pipelines. This gap between research and practice is a critical barrier to adoption in national or regional monitoring systems.

4.3 Privacy Risks in GeoAI Foundation Models

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

Beyond pixel-level masking, recent scholarship has begun to examine the systemic privacy and security risks of large-scale GeoAI foundation models—models trained on vast, multimodal geospatial Datasets (Rao et al., 2023). These models, while powerful, can inadvertently memorize and expose sensitive spatial patterns, such as the layout of private properties or the movement of individuals.

Rao et al. (2023) provide the most comprehensive analysis to date, mapping risks across the entire lifecycle of GeoAI models - from Data collection and training to inference and deployment. They identify Data provenance, model inversion, and membership inference as key threats, and propose a research agenda for building privacy-preserving and secure variants. Critically, this work is a vision paper, not a validated framework. As of 2026, no production system has implemented its recommendations at scale. This underscores a broader challenge which is that, while technical solutions are advancing, governance, policy, and institutional capacity lag behind.

4.4 Edge Computing and Agentic Limitations

A fourth, emerging theme explores architectural innovation, specifically, edge computing and agentic AI as a means of embedding privacy by design into EO systems. Orbital edge computing shifts lightweight AI inference from ground stations to satellite processing units, enabling onboard feature detection before downlink (Denby & Lucia, 2020). This reduces ground infrastructure costs and end-to-end latency, but more importantly, it prevents raw personal spatial Data, such as high-resolution imagery of private properties, from ever being transmitted over radio frequencies. While computationally constrained, orbital edge computing represents a privacy-preserving architectural shift, aligning with the Data minimization principle of Data protection law.

Conversely, agentic AI which is an autonomous large language models orchestrating geospatial tools, presents significant operational and legal risks. Benchmarks of state-of-the-art LLM-based geospatial agents show high failure rates due to spatial reasoning errors, rendering them legally precarious for autonomous compliance enforcement without a human-in-the-loop (Talemi et al., 2026). This limits their use in high-stakes governance contexts, where accountability and explainability are non-negotiable. Thus, while edge computing enhances privacy and efficiency, agentic AI introduces new instability. The future of ethical EO systems may lie not in full autonomy, but in human-AI collaboration, where edge intelligence handles preliminary filtering, and human oversight ensures legal and ethical compliance.

5. Theoretical Vulnerabilities in the Global EO Value Chain

Synthesizing the legal constraints with the technological baseline reveals systemic privacy vulnerabilities embedded in the standard Earth Observation (EO) value chain. These are not isolated shortfalls, but structural misalignments between legacy operational design and modern Data protection principles.

5.1 Upstream: Mission Planning and the Data Minimization Gap

Legacy mission planning systems prioritize image geometry, coverage, and sensor efficiency, often collecting wider swaths than strictly necessary for a given task (Holvoet et al., 2018). While justified by cloud-cover contingency, sensor calibration or multi-purpose tasking, this practice results in the routine collection of high-resolution imagery over urban zones during non-emergency periods. This creates a theoretical privacy exposure that exists regardless of intent and this is a direct misalignment with the Data minimization principle enshrined in Nigeria's NDPA (Section 24). As noted in policy analyses, higher-resolution satellite imagery can infringe upon individual privacy by enabling tracking of movements and mapping of private spaces (OECD, 2023). Current traditional planning frameworks do not incorporate privacy-by-design logic, leaving personal spatial Data such as residential layouts or vehicle positions unavoidably captured at the source.

5.2 Midstream: Telemetry and Jurisdictional Ambiguity

Legacy satellite buses typically lack onboard edge-processing capability, necessitating the transmission of entire, unredacted image scenes to ground stations. When these Data flows traverse international relay nodes or foreign ground stations, they trigger the jurisdictional ambiguities discussed in this paper.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

The absence of onboard anonymization or selective downlink means that personal information is exposed during transmission, creating a compliance risk under cross-border Data transfer rules. As demonstrated in security research, Data received at ground stations is distributed to hundreds of downstream systems, amplifying the risk of spoofing or unauthorized access (Firefly Research Team, 2025). This is not a hypothetical concern but a structural vulnerability in the global EO infrastructure.

5.3 Downstream: Manual Redaction and Emergency Response Delays

Globally, manual redaction remains the primary method for preventing unlawful disclosure of personal information in high-resolution imagery (Kitchin, 2022). Compliance personnel review image grids to crop or blur sensitive features, a process that is time-intensive and prone to inconsistency, especially when structures are informal or irregular.

This bottleneck is distinct from initial disaster alerting, which systems like the ECOWAS Multi-Hazard Early Warning and Action System perform rapidly (ECOWAS, 2024). The delay this paper addresses occurs downstream, in the clearance of detailed imagery for damage assessment and coordinated response - a step existing early-warning systems are not designed to perform.

In a sudden-onset emergency such as regional flooding, this delay can impede timely humanitarian action. Moreover, the subjectivity of manual review introduces inconsistency, undermining both privacy protection and operational reliability.

6. A Theoretical Three-Segment Privacy DP-EO Data Architecture

To address the latency of manual downstream redaction, comply with Nigeria Data Protection Act (NDPA) 2023 mandates, and facilitate secure cross-border Data sharing under UN-SPIDER, UN COPUOS, and the ECOWAS Policy for Disaster Risk Reduction, this paper proposes a theoretical Privacy-by-Design architecture for satellite Earth Observation, termed the DP-EO Data Architecture, mapped across the three segments of the EO value chain: upstream mission planning, midstream telemetry processing, and downstream data dissemination.

This DP-EO Data Architecture advances beyond generic Privacy-by-Design guidance (Cavoukian, 2009) and from industry-level policy overviews (WGIC, 2020) by mapping specific technical controls to named statutory provisions of the NDPA at each stage of the satellite Earth Observation (EO) value chain. It is tailored to a jurisdiction - Nigeria - balancing domestic Data sovereignty with multilateral disaster-response obligations. To the author's knowledge, no prior published framework performs this granular, jurisdictionally anchored mapping for an emerging space nation.

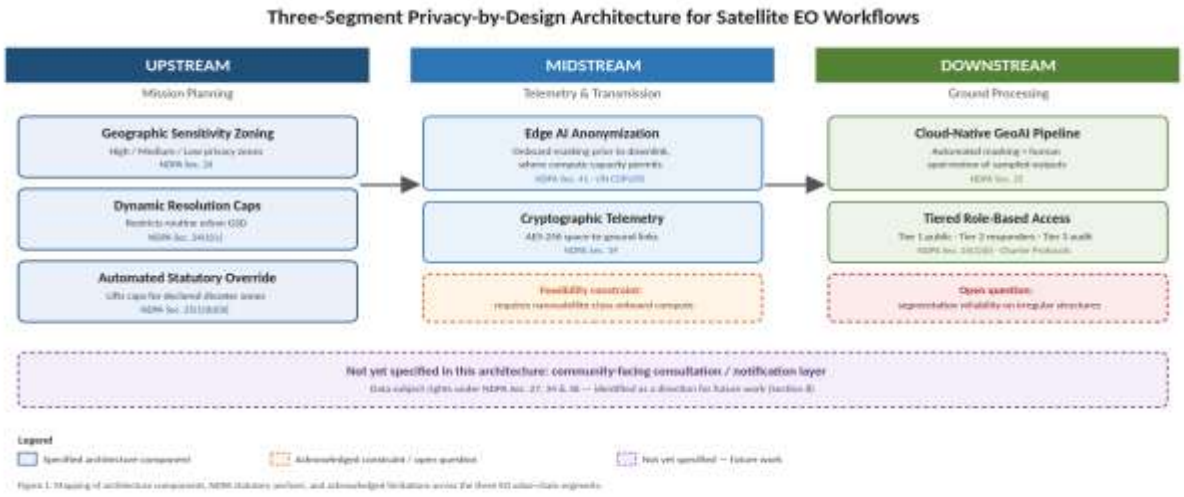

Figure 1. Three-Segment Privacy-by-Design DP-EO Data Architecture

Mapping of DP-EO Data architecture components, NDPA statutory anchors, and acknowledged limitations across the three EO value-chain segments.

Table 1: Components of the Three-Segment Privacy DP-EO Data Architecture

International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.67317/IJMSRT26AUG176

Segment	DP-EO Data Architecture Component	Mechanism of Action	Statutory & Multilateral Alignment
Upstream	Geographic Sensitivity Zoning	Partitions mission control Databases into High/Medium/Low privacy zones.	Principles of Processing (NDPA Sec. 24)
	Dynamic Resolution Caps	Programmatically restricts routine urban collection to non-identifying ground sample distances.	Data Minimization (NDPA Sec. 24(1)(c))
	Automated Statutory Override	Lifts resolution caps exclusively for declared disaster boundaries via authenticated API.	Vital Interest Basis (NDPA Sec. 25(1)(b)(iii); UN-SPIDER Protocols)
Midstream	Edge AI Anonymization	Executes preliminary structural masking (e.g., building footprint blurring) onboard the satellite prior to downlink, where onboard compute capacity permits.	Cross-Border Transfer Mitigation (NDPA Sec. 41; UN COPUOS Standards)
	Cryptographic Telemetry	Secures Space-to-Ground links via AES-256 to insulate Data from foreign relays.	Security of Processing (NDPA Sec. 39)
Downstream	Cloud-Native GeoAI Pipeline	Deploys containerized deep-learning models to automate spatial feature masking, subject to human spot-review of 10–15% of outputs.	Lawful Basis of Processing (NDPA Sec. 25)
	Tiered Role-Based Access	Distributes unredacted imagery only to vetted responders via signed Data Sharing Agreements (DSAs).	Purpose Limitation (NDPA Sec. 24(1)(b); International Charter Protocols)

6.1 Upstream Segment: Privacy-by-Design Mission Planning

This segment embeds privacy into orbital mission planning software. By enforcing dynamic resolution caps based on geographic sensitivity zoning, the DP-EO Data architecture ensures non-essential personal spatial Data is not collected during routine operations.

An automated statutory override triggered only upon official disaster declaration would allow the system to pivot to high-resolution collection exclusively over a declared disaster boundary when human life is at risk, engaging the vital-interest basis at Section 25(1)(b)(iii) of the NDPA and corresponding international emergency activations under UN-SPIDER protocols. This ensures high-resolution collection is exception-based, not routine, preserving privacy while enabling life-saving response.

6.2 Midstream Segment: Secure Telemetry and Edge Anonymization

This segment secures orbital Data transmission against jurisdictional ambiguity and cross-border transfer risks. Where satellite platforms support sufficient onboard compute, containerized GeoAI inference engines (e.g., lightweight U-Net models) execute preliminary structural masking prior to downlink, following the approach demonstrated by Denby and Lucia (2020) for nanosatellites.

Paired with AES-256 encrypted telemetry links, this ensures foreign ground stations act as secure conduits and not points of exposure, while fulfilling UN COPUOS Data-sharing norms and complying with NDPA Section 39.

The feasibility of this segment is contingent on satellite-class hardware. The onboard edge-computing capability documented in the literature (Denby & Lucia, 2020) presumes a nanosatellite-class compute and power budget. For legacy or lower-capability satellites, the DP-EO Data architecture defaults to encrypted downlink with ground-based GeoAI processing, deferring edge benefits until next-generation satellites are fielded. This is a deployment constraint, not a design flaw.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

6.3 Downstream Segment: Cloud-Native GeoAI and Tiered Dissemination

To reduce reliance on manual redaction, this segment deploys cloud-native deep-learning models to ingest telemetry and mask residential footprints. Human spot-review of a statistical sample (e.g., 10–15%) ensures reliability without bottlenecking response.

Data dissemination follows a three-tier API architecture:

- Tier 1: Public, anonymized Data for ECOWAS research.
- Tier 2: Unredacted Data for vetted responders under International Charter DSAs.
- Tier 3: Immutable audit logs for Data protection regulators.

Access is enforced via Role-Based Access Control (RBAC), ensuring high-resolution imagery reaches only authorized personnel.

Notably, the DP-EO Data architecture is regulator- and responder-facing but lacks community visibility. That is, it does not currently include any mechanism through which the communities whose settlements are imaged, who bear the privacy risk this architecture is meant to manage, can have visibility into or input on how their Data is classified and shared. As Bennett et al. (2024) argue, ethical EO must extend beyond compliance to include community engagement.

Incorporating a community-facing consultation or notification layer, for instance, post-activation notifications via local disaster authorities that imagery of an affected area was captured and how it was used is identified here as a design extension worth developing in future work and not a current feature.

7. Illustrative Evaluation: A Disaster Response Scenario

To examine the conceptual DP-EO Data architecture, this section considers an illustrative scenario modelling a cross-border flood emergency within the West African region, where regional space agencies coordinate rapid intelligence sharing via UN-SPIDER and the International Charter: Space and Major Disasters.

Under NDPA Section 25(1)(b)(iii), processing spatial personal Data in this context is legally justified on the grounds of vital interest. However, this justification demands proportionality, security, and accountability, especially when Data crosses borders via foreign ground stations or shared platforms.

This paper does not present a quantified performance comparison between legacy workflows and the proposed DP-EO Data architecture. No published empirical benchmark exists for manual redaction latency in disaster-response EO pipelines and the methodology employed in this study is explicitly theoretical, not empirical.

However, qualitatively evidence from literature supports the two significant claims that inspired the DP-EO Data architecture proposed in this paper:

i. **Manual redaction introduces latency**

Human-in-the-loop review, while essential for accuracy, creates multi-stage bottlenecks in time-sensitive contexts. As Kitchin (2022) notes, compliance workflows requiring individual image inspection inherently delay dissemination, a critical vulnerability during rapid-onset disasters.

ii. **GeoAI enables near-real-time processing**

Deep learning models for semantic segmentation (e.g., U-Net, Mask R-CNN) have demonstrated sub-second inference speeds on cloud and edge platforms in adjacent domains (Rao et al., 2023). Onboard inference has already reduced ground-dependence in nanosatellite constellations (Denby & Lucia, 2020), proving the technical feasibility of early anonymization.

Whether the latency differential between legacy and proposed workflows justifies implementation cost is an open empirical question, one this paper does not resolve. It is, however, a critical direction for future research.

7.1 Architectural Shifts and Their Impact

The proposed DP-EO Data architecture restructures the EO pipeline to embed privacy and security by design, not as afterthoughts. Each shift addresses a specific vulnerability and maps to a named NDPA provision.

Table 2: Mapping the Architectural Shifts and their Impact

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

Legacy Workflow	Proposed Architecture	Vulnerability Addressed	NDPA Alignment
Post-hoc manual redaction	Pre-acquisition Data minimization via dynamic resolution caps and sensitivity zoning	Latency, inconsistency	Section 24(1)(c) – Data Minimization
Cleartext downlink to foreign relays	AES-256 encrypted telemetry + onboard edge screening	Cross-border exposure	Section 39 – Security of Processing; Section 41 – Cross-Border Transfers
Ad hoc sharing via email or physical media	Tiered, logged API access with RBAC and audit trails	Unauthorized access, lack of accountability	Section 24(1)(b) – Purpose Limitation; Section 40 – Accountability

These shifts do not depend on claimed performance gains. Their value lies in structural compliance: they proactively embed legal and ethical constraints into the technical architecture, reducing reliance on error-prone human workflows and opaque Data transfers.
This is the core contribution of the framework: a jurisdictionally grounded, technically feasible model for ethical Earth Observation in emerging space nations.

8. Policy Implications and Conclusion

This paper's principal contribution is a jurisdictionally grounded, technically actionable Privacy-by-Design DP-EO Data architecture for satellite Earth Observation (EO). It maps specific technical controls to provisions of the Nigeria Data Protection Act (NDPA) 2023 across the EO value chain—upstream mission planning, midstream telemetry, and downstream dissemination. This level of operational specificity addresses a critical gap left by generic privacy frameworks and high-level policy analyses, offering national space programs concrete starting points for compliance.
As EO systems grow in resolution and frequency, the capture of spatial personal information, from informal settlements to disaster-affected communities, demands governance that balances open-Data utility with stringent privacy mandates. For Data fiduciaries like NASRDA, this balance is not optional; it is legally required under the NDPA 2023.
When national space agencies engage in multilateral frameworks, such as UN-SPIDER advisory missions, UN COPUOS sessions, or the International Charter: Space and Major Disasters, they must navigate domestic Data sovereignty without compromising international humanitarian obligations. This architecture provides a compliance scaffold that enables responsible Data sharing while respecting the vital interest basis under NDPA Section 25(1)(b)(iii).

8.1 Future Research Directions

This study is theoretical, and its limitations are not caveats but invitations to action. Each gap identifies a clear, actionable next step for applied research and institutional validation.

i. **Institutional Validation**
The DP-EO Data architecture has not yet been tested against NASRDA's technical specifications or NDPC's compliance protocols. The next phase must include document analysis of satellite mission profiles and structured consultations with engineering and legal personnel at NASRDA, NDPC, and ECOWAS disaster coordination units. This will ensure the framework reflects actual agency capacity, not just idealized design.

ii. **Empirical Latency Benchmarking**
While GeoAI promises near-real-time processing, no empirical Data exists on the latency differential between manual redaction and automated pipelines in disaster-response EO workflows. A pilot deployment—using simulated or real tasking—should measure this gap directly, informing cost-benefit decisions for implementation.

iii. **Onboard Compute Feasibility**
The midstream segment assumes edge-AI anonymization, but NASRDA's current or near-term satellite fleet may lack the onboard processing power required. A technical audit of onboard compute (e.g., FPGA/GPU capacity, power budget) is essential before any deployment planning.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

iv. **GeoAI Reliability on Informal Structures**
Automated masking must perform reliably on irregular, informal urban forms—the very structures most common in vulnerable communities. Future work should benchmark segmentation models (e.g., U-Net, DeepLab) against Nigerian and West African urban imagery, focusing on false negatives that could expose individuals.

v. **Community-Facing Governance**
The DP-EO Data architecture currently lacks direct community input. Future iterations should co-develop governance mechanisms with local stakeholders, drawing on critical remote sensing principles (Bennett et al., 2024). Engaging local disaster-response authorities as intermediaries could bridge technical and community needs.

vi. **POPIA-Specific Legal Adaptation**
South Africa's Protection of Personal Information Act (POPIA) lacks a direct vital-interest basis equivalent to the NDPA. Adapting this framework to POPIA would require a dedicated analysis of Section 11(1)(d) (protection of vital interests) and Section 11(1)(e) (legitimate interests), particularly in cross-border humanitarian contexts.

8.2 Broader Applicability and Policy Relevance

While the DP-EO Data architecture presented here is rooted in Nigeria's legal and technical landscape, it offers a transferable model for other African space programs. Kenya and South Africa, both with comparable Data protection statutes and active national space initiatives, could adapt its core principles, subject to the same empirical and institutional validations.

This paper argues that systematically aligning technical controls with statutory provisions is more actionable than generic privacy engineering or isolated legal commentary. It is a practical bridge between law and space science, enabling emerging space nations to innovate responsibly.

In the discourse on shaping Nigeria's Data governance and space policy, this framework serves as foundational literature for diagnosis, dialogue, testing, and refinement, offering real potential to influence how Africa's Earth Observation programs safeguard privacy in the age of high-resolution satellites.

References

1.Bennett, M. M., Gleason, C. J., Tellman, B., Alvarez Leon, L. F., Friedrich, H. K., Ovienmhada, U., & Mathews, A. J. (2024). Bringing satellites down to Earth: Six steps to more ethical remote sensing. Global Environmental Change Advances, 2, 100003. https://doi.org/10.1016/j.gecadv.2023.100003

2.Bygrave, L. A. (2021). *Data Protection Law in South Africa: A Commentary on POPIA.* Oxford University Press.

3.Cannas, E. D., Mandelli, S., Bestagini, P., Tubaro, S., & Delp, E. J. (2023). Deep image prior amplitude SAR image anonymization. Remote Sensing, 15(15), 3750. https://doi.org/10.3390/rs15153750

4.Carroll, J. M. (2000). Making use: Scenario-based design of human-computer interactions. MIT Press.

5.Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

6.Denby, B., & Lucia, B. (2020). Orbital edge computing: Nanosatellite constellations as a new class of computer system. Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '20), 939–954. https://doi.org/10.1145/3373376.3378473

7.Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–407. https://doi.org/10.1561/0400000042

8.Economic Community of West African States [ECOWAS]. (2003). ECOWAS Policy for Disaster Risk Reduction. ECOWAS Commission.

9.Economic Community of West African States [ECOWAS]. (2024). ECOWAS official statement. Africa Regional Platform for Disaster Risk Reduction. https://afrp.undrr.org/publication/ecowas-official-statement

10.European Data Protection Board [EDPB]. (2018). Guidelines 2/2018 on the derogations of Article 49 under Regulation 2016/679. EDPB Secretariat.

11.European Parliament and Council of the European Union - GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
12.Federal Republic of Nigeria. (2023). Nigeria Data Protection Act 2023. Official Gazette, No. 119, Vol. 110, 1 July 2023.
13.Firefly Research Team. (2025). *Spoofing Earth observation satellite Data through radio overshadowing*. In Proceedings of the Network and Distributed System Security (NDSS) Symposium. https://www.ndss-symposium.org
14.General Data Protection Regulation (GDPR). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
15.Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.
16.Holvoet, N., Chaimatanan, S., & Delahaye, D. (2018). *Mission planning for a non-homogeneous Earth observation satellite constellation for disaster response.* In 2018 SpaceOps Conference. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2018-2658
17.Information Regulator of South Africa. (2022). *Advisory Opinion on the Processing of Personal Information by Municipalities for Housing and Service Delivery Purposes.* Case No: IR-AD-2022-001. Pretoria: Information Regulator. https://www.justice.gov.za/inforeg/
18.Iranmanesh, A., & Kamalipour, H. (2023). A configurational morphogenesis of incremental urbanism: A comparative study of the access network transformations in informal settlements. Cities, 140, 104444. https://doi.org/10.1016/j.cities.2023.104444
19.Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. International Journal of Qualitative Methods, 8(4), 49–62. https://doi.org/10.1177/160940690900800406
20.James, G., Akinyede, J., & Halilu, S. (2014). The Nigerian space program and its economic development model. New Space, 2(1), 23–29. https://doi.org/10.1089/space.2013.0041
21.Janowicz, K., Gao, S., McKenzie, G., Hu, Y., & Bhaduri, B. (2020). GeoAI: Spatially explicit artificial intelligence techniques for geographic knowledge discovery and beyond. International Journal of Geographical Information Science, 34(4), 625–636. https://doi.org/10.1080/13658816.2019.1684500
22.Kenya Data Protection Act, No. 24 of 2019 (Kenya).
23.Kitchin, R. (2022). The ethical, privacy and political challenges of geocoding and spatial big Data. Dialogues in Human Geography, 12(2), 174–192. https://doi.org/10.1177/20438206211055818
24.Kounadi, O., & Resch, B. (2024). Privacy risk in GeoData: A survey. arXiv. https://doi.org/10.48550/arXiv.2402.03612
25.McAmis, R., Sim, M., Bennett, M., & Kohno, T. (2024). Over fences and into yards: Privacy threats and concerns of commercial satellites. Proceedings on Privacy Enhancing Technologies, 2024(1), 379–396. https://doi.org/10.56553/popets-2024-0022
26.Nigeria Data Protection Commission [NDPC]. (2025). General application and implementation directive (GAID) 2025. Federal Republic of Nigeria.
28.Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
29.Organisation for Economic Co-operation and Development (OECD). (2023 & 2026). *Expanding access to satellite Earth observation Data: What it means for privacy, security and trust.* OECD Publishing.
30.Protection of Personal Information Act 4 of 2013 (POPIA) (South Africa).
31.Rao, J., Gao, S., Mai, G., & Janowicz, K. (2023). Building privacy-preserving and secure geospatial artificial intelligence foundation models (vision paper). Proceedings of the 31st ACM International Conference on Advances in Geographic Information Systems, 1–4. https://doi.org/10.1145/3589132.3625611
32.Talemi, N. A., Boone, J., & Afghah, F. (2026). Agentic AI in remote sensing: Foundations, taxonomy, and emerging systems. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops, 786–799.

ISSN:2584-2706 DOI: https://doi.org/10.67317/IJMSRT26AUG176

33.United Nations Office for Outer Space Affairs [UNOOSA]. (n.d.). UN-SPIDER knowledge portal. Retrieved 2026, from https://un-spider.org
34.United Nations Platform for Space-based Information for Disaster Management and Emergency Response [UN-SPIDER]. (n.d.). Nigeria Regional Support Office. https://un-spider.org/network/regional-support-offices/nigeria-regional-support-office
35.World Geospatial Industry Council [WGIC]. (2020). Geospatial information and privacy: Policy perspectives and imperatives for the geospatial industry.
36.Yang, Z., Yan, X., Chen, G., & Tian, X. (2025). Adaptive differential privacy for satellite image recognition with convergence-guaranteed optimization. Electronics, 14(18), 3680. https://doi.org/10.3390/electronics14183680
37.Zandbergen, P. A. (2014). Spatial analysis and privacy: An examination of geocoding and location-based services. Geocoding and Location Analysis, 6(1), 37–64.