Digital Surveillance and Human Dignity (*Ḥifẓ al-ʿIrḍ*): An Islamic Ethical Appraisal with Reflections from Nigeria

Assayouti, Ismail Oseni, Ogunwolu, Sulaimon Adio

Islamic Studies Department, Federal College of Education, Abeokuta, Nigeria

DOI: https://dx.doi.org/10.47772/IJRISS.2026.10200341

Received: 19 February 2026; Accepted: 25 February 2026; Published: 10 March 2026

ABSTRACT

The rapid expansion of digital surveillance technologies -including CCTV systems, biometric identification, mobile data tracking and social media monitoring- has transformed public and private spaces across the globe. In Nigeria, these technologies are increasingly deployed for security, governance and commercial purposes, often with limited ethical oversight. This article offers an Islamic ethical appraisal of contemporary digital surveillance through the lens of *ḥifẓ al-ʿirḍ* (protection of human dignity and reputation), a core objective of Islamic law. Drawing on Qurʾānic principles, Prophetic practice, *maqāṣid al-sharīʿah* theory and classical juristic discussions on privacy, suspicion and moral exposure, the study examines the moral boundaries of surveillance in relation to dignity, consent, proportionality and harm prevention. The article adopts a normative-contextual methodology, combining Islamic ethical reasoning with reflections from Nigeria's expanding surveillance landscape, including public CCTV usage, biometric governance systems and digital monitoring practices. It argues that while Islam does not reject surveillance categorically, it imposes strict ethical constraints to prevent dignity erosion, reputational harm and unjustified intrusion. By foregrounding *ḥifẓ al-ʿirḍ* as an underexplored *maqṣad* in digital ethics, the article contributes to contemporary Islamic moral discourse and offers a principled framework for evaluating surveillance practices in Muslim societies.

Keywords: Digital surveillance; *Ḥifẓ al-ʿIrḍ*; *Maqāṣid al-Sharīʿah*; Islamic digital ethics; Nigeria Data Protection.

INTRODUCTION

The rapid expansion of digital surveillance technologies has fundamentally reshaped the governance of privacy, security and individual autonomy in the twenty-first century. From closed-circuit television (CCTV) monitoring in urban centres to large-scale data collection by state, corporate and individual actors, surveillance has become a pervasive feature of both public and private spaces. Scholars in science, technology and society studies have highlighted that while these systems are often justified on grounds of crime prevention, public safety and administrative efficiency, they can simultaneously compromise personal dignity and autonomy when implemented without sufficient ethical and legal safeguards (Lyon, 2018; Zuboff, 2019). In Nigeria, the combination of rapid urbanisation and expanding digital infrastructure has accelerated the deployment of such surveillance mechanisms, particularly in metropolitan areas such as Lagos and Abuja. Yet, discourse around privacy rights, data protection and human dignity remains fragmented and underdeveloped, both in policy circles and academic scholarship.

The tension between the perceived benefits of surveillance for protecting public and private interests (*Maslahah*) and the potential risks to fundamental human rights calls for rigorous normative analysis. Central to this analysis is the ethical challenge of balancing collective security needs with respect for individual dignity -a challenge that becomes especially pressing in societies marked by socio-political pluralism and digital inequality. Islamic ethical thought provides a robust and underutilised normative framework for addressing these issues. Core concepts in Islamic moral philosophy -human dignity (*karāmah*), the honour and protection of private life (*ḥifẓ al-ʿird*) and the ethical limits of state authority- are elaborated in foundational sources including the Qur'ān, the Prophetic Sunna and classical jurisprudential literature (Kamali, 2002; Rahman, 2015). Collectively, these sources affirm the sanctity of individual moral agency and social trust, while simultaneously recognising the legitimate role of communal regulation to safeguard public welfare.

Scriptural sources emphasise the inviolability of the individual's inner life. The Qur'ān asserts, "*Say: No one in the heavens and the earth knows the unseen but Allah; and they do not know when they shall be raised*" (Qur'ān 27:65; 6:59) and reminds believers that *Allah* alone is the Knower of the unseen. The Prophetic tradition similarly cautions against unwarranted intrusion into private affairs, with the Prophet instructing the community to avoid suspicion and clandestine investigation of others (Rahman, 2015). Classical juristic scholarship elaborates a principled balance: oversight to protect communal order is permissible, yet surveillance must not cross ethical boundaries into the unwarranted invasion of privacy or judgement of internal intentions, which are ultimately known only to Allah (Al-Shāṭibī, 1997; Hallaq, 2009).

When applied to the Nigerian context, this normative framework underscores that digital surveillance cannot be evaluated solely in terms of technological capability. Instead, it must be assessed against ethical standards that protect dignity, privacy and human relations. Nigeria's evolving regulatory landscape, shaped by emerging data protection laws, security priorities and public concern over personal data misuse, offers a critical empirical backdrop for this analysis. Despite the growing deployment of CCTV and other digital monitoring initiatives by state and private actors, explicit engagement with Islamic ethical principles regarding dignity and privacy remains limited in both scholarly and policy discourse. This gap highlights the need for an interdisciplinary approach that integrates Islamic normative theory, contemporary ethics of digital governance and the lived experiences of Nigerians navigating increasingly surveilled environments.

This article addresses the following central research question: To what extent can the Islamic objective of *ḥifẓ al-ʿird* provide a coherent ethical framework for evaluating contemporary digital surveillance practices, particularly within the Nigerian socio-legal context? While existing scholarship examines privacy within Islamic law or critiques surveillance from secular human rights perspectives, limited attention has been given to systematically integrating *maqāṣid*-based dignity analysis with contemporary digital governance debates in sub-Saharan Africa. By foregrounding *ḥifẓ al-ʿird* as a normative lens and applying it to Nigeria's surveillance landscape, this study contributes both to Islamic ethical theory and to global discussions on dignity-centred digital governance. The article proceeds as follows: Section Two outlines the conceptual and theoretical foundations; Section Three explains the research methodology; Sections Four and Five provide normative and contextual analysis; Section Six advances policy implications; and the concluding section synthesises findings and proposes directions for future research.

CONCEPTUAL AND THEORETICAL FRAMEWORK

Digital surveillance encompasses a wide array of technologies designed to collect, process and analyse data on individuals and populations. These technologies range from ubiquitous closed-circuit television (CCTV) systems deployed in urban spaces to advanced artificial intelligence (AI)-driven monitoring tools used for behavioural profiling, facial recognition and predictive analytics (Mittelstadt, 2019). While surveillance promises enhanced security and administrative efficiency, it simultaneously raises profound ethical concerns related to privacy, autonomy and human dignity. In the era of algorithmic surveillance and data-driven governance, scholars have underscored how these systems can disrupt fundamental individual freedoms, induce self-censorship and diminish autonomy when deployed without robust protections (Wang et al., 2024; Donoghue, 2025). These ethical tensions are not confined to Western liberal contexts; they are global in scope and have particular salience in jurisdictions such as Nigeria, where regulatory and institutional frameworks are still evolving in response to expanding digital governance infrastructures.

At the heart of ethical debates on surveillance lies the concept of *privacy*, which, although not always explicitly articulated in classical Islamic texts, finds substantive grounding in principles that protect individual dignity and honour. Contemporary Islamic jurisprudential scholarship affirms that privacy encompasses control over personal information, respect for individual integrity and protection against unauthorised intrusion (Auda, 2008). This aligns with broader human rights discourse that frames privacy as a fundamental right, recognised in international law and moral philosophy as intrinsic to human dignity and self-determination. In the Islamic tradition, texts such as Qur'ān 49:12 explicitly warn against unwarranted suspicion and covert investigation, emphasising the moral imperative to respect others' private affairs, while the broader corpus of jurisprudence develops normative safeguards that limit unwarranted intrusion into personal life (Rahman, 2015).

Within the framework of *maqāṣid al-sharīʿah* (higher objectives of Islamic law), the protection of human dignity (*karāmah*) and private life (*ḥifẓ al-ʿird*) are central objectives that inform ethical evaluation of social practices and technologies (Kamali, 2002). Contemporary scholars working at the intersection of Islamic ethics and digital governance emphasise that digital privacy cannot be divorced from these foundational values. For instance, Kama (2008) argues for the urgent development of online data privacy guidelines rooted in trust (*amānah*), privacy (*ḥifẓ al-ʿird*), public benefit (*maṣlaḥah*) and proportionality, in order to guide organisations operating within Muslim communities in managing personal information ethically. Meanwhile, the ethical breaches inherent in digital profiling and personal data surveillance when conducted without informed consent, noting that such practices contravene the dignity-protecting aims of Islamic jurisprudence, particularly when driven by algorithmic manipulation characteristic of surveillance capitalism (Hashmi, 2022). These recent contributions indicate a growing consensus that digital privacy ethics must be grounded in normative resources capable of addressing both the social harm and moral disquiet engendered by pervasive data collection.

Islamic ethical perspectives on digital surveillance also resonate with broader interdisciplinary scholarship. Works exploring digital ethics in the age of AI and surveillance emphasise the need for transparency, accountability and respect for privacy in technological systems, arguing that ethical frameworks must guide technological design and governance to prevent abuses of power and erosions of civil liberties. These studies underscore how algorithmic bias, invasive monitoring and opaque data practices not only threaten individual privacy but risk engendering unequal treatment and discrimination, particularly in contexts of mass surveillance and predictive policing (International Journal of Academic Engineering Research, 2024; ThisDayLive, 2025). The normative insights offered by these secular analyses complement Islamic ethical imperatives by articulating the social harms that arise when surveillance technologies outpace legal and ethical protections.

Table 1: Core Islamic Ethical Concepts and Contemporary Parallels

Concept	Definition (Islamic Perspective)	Contemporary Equivalent	Ethical Function
Karāmah	Inherent human dignity granted by Allah (Qur'an17:70)	Human dignity (human rights law)	Moral foundation of personhood
Ḥifẓ al-ʿIrḍ	Protection of honour, reputation, privacy	Informational self-determination	Limits exposure & intrusion
Tajassus	Prohibited spying and covert investigation (Qur'an 49:12)	Mass surveillance / covert monitoring	Ethical prohibition principle
Maṣlaḥah	Public interest / welfare	Security justification	Conditional legitimisation
Ḍarūrah	Necessity	Emergency powers doctrine	Restrictive exception

In synthesising these perspectives, the present study adopts an analytical framework that situates *ḥifẓ al-ʿird* at the centre of ethical inquiry. This framework interprets privacy not merely as a defensive barrier against unwarranted observation but as an affirmative commitment to maintaining the intrinsic worth of individuals as moral agents capable of self-governance and social participation. Such a conceptualisation aligns with emerging scholarship that views privacy and dignity as interconnected social values that must be protected in both physical and digital realms to preserve human autonomy and social trust. By articulating the contours of digital surveillance and privacy and by grounding these in Islamic normative principles, this section sets the stage for the ensuing ethical appraisal of specific practices and governance mechanisms in the Nigerian context, moving from conceptual grounding to normative evaluation.

METHODOLOGY

This study adopts a qualitative normative-analytical research design grounded in Islamic legal theory and contemporary digital ethics scholarship. It combines doctrinal analysis of primary Islamic sources with contextual policy examination of Nigeria's emerging surveillance and data governance landscape. The objective is not to produce empirical field data, but to develop a principled ethical framework capable of evaluating contemporary digital surveillance practices within Muslim-majority and religiously plural societies. The research proceeds in three stages. First, a doctrinal analysis is undertaken of relevant Qurʾānic verses, Prophetic traditions and classical juristic discussions pertaining to privacy, dignity (*karāmah*), honour (*ʿird*) and the prohibition of unwarranted intrusion (*tajassus*). Particular attention is given to the *maqāṣid al-sharīʿah* framework as elaborated by classical and contemporary scholars, with emphasis on *ḥifẓ al-ʿird* as an ethical objective that regulates social exposure and reputational harm. This stage establishes the normative parameters governing legitimate oversight and impermissible intrusion.

Second, the study engages contemporary interdisciplinary literature on surveillance capitalism, algorithmic governance and digital privacy in order to situate Islamic ethical insights within broader global debates. This comparative engagement enables conceptual clarification and avoids isolating Islamic ethics from wider normative discourses on human rights, proportionality and informational self-determination.

Third, the Nigerian context is examined through analysis of publicly available policy documents, legislative instruments (including the Nigeria Data Protection Act), academic scholarship and documented surveillance practices in public institutions. Nigeria is selected as a case study due to its rapidly expanding digital infrastructure, evolving regulatory framework and pluralistic socio-religious composition. The contextual review is illustrative rather than statistical; it functions to test the applicability of Islamic ethical principles within a contemporary governance environment characterised by institutional asymmetry and uneven regulatory enforcement.

The study therefore advances a normative-contextual methodology: normative in its grounding in Islamic jurisprudential theory and contextual in its application to Nigeria's digital governance landscape. This design allows for ethical evaluation without presupposing empirical neutrality, while maintaining analytical rigour and theoretical coherence.

Analytical Framework and Evaluative Criteria

While this study adopts a normative-contextual methodology grounded in Qurʾānic ethics, Prophetic guidance, and *maqāṣid al-sharīʿah* theory, analytical precision requires a structured evaluative model. *Maqāṣid* scholarship, particularly as developed by contemporary jurists, emphasises that public policy must be assessed through demonstrable necessity, proportionality, and preservation of core protected interests (Kamali, 2008; Auda, 2008). Classical prohibitions against *tajassus* (Qurʾān 49:12) further establish a presumption against unwarranted intrusion into private life. Accordingly, this study evaluates surveillance practices through five interrelated Islamic ethical tests derived from *maqāṣid* theory, juristic principles of public authority, and contemporary governance standards.

Necessity (*Ḍarūrah* Test)

Islamic legal theory permits restricted intrusion only where a clear and evidence-based public harm exists. The doctrine of necessity (*ḍarūrah*) operates within strict limits and cannot be invoked for speculative risk or administrative efficiency (Kamali, 2008). Public welfare (*maṣlaḥah ʿāmmah*) must be demonstrable rather than presumed.

Proportionality Test.

Even where necessity is established, intervention must represent the least intrusive means capable of achieving the objective. Al-Shāṭibī's articulation of *maqāṣid* emphasises that harm removal must not generate equal or greater harm (Auda, 2008). Blanket or indiscriminate data aggregation therefore requires strong justification.

***Ḥifẓ al-ʿIrḍ* Impact Test.**

Protection of dignity and reputation is embedded within the higher objectives of Sharīʿah (Kamali, 2019). Qurʾān 49:12 explicitly prohibits unwarranted suspicion and spying. Surveillance that exposes, profiles, or unjustly associates individuals with wrongdoing conflicts with this protective ethic.

Accountability and Oversight Test.

Islamic governance doctrine rejects arbitrary authority. Ibn Taymiyyah's theory of *siyāsah sharʿiyyah* binds rulers to justice and accountability in pursuit of public welfare. Surveillance lacking oversight mechanisms

therefore risks ethical invalidity.

Consent and Transparency Threshold.

Islamic contractual ethics require informed and voluntary agreement. Contemporary Islamic legal scholarship affirms that informational asymmetry undermines fairness in public dealings (Kamali, 2008). Where compliance is effectively coerced, ethical legitimacy becomes questionable. These criteria convert the study from general ethical reflection into a structured normative assessment model.

Application of the Evaluative Framework to Nigeria's NIN Biometric Integration Policy

To operationalise the framework, Nigeria's National Identification Number (NIN) biometric integration policy provides a useful case. The policy links biometric registration to SIM cards and access to financial and telecommunications services. It is justified primarily on grounds of national security and crime prevention.

Under the necessity test, preservation of life and public order constitutes a legitimate objective within Islamic governance (Kamali, 2019). However, necessity requires demonstrable effectiveness. Comparative governance scholarship warns that mass biometric systems do not automatically correlate with reduced crime unless supported by targeted enforcement mechanisms (Lyon, 2018). Ethical legitimacy therefore depends on evidence rather than assumption. The proportionality test raises deeper concerns. Mandatory biometric consolidation across telecommunications and banking significantly expands state visibility into ordinary civic life. Surveillance studies scholarship demonstrates that large-scale data aggregation increases risks of function creep and secondary use (Zuboff, 2019; Lyon, 2018). If narrower investigative tools could achieve similar outcomes, blanket integration may exceed proportional limits recognised in maqāṣid theory (Auda, 2008).

From the perspective of *ḥifẓ al-ʿirḍ*, centralised identity databases heighten risks of profiling, reputational harm, and wrongful association. Data breaches in weak regulatory environments disproportionately affect vulnerable populations (Greenleaf, 2022). Where individuals may be excluded or stigmatised due to technical errors, the dignity-protective mandate of Islamic law is implicated. Accountability remains critical. Nigeria's Data Protection Act 2023 establishes regulatory structures; however, effective oversight depends on enforcement capacity and judicial accessibility. Islamic governance theory does not tolerate unchecked discretion (Kamali, 2008). Ethical surveillance requires independent review mechanisms.

Finally, consent in the NIN-SIM linkage context is structurally constrained. Denial of telecommunications access for non-registration transforms nominal consent into practical compulsion. Contemporary data protection standards emphasise that consent must be freely given and specific (ICO, 2023). Where refusal results in civic exclusion, voluntariness is weakened.

Security-Centred Justifications for Surveillance in Islamic Governance

Islamic legal thought does not advance an absolutist conception of privacy. The institution of *ḥisbah* historically authorised oversight in matters affecting public morality and market integrity (Cook, 2001). The doctrine of *siyāsah sharʿiyyah* permits discretionary measures to secure justice and social order where grounded in public welfare (Ibn Taymiyyah; see Kamali, 2008).

Classical jurists permitted suspicion-based intervention in cases of credible threat, particularly where public safety was endangered. However, such interventions were tightly circumscribed. Qurʾān 49:12 explicitly prohibits unwarranted suspicion and spying, establishing privacy as the normative baseline.

Contemporary Islamic governance scholarship stresses that public interest cannot override protected rights without strict evidentiary justification (Auda, 2008). Surveillance justified under security doctrines must therefore satisfy necessity and proportionality. Without these constraints, protective governance risks degenerating into systemic intrusion.

Security in Islamic thought is not an independent absolute but a value harmonised with justice and dignity (Kamali, 2019). Accordingly, while targeted monitoring in response to credible threats may be conditionally permissible, mass or indefinite surveillance lacking oversight contradicts the ethical architecture of *maqāṣid alsharīʿah*.

Islamic Norms on Privacy and Human Dignity: Sources and Ethical Limits

Islamic ethical engagement with privacy and dignity is anchored in a moral vision that affirms the intrinsic worth of the human person as a divinely honoured being. The Qur'ān establishes this ontological foundation unequivocally: *"Indeed, We have honoured the children of Ādam"* (Qur'ān 17:70). Classical exegetes interpret this verse as conferring an inherent dignity (*karāmah dhātiyyah*) upon all human beings, irrespective of status, belief, or social position. Contemporary Islamic ethicists have drawn on this foundational principle to argue that any social or political practice -technological or otherwise- that undermines human dignity demands rigorous ethical scrutiny (Kamali, 2023; Auda, 2021). Within this moral universe, privacy is not a peripheral concern but a necessary condition for the preservation of dignity, moral agency and social trust.

The Qur'ānic discourse on privacy is articulated through a network of injunctions that prohibit unwarranted intrusion into personal life. Among the most frequently cited is the prohibition of *tajassus* (spying): *"O you who believe, avoid much suspicion… and do not spy on one another"* (Qur'ān 49:12). This verse has been understood by jurists and ethicists as establishing a general presumption against invasive observation and speculative monitoring of others' affairs. Classical jurists such as al-Qurṭubī and Ibn ʿĀshūr emphasised that *tajassus* undermines social cohesion by eroding trust and exposing individuals to moral vulnerability. Recent scholarship extends this interpretation to contemporary forms of digital monitoring, arguing that algorithmic surveillance and mass data collection represent technologically mediated extensions of the same prohibited ethical posture when conducted without necessity, consent, or proportionality (Kamali, 2023; Auda, 2008).

Prophetic traditions further reinforce these ethical boundaries. Numerous *ḥadīth*s warn against intrusion into private spaces and concealed affairs, including the Prophet's instruction: *"Do not search for the faults of Muslims, for whoever searches for their faults, Allah will search for his faults"* (reported in Abū Dāwūd). Jurists have historically drawn from such reports to limit the scope of state and communal oversight, insisting that moral accountability is primarily inward and voluntary, not externally coerced. Al-Ghazālī, for instance, cautioned against excessive surveillance by authorities, arguing that it cultivates hypocrisy rather than moral reform. Contemporary scholars have revitalised this argument in digital contexts, noting that constant surveillance produces behavioural conformity rooted in fear rather than ethical conviction (Auda, 2021; Hashmi, 2022).

From a jurisprudential standpoint, the principle of *ḥifẓ al-ʿird* -the protection of honour, dignity and reputation- occupies a critical place within the *maqāṣid al-sharīʿah*. Although classical formulations of the *maqāṣid* emphasised the preservation of religion, life, intellect, lineage and property, later jurists and modern theorists have persuasively argued that *ʿird* constitutes either an independent objective or an indispensable dimension of these foundational aims (Al-Shāṭibī, 1997; Kamali, 2023). In contemporary Islamic legal theory, *ḥifẓ al-ʿird* has been expanded to include protection against reputational harm, exposure of private data and unwarranted public scrutiny -concerns that resonate strongly with debates on digital privacy and data ethics.

Recent Islamic legal and ethical scholarship increasingly frames digital surveillance as a test case for the operationalisation of *maṣlaḥah* (public interest) and *ḍarūrah* (necessity). While Islamic law recognises the legitimacy of limited surveillance to prevent concrete harm or uphold public order, such measures are subject to stringent ethical conditions: necessity must be real and demonstrable, intrusion must be proportionate and harm must not outweigh the anticipated benefit. Scholars writing in the post-COVID and AI-governance era caution

that appeals to security and efficiency are frequently overextended to justify pervasive monitoring, thereby hollowing out the very moral values that *maṣlaḥah* is meant to protect (Kamali, 2023). Within this framework, blanket or indiscriminate digital surveillance -particularly when automated, opaque and detached from meaningful oversight- constitutes a violation of *ḥifẓ al-ʿird* rather than its protection.

Importantly, Islamic ethics does not conceptualise privacy as absolute isolation from communal responsibility. Rather, it advances a relational model in which personal dignity is preserved within a morally accountable society. This balance is evident in juristic discussions on *hisbah* (public moral oversight), which permit intervention only in cases of manifest public harm (*munkar ẓāhir*) while strictly prohibiting intrusion into concealed or private matters (*munkar khafī*). Contemporary scholars have drawn parallels between these distinctions and modern debates on targeted versus mass surveillance, arguing that Islamic norms clearly reject indiscriminate data collection that treats all individuals as potential suspects (Auda, 2021; Hashmi, 2022).

Thus, Islamic normative sources articulate a coherent ethical architecture that affirms dignity, restrains surveillance and prioritises moral agency over coercive control. When translated into the digital age, these principles challenge dominant paradigms of surveillance governance that normalise constant observation as a prerequisite for security. Instead, they propose an ethics of restraint -one that demands transparency, accountability and moral justification for any intrusion into private life. This normative grounding provides a critical lens through which contemporary surveillance practices, particularly within socio-legally plural contexts such as Nigeria, may be ethically assessed. The next section builds upon this foundation by examining how these Islamic ethical norms intersect with Nigeria's emerging digital surveillance landscape and regulatory frameworks.

Ethical Appraisal: Digital Surveillance and *Ḥifẓ Al-ʿirḍ*

Islamic ethical engagement with digital surveillance is best situated within the broader framework of *maqāṣid al-sharīʿah*, which articulates the fundamental objectives of Islamic law aimed at safeguarding religion (*ḥifẓ aldīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-ʿaql*), progeny (*ḥifẓ al-nasl*) and property (*ḥifẓ al-māl*) (Kamali, 2002). Embedded within and intersecting these objectives is the protection of human dignity and honour, conceptualised through *karāmah* and *ḥifẓ al-ʿirḍ*. These concepts occupy a central normative position because they regulate social interaction, personal autonomy and the moral limits of observation. While contemporary surveillance technologies are frequently justified as instruments of *ḥifẓ al-ḍarūrāt*, particularly in relation to security and public order, their unrestrained deployment risks undermining *ḥifẓ al-ʿirḍ*, especially when ethical safeguards are weak or absent (Al-Shāṭibī, 1997; Hallaq, 2009). This structural tension between collective security and individual dignity necessitates a principled ethical appraisal grounded in both revealed sources and disciplined moral reasoning.

Table 2: *Maqāṣid* vs Surveillance Tension Matrix

Maqāṣid Objective	How Surveillance Claims to Protect It	Risk to *Ḥifẓ al ʿIrḍ*	Ethical Assessment
Ḥifẓ al-Nafs	Crime prevention, terrorism monitoring	Over-policing & profiling	Requires proportionality
Ḥifẓ al-Māl	Fraud detection, digital banking monitoring	Data commodification	Consent-dependent
Ḥifẓ al-ʿAql	Behavioural analytics	Psychological manipulation	Ethically problematic
Ḥifẓ al-Dīn	Moral monitoring	Religious policing	Strongly restricted
Ḥifẓ al-ʿIrḍ	Protection of reputation	Data exposure & stigma	Central normative limit

Surveillance, by its very nature, establishes an asymmetrical relationship between the observer and the observed. Contemporary scholars of digital governance describe this asymmetry through the lens of "surveillance capitalism," wherein personal data -ranging from movement patterns to behavioural preferences- are systematically extracted, analysed and commodified for predictive and regulatory purposes (Zuboff, 2019). The ethical concern here transcends technological capacity; it reflects a deeper moral shift from norms of informed consent and reciprocal trust to regimes of unilateral observation and opaque data processing. From an Islamic ethical perspective, the central problem lies not merely in the act of observation itself but in its detachment from moral accountability, thereby threatening *ḥifẓ al-ʿirḍ* through the erosion of personal dignity, reputation and moral agency.

The Qur'ān consistently affirms the sanctity of personal boundaries and private moral space. Although it does not explicitly address modern surveillance technologies, it articulates ethical principles that implicitly constrain intrusive forms of observation. Qur'ān 49:12 categorically prohibits suspicion and clandestine investigation *"Indeed, some suspicion is sin … and do not spy"*- thereby establishing a normative boundary against unjustified intrusion into the affairs of others. Such injunctions underscore that observation, where unavoidable, must be ethically restrained and justified by clear moral necessity. Classical juristic discourse reinforces this position by recognising oversight only in contexts of demonstrable harm and even then subjecting it to proportionality, evidentiary rigor and procedural fairness (Hallaq, 2009). These ethical constraints apply with equal force to physical surveillance mechanisms such as CCTV and to contemporary digital practices such as data mining, biometric identification and algorithmic profiling.

The juristic principle of *ḥifẓ al-ʿirḍ* finds a strong conceptual parallel in modern notions of privacy, personhood and informational self-determination. Classical Islamic jurisprudence historically protected a wide range of personal domains, including bodily privacy, confidentiality of correspondence, inviolability of domestic spaces and protection against slander and reputational harm (Kamali, 2002). Although premodern jurists did not encounter networked surveillance systems, their ethical commitments remain normatively transferable. Central to this tradition is the principle of *satr*, which presumes that individuals' private affairs should remain concealed unless compelling moral or legal grounds justify disclosure. This ethical orientation stands in tension with contemporary data-driven models that normalise continuous visibility and indiscriminate data accumulation.

Recent contributions by Muslim ethicists and scholars of Islamic digital ethics have extended these classical protections into the digital sphere. Mohamud and Uday (2024) argue persuasively that digital privacy, understood as the right to control personal information and resist unwarranted exposure, is integral to both *ḥifẓ al-ʿirḍ* and *karāmah*. Practices such as algorithmic profiling, indefinite data retention and covert tracking are thus ethically problematic because they violate the Islamic moral assumption that the "self" constitutes a protected domain. Complementing this view, Rofiq et al. (2025) emphasise that ethical data governance must be anchored in *amānah* and *maṣlaḥah* to prevent systemic harm to individual and communal dignity.

Underlying these discussions is a deeper juristic presumption: privacy and moral innocence remain operative until concrete harm is demonstrably established. Within Islamic ethical reasoning, surveillance is justified only where a clear causal link exists between observation and the prevention of identifiable harm and where less intrusive alternatives are demonstrably insufficient. This principle closely parallels contemporary doctrines of proportionality and necessity in administrative and human rights law, yet it is rooted in a distinctly Islamic moral anthropology that privileges restraint, humility and respect for human dignity.

A persistent ethical deficiency in contemporary surveillance regimes lies in the absence of meaningful consent. Empirical studies indicate that even in technologically advanced societies, individuals exercise minimal control over how their data are collected, processed and repurposed (International Journal for Multidisciplinary Research, 2024). In contexts such as Nigeria, where data protection infrastructures are still evolving and enforcement remains uneven, these vulnerabilities are further amplified. Islamic ethics assigns profound moral weight to intentionality and consent; consequently, observation or data use without informed consent is ethically suspect unless justified by an overriding public interest grounded in *maṣlaḥah*. The opacity of algorithmic governance and complex digital infrastructures thus poses a serious challenge to Islamic ethical commitments to voluntary moral agency.

This ethical position diverges sharply from utilitarian frameworks that assess surveillance solely in terms of aggregate security outcomes. Islamic ethical theory insists on a more comprehensive moral calculus, one that evaluates not only consequences but also methods and moral costs. As Rahman (2025) observes, digital technologies must be scrutinised not merely for what they achieve, but for how they reconfigure social relations, distribute power and normalise forms of intrusion that erode dignity over time.

Surveillance technologies also tend to reproduce and intensify existing power asymmetries. At the global level, technologically advanced states and corporate actors deploy sophisticated monitoring infrastructures to conduct geopolitical surveillance and behavioural extraction, often with limited transparency or accountability (Smith & Kumar, 2023). These global dynamics find local expression within Nigeria, where expanding surveillance practices intersect with socio-economic inequalities, resulting in uneven exposure to monitoring and unequal capacity to challenge abuses. Islamic ethical teachings on justice (*ʿadl*), equity (*musāwāh*) and protection of the vulnerable provide critical normative resources for interrogating such asymmetries and resisting their normalisation.

Table 3: Ethical Conditions for Legitimate Surveillance (Islamic Criteria)

Ethical Condition	Juristic Basis	Contemporary Legal Parallel
Necessity (*Ḍarūrah*)	Al-Shāṭibī	Emergency doctrine
Proportionality	*Usul al-Fiqh* harm principle	Human rights law
Clear Public Harm	*Hisbah* limits	Criminal threshold
No Indiscriminate Monitoring	*Tajassus* prohibition	Anti-mass surveillance norms
Accountability	*ʿAdl* & *Amānah*	Oversight institutions
Consent (Where Possible)	Moral intentionality	Data protection law

Classical jurists consistently warned against the unjust exercise of power, regardless of its source or intent. Applied to the digital age, this caution demands surveillance governance frameworks that are transparent, accountable and responsive to harm. Such an approach aligns with emerging international human rights discourses advocating algorithmic fairness, non-discrimination and participatory oversight, while grounding these concerns in a moral tradition that prioritises dignity over expediency.

Empirical and Contextual Reflections from Nigeria

The ethically charged debates on digital surveillance and privacy acquire concrete urgency when situated within the Nigerian socio-legal and technological landscape. Recent scholarship on Nigeria's digital economy reveals that surveillance capitalism -the commercial appropriation of personal data through pervasive monitoring practices- poses significant challenges to individual autonomy and dignity, particularly in contexts where regulatory institutions are still consolidating capacity and public awareness remains limited (Singler & Babalola, 2024). This dynamic is visible in the rollout of emerging surveillance technologies such as CCTV infrastructure, biometric systems and algorithmic profiling tools, which have been increasingly adopted in urban centres to address public safety and administrative inefficiencies. However, the ethical implications of these deployments extend far beyond instrumental justifications, implicating fundamental questions of consent, transparency and socio-political equity.

Table 4: Nigerian Surveillance Landscape Overview

Surveillance Type	Actor	Justification	Ethical Concern
Public CCTV	State	Crime control	Overreach
Biometric ID (NIN)	Government	Identity verification	Data centralisation

AI-based profiling	Public institutions	Efficiency	Bias & opacity
Telecom data tracking	Private sector	Marketing/security	Consent deficit
Electoral biometrics	Electoral bodies	Fraud prevention	Transparency issues

Scholars examining Nigeria's legal framework identify a crucial tension between existing privacy protections and the operational realities of contemporary surveillance. The Nigeria Data Protection Act (NDPA) of 2023 embodies an important legislative effort to align national practice with international standards such as the European Union's GDPR. Nevertheless, enforcement challenges persist. Weak institutional capacity, limited public literacy on data rights and broad national security exceptions have diluted the efficacy of these protections, creating spaces in which surveillance can flourish with minimal accountability (Singler & Babalola, 2024). These gaps are compounded by the fact that many surveillance technologies operate through opaque contracts, proprietary systems and private data brokers whose operations are scarcely regulated, much less subject to democratic oversight.

Recent scholarship on AI deployment and surveillance systems highlights significant ethical challenges, especially related to algorithmic bias, privacy and discriminatory outcomes. For example, Almasoud and Idowu (2025) show that predictive policing algorithms can amplify societal biases and undermine fairness in decision-making processes. Similarly, research on AI adoption in Nigerian public institutions underscores broad concerns about transparency, regulatory capacity and ethical governance of AI system (Olawale et al., 2025). The rapid deployment of such systems often outpaces the development of ethical governance frameworks, thereby exposing citizens to potential harms that are both structural and relational. These harms include the erosion of trust in public institutions, arbitrary exclusions based on imperfect data classifications and the entrenchment of socio-economic inequalities through differential access to redress mechanisms. In a context where infrastructural deficits and institutional opacity are already salient, the introduction of advanced surveillance systems without adequate safeguards risks deepening existing vulnerabilities.

Academic commentary on digital surveillance and privacy in Nigeria also highlights a broader cultural and political dimension. Public debate around biometric systems, such as national identity and electoral verification tools, often reveals a persistent scepticism toward government capacity and intention, rooted in historical experiences of administrative opacity and governance failures. Citizens' mistrust in state institutions can thus amplify ethical concerns about surveillance, as the technology becomes entangled with wider anxieties about state power, accountability deficits and democratic fragility. These dynamics mirror global patterns observed in the literature, where surveillance technologies are deployed in contexts of weak governance, often resulting in a disproportionate burden on marginalised groups and a diminution of civil liberties under the banner of security enhancement.

In Islamic ethical terms, these empirical vectors in Nigeria heighten the relevance of normative principles such as *ḥifẓ al-ʿird* and *ʿadl* (justice), because the real-world ramifications of surveillance extend into domains of social trust, dignity and equitable treatment. The Nigerian experience thereby underscores a core insight from the broader literature: that surveillance practices cannot be ethically assessed in abstraction from their sociopolitical contexts. Instead, they must be evaluated through integrated frameworks that consider how technology interacts with legal systems, cultural norms and power relations. This empirical specificity enriches the normative appraisal advanced in earlier sections, grounding it in the lived realities of a pluralistic and digitally evolving society.

Table 5: NDPA 2023 vs Islamic Ethical Principles

NDPA Provision	Ethical Strength	Gap Identified	*Ḥifẓ al-ʿIrḍ* Assessment
Data subject rights	Strong normative alignment	Weak enforcement	Partially protective
Consent requirement	Positive	Clickwrap weakness	Procedural, not substantive

National security exception	Broad	Abuse risk	Ethically sensitive
Data minimisation	Aligned	Poor compliance	Needs enforcement

Moreover, recent interdisciplinary work in Nigeria reinforces the need for contextualised ethical frameworks that account for both technological innovation and socio-ethical robustness; studies on digital governance emphasise the importance of rights-based approaches to privacy and AI governance that are culturally cognisant and legally enforceable (Alakitan & Makinde, 2025). Such approaches foreground not only statutory compliance but also ethical literacy, public participation and institutional accountability as pillars of a just digital order. In this regard, the Islamic ethical lens developed in earlier sections complements secular human rights frameworks by offering additional moral resources -rooted in dignity, trust and communal welfare- that resonate with Nigeria's religious and cultural pluralism.

Policy And Regulatory Implications

The preceding analysis demonstrates that ethical legitimacy in surveillance governance cannot rest solely on security justification. It requires institutional safeguards that operationalise necessity, proportionality, dignity protection, accountability, and meaningful transparency. Accordingly, the following reforms are proposed within Nigeria's evolving data protection framework.

First, an independent Data Protection Compliance Tribunal should be established under subsidiary regulation of the Nigeria Data Protection Act 2023. While the Act provides regulatory authority through the Nigeria Data Protection Commission, adjudicatory capacity remains limited. A specialised tribunal with statutory independence, public annual reporting obligations, and appellate review channels would strengthen oversight and align with the accountability principles recognised in Islamic governance theory (Kamali, 2008; NDPA, 2023). Transparent publication of surveillance authorisations and aggregate compliance statistics would further institutionalise answerability.

Second, a Surveillance Necessity Certification Requirement should be introduced for large-scale biometric or data integration initiatives. Before deployment, agencies should be required to publish a narrowly tailored impact assessment demonstrating (a) demonstrable public harm, (b) proportional design, (c) defined retention limits, and (d) safeguards against reputational injury. This approach parallels international data protection standards requiring data protection impact assessments for high-risk processing (ICO, 2023). Embedding such certification procedures would reflect the Islamic legal doctrine that necessity must be evidence-based rather than presumed.

Third, consent procedures under NIN-linked services should be restructured through mandatory plain-language data notices not exceeding 250 words, accompanied by clearly stated retention periods and inter-agency datasharing limits. Contemporary regulatory practice emphasises that consent is valid only when intelligible and freely given (ICO, 2023). Where essential civic participation depends on registration, additional transparency safeguards become ethically indispensable.

Fourth, statutory limits on data retention and secondary use should be codified. Biometric and identity data should be retained only for explicitly defined security purposes and subject to automatic review after fixed intervals. Comparative data governance research demonstrates that indefinite retention increases risks of misuse and function creep (Lyon, 2018; Greenleaf, 2022). Institutionalising retention ceilings would reflect the proportionality constraints inherent in maqāṣid theory (Auda, 2008).

Fifth, a publicly accessible Dignity Redress Mechanism should be created to allow individuals to challenge wrongful profiling, identity misattribution, or reputational harm arising from surveillance databases. Protection of reputation (*ḥifẓ al-ʿirḍ*) requires accessible correction procedures. Without remedy pathways, even well-intentioned systems risk undermining public trust and violating the moral architecture of Islamic law.

Table 6: Policy Recommendations Matrix

Policy Domain	Operational Recommendation	Islamic Ethical Foundation	Institutional Mechanism
Oversight & Accountability	Establish independent Data Protection Compliance Tribunal with annual public reporting	*ʿAdl* (justice); *Amānah* (trust)	Statutory tribunal under NDPA with appellate review
Necessity Verification	Mandatory Surveillance Necessity Certification & Impact Assessment before large-scale biometric deployment	*Ḍarūrah* (restricted necessity); *Maṣlaḥah* (public welfare)	Pre-deployment regulatory approval & published impact reports
Consent & Transparency	Plain-language data notices (≤250 words) specifying retention & data-sharing limits	Moral intentionality; contractual fairness	Subsidiary regulation under NDPA
Data Minimisation	Statutory limits on data retention & prohibition of undefined secondary use	Proportionality; harm prevention	Automatic review periods & retention ceilings
Dignity Protection	Public Dignity Redress Mechanism for wrongful profiling or reputational harm	*Ḥifẓ al-ʿIrḍ* (protection of dignity)	Accessible complaint portal & correction mandate

These measures do not reject surveillance as a governance tool. Rather, they translate Islamic ethical constraints into institutional design principles. By embedding necessity verification, proportional safeguards, independent oversight, intelligible consent, and reputational protection within regulatory architecture, Nigeria's surveillance regime can move closer to a model that harmonises public security with the preservation of human dignity.

CONCLUSION

Towards a Just and Dignity-Centered Surveillance Regime

This study has argued that digital surveillance, while not categorically prohibited within Islamic governance, is ethically legitimate only under strict normative constraints. By foregrounding *ḥifẓ al-ʿirḍ* as a central but underexplored objective of Sharīʿah, the article has demonstrated that dignity and reputational protection must function as limiting principles in the design and deployment of surveillance systems. Through a structured evaluative framework grounded in necessity, proportionality, dignity impact, accountability, and consent transparency, the analysis moved beyond abstract moral reflection to normative assessment. Application of this framework to Nigeria's NIN biometric integration regime revealed that security justification alone is insufficient; ethical validity depends on demonstrable necessity, narrowly tailored design, enforceable oversight, and accessible redress mechanisms.

Engagement with security-centred doctrines such as *ḥisbah* and *siyāsah sharʿiyyah* further clarified that Islamic legal tradition accommodates protective intervention, yet does not sanction indefinite or indiscriminate intrusion. Surveillance is therefore conditionally permissible, but only within a governance architecture that harmonises public safety with the inviolability of human dignity. The article's contribution lies in translating *maqāṣid*-based ethics into institutional design principles. By proposing concrete oversight, certification, transparency, retention, and redress mechanisms, it bridges Islamic moral theory and contemporary regulatory practice. In doing so, it advances a dignity-centred framework capable of informing digital governance debates in Muslim societies navigating expanding surveillance infrastructures.

REFERENCES

1. Abdul Rahman, M. F., Rofiah, N., & Nurbaiti. (2025). Islamic bioethics construction. *Journal of Comprehensive Science, 4*(3). https://www.researchgate.net/publication/390593246_Islamic_Bioethics_Construction
2. Alakitan, M., & Makinde, E. (2025). Where are the ethical guidelines? Examining the governance of digital technologies and AI in Nigeria. *Policy & Internet, 17*, Article e416. https://doi.org/10.1002/poi3.416
3. Al-Shāṭibī, I. I. (1997). *Al-Muwāfaqāt fī uṣūl al-sharīʿah* (M.-U. Faruqi, Trans., Vols. 1-3). Islamic Texts Society. https://www.islamictextssociety.org/product/al-muwaffaqat/
4. Auda, J. (2008). *Maqasid al-shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought. https://iiit.org/en/book/maqasid-al-shariah-as-philosophy-of-islamic-law-a systems-approach/
5. Auda, J. (2021). The maqasid methodology: A guide for the researcher in the research network. *Journal of Contemporary Maqasid Studies, 1*(1), 1-30. https://doi.org/10.52100/jcms.v1i1.59
6. Cook, M. (2001). *Commanding right and forbidding wrong in Islamic thought*. Cambridge University Press. https://doi.org/10.1017/CBO9780511496364
7. Donoghue, R. (2025). Freedom under algorithms: How unpredictable and asocial management erodes free choice. *Frontiers in Artificial Intelligence, 8*, 1582085. https://doi.org/10.3389/frai.2025.1582085
8. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Morley, J., et al. (2018). AI4People -An ethical framework for a good AI society. *Minds and Machines, 28*(4), 689-707. https://doi.org/10.1007/s11023-018-9482-5
9. Goldschmitt, M., Gleim, P., Mandelartz, S., Kellmeyer, P., & Rigotti, T. (2025). Digitalizing informed consent in healthcare: A scoping review. *BMC Health Services Research, 25*, Article 893. https://doi.org/10.1186/s12913-025-12964-7
10. Greenleaf, G. (2022). Global data privacy laws 2022. *Privacy Laws & Business International Report*. https://www.privacylaws.com/Publications/Global-Data-Privacy-Laws.aspx
11. Hallaq, W. B. (2009). *An introduction to Islamic law*. Cambridge University Press. https://www.cambridge.org/core/books/introduction-to-islamic law/3F1B6A89A66E7F5E64D4A8B1B2B55F45
12. Hashmi, S. H. (2022). Islamic ethics and artificial intelligence. *Journal of Religious Ethics*. https://doi.org/10.1111/jore.12412
13. Ibn Taymiyyah. (2008). *Al-siyāsah al-sharʿiyyah fī iṣlāḥ al-rāʿī wa-al-raʿīyah* [Public policy in reforming the ruler and the ruled]. Dār ʿĀlam al-Fawāʾid lil-Nashr wa-al-Tawzīʿ. https://openlibrary.org/works/OL325949W/
14. Kamali, M. H. (2008). *Sharīʿah law: An introduction*. Oneworld Publications. https://oneworld-publications.com/work/shariah-law/
15. Kamali, M. H. (2002). *Principles of Islamic jurisprudence* (3rd ed.). Cambridge University Press. https://www.cambridge.org/core/books/principles-of-islamic
16. Kamali, M. H. (2019). *The middle path of moderation in Islam*. Oxford University Press. https://global.oup.com/academic/product/the-middle-path-of-moderation-in-islam-9780190941217
17. Kamali, M. H. (2023). Maqasid al-shariah and sustainable development: Foundation for a universal paradigm. *Journal of Islamic Studies, 15*(2), 89-102. Retrieved from https://mjsl.usim.edu.my/index.php/jurnalmjsl/article/view/798
18. Kamarinou, D., Millard, C., & Singh, J. (2023). Algorithmic transparency and accountability: A data protection perspective. *Information & Communications Technology Law, 32*(1), 22-47. https://doi.org/10.1080/13600834.2022.2125440
19. Kuner, C., Svantesson, D. J. B., Cate, F. H., Millard, C., & Lynskey, O. (2024). Harmonizing data protection: Foundations of modern privacy governance. *International Data Privacy Law, 14*(1), 4-18. https://doi.org/10.1093/idpl/ipad021
20. Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press. https://politybooks.com/bookdetail/?isbn=9780745635929
21. Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press. https://politybooks.com/bookdetail/?isbn=9780745699358
22. Lyon, D. (2024). *Surveillance: A very short introduction*. Oxford University Press. https://books.google.com/books/about/Surveillance.html?id=2V0QEQAAQBAJ

23. McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly, 68*(2), 309-343. https://doi.org/10.1017/S0020589319000046
24. Mittelstadt, B. D. (2019). Principles alone cannot guarantee ethical AI. *Ethics and Information Technology, 21*(1), 1-10. https://doi.org/10.1007/s10676-019-09502-2
25. Narayanan, A., & Vallor, S. (2023). Ethics of algorithms and the digital society. *Annual Review of Political Science, 26*, 185-205. https://doi.org/10.1146/annurev-polisci-051120-104443
26. National Information Technology Development Agency. (2019). *Nigeria data protection regulation (NDPR)*. https://nitda.gov.ng/regulations-and-guidelines/
27. Nigeria Data Protection Act 2023. (2023). https://ndpc.gov.ng/
28. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://www.sup.org/books/title/?id=8864
29. Olawade, D. B., David-Olawade, A. C., Gore, M. N., & Wada, O. Z. (2025). Perceptions and challenges of artificial intelligence adoption in Nigerian public healthcare: Insights from consultant doctors. *Clinical Epidemiology and Global Health, 29*, 101735. https://doi.org/10.1016/j.cegh.2025.101735
30. Rahman, F. (2015). *Islam* (2nd ed.). University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/I/bo3622687.html
31. Raji, I. D., Smart, A., White, R. N., Mitchell, M., & Gebru, T. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency (FAccT '20)* (pp. 33-44). Association for Computing Machinery. https://doi.org/10.1145/3351095.3372873
32. Record of Law. (2025). The legal and ethical challenges of digital consent in the era of surveillance capitalism. https://recordoflaw.in/the-legal-and-ethical-challenges-of-digital-consent-in-the-era-of-surveillance-capitalism/
33. Singler, S., & Babalola, O. (2024). Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices. *Social & Legal Studies, 34*(5), 673-694. https://doi.org/10.1177/09646639241287022
34. Smith, P., & Kumar, R. (2023). Geopolitical surveillance and digital sovereignty. *Journal of Global Security Studies, 8*(2), 204-224. https://doi.org/10.1093/jogss/ogac046
35. THISDAYLIVE. (2025, August 19). Ethical problems in AI and digital legislation in Nigeria (Part 4). https://www.thisdaylive.com/2025/08/19/ethical-problems-in-ai-and-digital-legislation-in-nigeria-part-4/
36. Wang, X., Wu, Y. C., & Zhou, M. (2024). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. *Frontiers in Big Data, 7*, 1337465. https://doi.org/10.3389/fdata.2024.1337465
37. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs. https://doi.org/10.2307/j.ctvnjbh1c