Vol. 1, No. 1, 2026, pp. 23-41
Publisher LaKaspia (Lembaga Kajian Sosial Politik Aceh)

JIEI Journal of Islamic Ethical Inquiry

Digital Surveillance, Human Dignity, and the Qur'anic Prohibition of *Tajassus*

Sitti Suhana[1], Antika Wulandari[2]

[1]Universitas Islam Negeri Sulthan Thaha Saifuddin, Jambi, Indonesia;
[2]Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia
Correspondence: Sitti Suhana, sittisuhana135@gmail.com

ABSTRACT

Digital surveillance turns observations that were once merely accessible into institutional capacities to classify people and act on those classifications. This article asks how Qur'anic ethical reasoning can govern that transformation without equating every form of monitoring with the prohibited *tajassus*. The study is a qualitative textual and constructive normative analysis. It reads Qur'an 49:12, 24:27–29, 17:70, and 4:58 alongside selected Arabic commentaries by al-Ṭabarī, al-Qurṭubī, Ibn Kathīr, and al-Saʿdī, and then compares the interpretive findings with privacy scholarship and AI governance. The textual analysis distinguishes suspicion from investigative entitlement. It identifies permission and consequential refusal as conditions of protected access, connects human honor with entrusted responsibility, and separates acquiring information from exposing it. These findings support a model of stage-specific institutional justification covering authorization, collection, inference, retention, disclosure, and remedy. Legitimate purpose, necessity, proportionality, dignity, and accountability each constrain these operations, and none can substitute for another. The model offers a traceable, Qur'an-informed explanation of why permission to acquire information does not confer unrestricted authority over later uses. Comparison with contextual integrity, reasonable inferences, privacy harms, and lifecycle governance clarifies what this contribution adds. A hypothetical safety investigation shows how credible danger can justify bounded inquiry, and how uncertain attribution should limit judgement and disclosure. The analysis offers a normative account of informational authority. Whether institutions apply such an account effectively is a separate empirical question.

ARTICLE HISTORY

Received 5 March 2026
Revised 5 May 2026
Accepted 15 May 2026
Online / Published
30 June 2026

KEYWORDS

Qur'anic ethics; informational power; institutional justification; privacy governance; tajassus

Article URL: https://ojs.lakaspia.org/index.php/jiei

Access license: Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0), https://creativecommons.org/licenses/by-sa/4.0/.
Copyright: © 2026 the Author(s). Published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

How to cite: Suhana, Sitti, and Antika Wulandari. "Digital Surveillance, Human Dignity, and the Qur'anic Prohibition of *Tajassus*." *Journal of Islamic Ethical Inquiry* 1, no. 1 (2026): 23–41.

Introduction

A camera recording an entrance and a system reconstructing a person's associations may draw on the same images, yet they perform different acts. The first records an event. The second connects observations into a claim about an identifiable life. Once that claim informs discipline, employment, or access to services, surveillance has become an exercise of institutional judgement. The ethical problem therefore concerns more than whether information was visible at the moment of collection. It concerns who may turn visibility into knowledge, what that knowledge is taken to establish, and which decisions it can justify. The United Nations privacy report on intrusive tools, encryption, and public-space monitoring places these transformations within a wider threat to rights and freedoms. For present purposes its significance is institutional: the capacity to acquire and connect information needs scrutiny before a particular injury becomes publicly demonstrable.[1]

Privacy scholarship has already made this problem central. Contextual integrity rejects the assumption that information available in one relationship is available for every other use. Studies of surveillance show how dispersed records become interconnected representations of persons, and research on predictive inference shows that disclosed traces can reveal attributes no one intended to disclose. These accounts move beyond a simple contrast between secret information and harmless public observation. They also make blanket judgements about technology inadequate. Identifying a person at a restricted laboratory entrance differs from recording that person's movements across an entire campus, even where both arrangements are justified by safety. The defensibility of a protective purpose has to be distinguished from the defensibility of the operations carried out in its name.[2]

Islamic scholarship offers substantial grounds for examining this distinction. Qur'anic prohibitions concerning suspicion, *tajassus*, and backbiting have already been connected to digital privacy. Lum'ah and colleagues develop that link through Hamka's *Tafsir al-Azhar*, including protection against unauthorized access and damaging circulation. Mustapha and Malkan likewise identify necessity, proportionality, dignity, and accountability in their account of AI surveillance. Together these studies supply an ethical vocabulary for evaluating digital intrusion. What remains open is how that vocabulary connects to particular institutional obligations. What does a justified purpose permit an institution to do, and when does a later use of information require a separate justification?[3]

---

[1] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/51/17 (August 4, 2022), summary and secs. II–IV, https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

[2] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 119–58, abstract and introductory argument, https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/; Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (2000): 605–22, abstract, https://doi.org/10.1080/00071310020015280; Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences* 110, no. 15 (2013): 5802, conclusions, https://doi.org/10.1073/pnas.1218772110.

[3] Diana Durrotul Lum'ah, Suqiyah Musafa'ah, and Muhammad Ihsan Mahbub, "The Paradigm of Digital Privacy in Indonesian Tafsir: A Study of Tafsir Al-Azhar on QS. Al-Hujurāt (49): 12 in the Age of Information," *MUSHAF: Jurnal Tafsir Berwawasan Keindonesiaan* 5, no. 2 (2025): 241–44, https://doi.org/10.33650/mushaf.v5i2.11148; Ramlan Mustapha and Siti Norma Aisyah Malkan@Molkan, "AI

The issue becomes acute at transitions between consequential uses of information. Grounds for acquiring a record may leave unjustified the inference of an intimate attribute, prolonged storage, circulation, or an adverse judgement. Contemporary privacy law and lifecycle governance already recognise these differences. Within the Islamic discussion examined here, the interpretive task is to explain how restraints on suspicious inquiry, protected entry, and entrusted authority support that differentiation. Reading these resources together clarifies both the object of permission and its limits. The article develops that relationship into an account of informational power whose institutional requirements can be assessed against both its textual grounds and established governance theories.

Two connected questions guide the inquiry. Which constraints on investigative knowledge and protected access emerge from the selected verses and commentaries? How can those constraints support separate institutional justifications for authorization, collection, inference, retention, disclosure, and remedy? The central argument is that legitimate access confers no general entitlement over the person made knowable through it. Justification must be renewed whenever an operation changes the protected interest, the informational claim, the recipient, the duration, or the consequence involved. Five established principles organise the account: legitimate purpose, necessity, proportionality, human dignity, and accountability. Integrating them with specific interpretive reasons makes the burden of justification examinable at each decision point. A difficult safety case then tests whether the account can protect potential victims while keeping meaningful limits on investigative authority.

Qur'anic privacy raises two questions: an exegetical one about the objects of prohibition and permission, and a constructive one about their relevance to changing institutions. The selected commentaries associate *tajassus* with searching concealed affairs and faults, and associate permission with entry into another's dwelling. The distinction matters. Investigating hidden misconduct is different from seeing what is apparent, and controlling entry concerns a protected relationship between visitor and occupant. An account that folds these objects into a single timeless category of privacy loses the distinctions needed to evaluate digital practices. Close interpretation supplies the reasons and qualifications through which a contemporary extension can be defended.[4]

The contemporary Islamic studies considered here approach this relationship by different routes. Lum'ah and colleagues' thematic reading of Hamka stresses the social and moral connection between suspicion, intrusive searching, and exposure in digital conduct. Mustapha and Malkan frame surveillance through Islamic jurisprudence and the

Surveillance, Privacy (Ḥifẓ *al-ʿIrḍ*), and Human Dignity in Islamic Jurisprudence," *International Journal of Islamic Theology & Civilization* 4, no. 1 (2026): 11–28, abstract, https://doi.org/10.5281/zenodo.18295050.

[4] Abū Jaʿfar Muḥammad ibn Jarīr al-Ṭabarī, *Jāmiʿ al-bayān*, Arabic electronic commentary, King Saud University, accessed October 31, 2026, commentary on 49:12 and 24:27–28, https://quran.ksu.edu.sa/tafseer/tabary/sura49-aya12.html; https://quran.ksu.edu.sa/tafseer/tabary/sura24-aya27.html; https://quran.ksu.edu.sa/tafseer/tabary/sura24-aya28.html; Abū ʿAbd Allāh Muḥammad ibn Aḥmad al-Qurṭubī, *Al-Jāmiʿ li-aḥkām al-Qurʾān*, Arabic electronic commentary, King Saud University, accessed October 31, 2026, commentary on 49:12, questions 2–4, https://quran.ksu.edu.sa/tafseer/qortobi/sura49-aya12.html.

protection of honour and privacy; their published abstract identifies overlapping institutional safeguards. These contributions show continuity between Islamic moral concerns and contemporary information practices. Reza's doctrinal and historical comparison adds a necessary distinction between normative resources and institutional history. Grounds for protections analogous to modern search safeguards do not show that those safeguards routinely operated. How an institution should use information therefore remains open to constructive argument, even where its scriptural and historical resources are substantial.[5]

Privacy theories identify different objects for evaluation. Nissenbaum's contextual integrity asks whether gathering and dissemination fit the norms of a context. Solove's taxonomy separates privacy problems so that analysis does not rest on an undivided appeal to privacy. Haggerty and Ericson explain how surveillance systems converge through the production of virtual "data doubles." These approaches help distinguish a record from the new relationships built around it. Their methods also differ: normative analysis of appropriate flows, legal-conceptual classification, and sociological explanation cannot simply stand in for one another. Taken together, however, they challenge the premise that the moral character of a surveillance practice is settled by the accessibility of its inputs. The remaining question is what warrants each use of those inputs, and who is entitled to challenge it.[6]

Cohen and Richards deepen this institutional focus by naming the interests surveillance can threaten. Cohen connects privacy with the conditions under which subjectivity and self-determination develop, while Richards emphasises intellectual privacy and the unequal power between watchers and watched. Citron and Solove explain why dispersed, prospective, or hard-to-individualise injuries deserve recognition. Together these accounts extend the problem beyond the unauthorised disclosure of an embarrassing secret. A standing capacity to classify people can shape the conditions under which they act, well before anything is published. Assessing that capacity still demands a discriminating judgement about its object, use, and consequences. A record needed for a bounded protective task presents a different case from an open-ended dossier.[7]

Inference sharpens the distinction between inputs and institutional claims. Kosinski, Stillwell, and Graepel show that Facebook Likes can support predictions about sensitive attributes. Their finding concerns a mechanism, not the accuracy of every later profiling

---

[5] Lum'ah, Musafa'ah, and Mahbub, "Paradigm of Digital Privacy," 241–44; Mustapha and Malkan@Molkan, "AI Surveillance," abstract; Sadiq Reza, "Islam's Fourth Amendment: Search and Seizure in Islamic Doctrine and Muslim Practice," *Georgetown Journal of International Law* 40, no. 3 (2009): 703–806, abstract, https://scholarship.law.bu.edu/faculty_scholarship/2581/.

[6] Nissenbaum, "Privacy as Contextual Integrity," abstract; Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006): 477–564, abstract, https://scholarship.law.gwu.edu/faculty_publications/921/; Haggerty and Ericson, "Surveillant Assemblage," abstract.

[7] Julie E. Cohen, "What Privacy Is For," *Harvard Law Review* 126, no. 7 (2013): 1904–33, introductory argument, https://harvardlawreview.org/print/vol-126/what-privacy-is-for/; Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review* 126, no. 7 (2013): 1934–65, introductory argument, https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/; Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," *Boston University Law Review* 102 (2022): 793–94, https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

system. Wachter and Mittelstadt's right to reasonable inferences makes a corresponding normative demand: high-risk inferences require justification before use and a route to challenge afterwards. Their argument already separates lawful acquisition from defensible inference. The present inquiry develops the Islamic ethical grounds for that separation and links it to continuing responsibility for custody and exposure. This requires an account of the protected affairs an inference seeks to reveal, and of the authority it enables. Computation should not be equated with *tajassus*.[8]

Islamic engagement with technology can examine how new practices reorganise moral relationships. Ghaly's account of AI-mediated work proceeds through the goods of work, permissible professions, and the relationships among stakeholders. It offers a useful methodological comparison: the ethical question turns on what a technology changes in the responsibilities of those involved. Surveillance similarly reorganises relations among institutions, the people they investigate, and those seeking protection. Applying that insight to investigative access requires its own textual and normative argument. The overlap between Islamic surveillance safeguards and international AI principles makes such a comparison possible, while leaving their sources of authority and forms of justification distinguishable.[9]

Moving from principles to obligations is also a central problem in AI governance. Jobin, Ienca, and Vayena identify convergence around high-level principles alongside divergence in interpretation and implementation. Mittelstadt asks whether agreement on principles supplies the institutions and practices needed to make them effective. Raji and colleagues address that problem through internal auditing across organisational development. NIST connects governance with recurring risk assessment. European data protection law differentiates purpose, necessity, storage, transparency, and remedies, and the EDPB's video-surveillance and consent guidance makes these distinctions operational. This literature shows that institutional accountability already extends across information practices. The question pursued here is what the selected Qur'anic resources contribute to explaining the obligations that arise when one permitted use becomes another, and how that explanation can sharpen institutional reasoning.[10]

---

[8] Kosinski, Stillwell, and Graepel, "Private Traits and Attributes," 5802–5; Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review* 2019, no. 2 (2019): 495, https://doi.org/10.7916/cblr.v2019i2.3424.

[9] Mohammed Ghaly, "What Makes Work 'Good' in the Age of Artificial Intelligence (AI)? Islamic Perspectives on AI-Mediated Work Ethics," *Journal of Ethics* 28 (2024): 429–53, secs. 1 and 3, https://doi.org/10.1007/s10892-023-09456-3; UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (November 23, 2021), secs. III.1–III.2, https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence.

[10] Anna Jobin, Marcello Ienca, and Effy Vayena, "The Global Landscape of AI Ethics Guidelines," *Nature Machine Intelligence* 1 (2019): 389–99, abstract, https://doi.org/10.1038/s42256-019-0088-2; Brent Mittelstadt, "Principles Alone Cannot Guarantee Ethical AI," *Nature Machine Intelligence* 1 (2019): 501–7, abstract, https://doi.org/10.1038/s42256-019-0114-4; Inioluwa Deborah Raji, Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes, "Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing" (arXiv, January 3, 2020), secs. 4–5, https://arxiv.org/abs/2001.00973; National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (January 2023), secs. 1.2 and 5, https://doi.org/10.6028/NIST.AI.100-1; European Parliament and Council of the European Union, Regulation (EU) 2016/679 of April 27, 2016 (General Data Protection Regulation), *Official Journal of the European Union* L 119 (May 4, 2016): 1–88, arts. 5–6, 12–22, and 35, https://eur-

Method

The study combined qualitative textual interpretation with constructive normative inquiry into the relationship between investigative access and subsequent informational power. Qur'anic passages and commentaries supplied interpretive reasons. Privacy scholarship and governance documents supplied comparative arguments and institutional specifications. The analysis first identified the objects and limits of the textual permissions and prohibitions, then examined their ethical implications, and finally developed and tested a contemporary decision model. Any analogy had to rest on a stated connection between the protected interest in the text and the informational operation under examination. Contemporary regulatory terminology offered no independent evidence of Qur'anic meaning.

The Qur'anic corpus was selected by argumentative function. Qur'an 49:12 addresses suspicion, intrusive searching, and backbiting. Qur'an 24:27–28 addresses permission and refusal, and 24:29 is retained to qualify domestic exclusion. Qur'an 17:70 provides the wider horizon of human honour, and 4:58 links entrusted responsibility with just judgement. Taken together, these verses allowed the analysis to examine the relationship between restraint in acquiring knowledge and responsibility for its possession and use. The adjacent qualification and broader passages also tested whether an interpretation of the primary prohibition had been stretched beyond its grounds.

The exegetical corpus comprised al-Ṭabarī on 49:12 and 24:27–28; al-Qurṭubī on 49:12, especially questions 2–4; Ibn Kathīr on 24:27–29; and al-Saʿdī on 49:12, 24:27, 17:70, and 4:58. These selections bring together transmitted explanation, juridical distinctions, and concise ethical exposition. The sources were the verse-indexed Arabic electronic texts hosted by King Saud University. Citations identify commentator and verse because these witnesses were not collated against manuscripts or a critical print edition. Arabic extracts were checked in their surrounding commentary and translated for this analysis. The corpus provides contrasting interpretive resources rather than a representative sample of exegetical traditions.[11]

Contemporary materials were chosen purposively for their contribution to the argument. Islamic privacy and AI studies established prior work; privacy theories clarified information flows, injury, and power; technical studies established inferential mechanisms

lex.europa.eu/eli/reg/2016/679/; European Data Protection Board, *Guidelines 3/2019 on Processing of Personal Data through Video Devices*, version 2.1 (February 26, 2020), secs. 3, 4, and 8, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf; European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, version 1.1 (May 13, 2020), sec. 3.1, https://www.edpb.europa.eu/system/files/documents/files/file1/edpb_guidelines_202005_consent_en.pdf.

[11] Al-Ṭabarī, *Jāmiʿ al-bayān*, commentary on 49:12 and 24:27–28; Al-Qurṭubī, *Al-Jāmiʿ li-aḥkām al-Qurʾān*, commentary on 49:12, questions 2–4; Abū al-Fidāʾ Ismāʿīl ibn ʿUmar Ibn Kathīr, *Tafsīr al-Qurʾān al-ʿaẓīm*, Arabic electronic commentary, King Saud University, accessed October 31, 2026, commentary on 24:27–29, https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya27.html; https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya28.html; https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya29.html; ʿAbd al-Raḥmān ibn Nāṣir al-Saʿdī, *Taysīr al-karīm al-raḥmān*, Arabic electronic commentary, King Saud University, accessed October 31, 2026, commentary on 49:12, 24:27, 17:70, and 4:58, https://quran.ksu.edu.sa/tafseer/saadi/sura49-aya12.html; https://quran.ksu.edu.sa/tafseer/saadi/sura24-aya27.html; https://quran.ksu.edu.sa/tafseer/saadi/sura17-aya70.html; https://quran.ksu.edu.sa/tafseer/saadi/sura4-aya58.html.

and evaluation problems; and primary governance documents offered operational comparisons. Targeted searches combined "*tajassus*," "digital privacy," "AI surveillance," "reasonable inferences," "Islamic ethics," and "AI governance." Results were then checked against exact titles and official versions on publisher sites, author repositories, and institutional portals through October 31, 2026. This was a critical selection, not a systematic census. Where access was limited to an abstract or introductory argument, the comparison was confined to that material, as the notes identify.

The unit of textual analysis was a verse together with the selected commentary on its object, qualifications, and implications. Close reading distinguished the act prohibited or permitted, the person whose affairs or space were implicated, the grounds for judgement, and the consequences of refusal or exposure. Comparison then identified convergence and disagreement across these passages. Reports reproduced by commentators were treated as evidence of how they were interpreted, not as independently authenticated historical events. This preserved both the differences among the explanations of *tajassus* and *taḥassus*, and the distinction between warnings about rulers and evidence of historical state practice.

Normative reconstruction separated textual meaning, ethical implication, and contemporary application. The first identified what a verse and commentary concern. The second formulated the reason supported by that reading. The third stated the premise linking the reason to a digital operation. Extending the domestic boundary to communications, for example, required identifying the intimate affairs exposed. Extending it to aggregated public traces required a further explanation of the new information being reconstructed. These connections were compared with the contemporary literature before the six-stage model was formulated. The Results report the textual patterns, and the Discussion develops their institutional significance and evaluates the proposed extension.

Five criteria assessed the reconstruction. Textual fit tested whether a proposed implication respected the object and qualifications of a passage. Conceptual coherence tested the distinction between evidence, permission, and authority, and the relationship among the five principles. Contextual relevance examined the actual information practice and its effects on access or exposure. Normative defensibility required reasons that address both investigated persons and potential victims, including feasible alternatives and evidential uncertainty. Resistance to counterexamples tested the account against attendance monitoring, restricted-entry logging, and a hypothetical safety investigation. Varying corroboration, scope, urgency, and subsequent use showed which changes in a case should alter the judgement. These were tests of the argument. The study makes no empirical claim about the model's institutional performance.

Results

Suspicion and Investigative Entitlement

Qur'an 49:12 places *wa-lā tajassasū* between a warning against suspicion and a prohibition of backbiting. Al-Ṭabarī explains the prohibition through concealed affairs and faults: "ولا يبحث عن سرائره," rendered here as "nor search into his concealed affairs." His surrounding explanation contrasts seeking hidden faults with attending to what is

apparent. Al-Saʿdī likewise associates *tajassus* with searching for concealed faults, and describes how unfounded suspicion can develop into wrongful words and actions. The convergence identifies a directed pursuit of what another has not exposed, situated within a relationship between judgement, inquiry, and injury. Observation as such is broader than the conduct these explanations describe.[12]

Al-Qurṭubī qualifies this pattern by distinguishing accusation that lacks a sound indication from judgement grounded in evidence. His second and third questions preserve room for reasoned probabilistic judgement, so the warning against suspicion cannot be read as an injunction against every uncertain assessment. His fourth question records differing explanations of *tajassus* and *taḥassus*, and reproduces warnings about rulers who seek out people's hidden faults. The object of interpretation therefore includes the conduct of authority as well as relations among individuals. Across these distinctions, the relevant questions concern both the ground of an accusation and the pursuit of affairs that remain concealed.[13]

The textual evidence distinguishes having a suspicion from being entitled to pursue its object. Al-Ṭabarī and al-Saʿdī emphasise the concealed affairs sought and the wrongful conduct associated with that pursuit, while al-Qurṭubī separates evidentially grounded judgement from unsupported accusation. Read together, these explanations locate restraint in the relationship between what is believed, what is sought, and what is subsequently said. A wish to settle uncertainty gives no automatic warrant to search another's concealed affairs. At the same time, the differentiation among kinds of suspicion preserves the possibility of justified judgement. The conclusion is therefore more specific than either an absolute prohibition of inquiry or an unrestricted entitlement to investigate whatever gives rise to doubt.

Permission, Refusal, and Protected Boundaries

Qur'an 24:27–28 concerns entering houses other than one's own. Al-Ṭabarī records explanations of *tastaʾnisū* that involve seeking permission and making one's presence known. His preferred account connects seeking admission with informing the occupants. His explanation of 24:28 maintains the boundary even when no one able to admit the visitor is found. Absence does not make the house available, and the command to withdraw when told to return gives refusal a practical consequence. Permission therefore concerns the occupant's recognised position in deciding entry. The visitor's assurance of benign intent does not settle the matter. The textual pattern is conditional admission, and its limits remain meaningful even when access would be convenient.[14]

Ibn Kathīr reinforces the occupant's position in his commentary on 24:28: "فإن شاء أذن، وإن شاء لم يأذن," translated here as "if he wishes, he permits; if he wishes, he does not permit." His treatment of 24:27 also addresses permission before entry and the avoidance of unwanted sight. Al-Saʿdī explains domestic protection through the exposure of what a

[12] Al-Ṭabarī, *Jāmiʿ al-bayān*, commentary on 49:12, explanation of *wa-lā tajassasū*; Al-Saʿdī, *Taysīr al-karīm al-raḥmān*, commentary on 49:12.
[13] Al-Qurṭubī, *Al-Jāmiʿ li-aḥkām al-Qurʾān*, commentary on 49:12, questions 2–4.
[14] Al-Ṭabarī, *Jāmiʿ al-bayān*, commentary on 24:27, concluding interpretation, and 24:28.

house conceals. The commentators thus link the rule of entry with two things: a person entitled to admit or refuse, and a condition under which unwanted access can reveal what is private. Their agreement is functional as well as spatial. The dwelling protects something about its inhabitants that an outsider's entry can expose.[15]

Qur'an 24:29 qualifies the preceding rule by permitting entry into uninhabited houses where a relevant use is involved. Ibn Kathīr discusses accommodation and reports other explanations concerning trading and travel premises. The immediate context therefore distinguishes types of access rather than treating every building or every entry in the same way. Read with 24:27–28, the qualification shows a pattern of protected boundaries, consequential refusal, and contextual permission. It prevents domestic exclusion from being generalised into a prohibition of all entry, while leaving the protection of inhabited space intact. What matters here is how access is situated and authorised. Its scope cannot be determined from the outsider's claim of benefit alone.[16]

Human Dignity and Entrusted Authority

Qur'an 17:70 attributes honour to the children of Adam. Al-Saʿdī explains that honour through divine generosity, human capacities, and provision. The verse's reference to humanity is broader than the believer-centred language in the selected explanations of 49:12, and the difference matters for the comparison. Honour is presented as a condition of human standing, not merely as the reputation of a person whose conduct others approve. The passage offers a broader ethical horizon for interpreting injury and exposure, but it leaves the specific form of any resulting obligation to further argument. Human honour and the judgement of particular conduct are related yet distinguishable objects of evaluation.[17]

Qur'an 4:58 joins the discharge of trusts with just judgement. Al-Saʿdī includes "أمانات الولايات والأموال والأسرار," rendered here as "trusts of authority, property, and secrets," among entrusted matters. His explanation also extends just judgement across differences of relationship and moral standing. The passage therefore connects responsibilities of custody with responsibilities of judgement. A trust is evaluated by how it is discharged, and possession alone does not exhaust that evaluation. Read alongside 17:70, the commentary places the standing of persons and the responsibilities of those entrusted with power within the same ethical field, without reducing either to personal reputation.[18]

The interpretive pattern is a conjunction of honour and answerable authority. Qur'an 17:70 establishes the human horizon within which treatment is considered. Qur'an 4:58 concerns what is owed in discharging a trust and in judging others. Al-Saʿdī's inclusion of secrets makes entrusted information relevant to this relationship. These resources distinguish the person whose affairs are known from the responsibilities of the person who knows them. Responsibility within a relationship of control is the issue here. Holding

[15] Ibn Kathīr, *Tafsīr al-Qurʾān al-ʿaẓīm*, commentary on 24:27–28; Al-Saʿdī, *Taysīr al-karīm al-raḥmān*, commentary on 24:27.
[16] Ibn Kathīr, *Tafsīr al-Qurʾān al-ʿaẓīm*, commentary on 24:29.
[17] Al-Saʿdī, *Taysīr al-karīm al-raḥmān*, commentary on 17:70.
[18] Al-Saʿdī, *Taysīr al-karīm al-raḥmān*, commentary on 4:58.

something in trust carries an obligation about its disposition, while the moral standing of those affected is a separate consideration. This distinction links the earlier restraints on entry and inquiry with the evaluation of what follows access.

Acquisition, Exposure, and Informational Responsibility

Across the corpus, acquiring knowledge and communicating it are distinct acts within connected conduct. Qur'an 49:12 separates suspicion, searching, and backbiting. Qur'an 24:27–29 separates seeking permission, gaining entry, refusing access, and qualified admission. Qur'an 4:58 evaluates the discharge of entrusted responsibilities. The interpretive pattern is a sequence of morally differentiated relations. It does not attach one judgement to information possession as a whole. An objection to how information is obtained and an objection to its exposure concern different actions. The texts consequently provide grounds for asking what follows access, without assuming that a judgement about the initial encounter settles the conduct that comes afterwards.

Al-Ṭabarī's explanation of backbiting concerns saying, in another's absence, what that person would dislike. Al-Saʿdī's discussion retains the wrongfulness of such speech even where its content is true. Within the conduct criticised by 49:12, truth therefore does not by itself remove the moral question concerning communication. This gives the distinction between acquisition and exposure substantive force: what is known and what may rightly be said are not the same question. Together with the obligations of trust in 4:58, the finding completes the textual pattern of restraint before access and responsibility afterwards. It supplies the interpretive grounds for examining later uses of information, and leaves their contemporary institutional form to normative construction.[19]

Discussion

Informational Power and Renewed Justification

The findings make the scope of informational authority an ethical question in its own right. Restraint in pursuing concealed affairs concerns the warrant for seeking knowledge. Permission and refusal concern the boundary being crossed. Entrusted responsibility concerns how what has been obtained is used. Their conjunction supports the article's central proposition: a justified point of access creates a limited permission, not general authority over the person made knowable through it. The institutional implication is that reasons must follow changes in what information reveals and what it enables. A continuing protective purpose may remain legitimate even while a new operation exceeds the authority originally justified.

Extending these findings to digital surveillance depends on identifying the protected relationship. A database is not a dwelling. Access to intimate communications most closely resembles the exposure at stake in domestic entry. Aggregating public traces requires a further premise: the combination may reconstruct relationships or attributes that no isolated observation reveals. Technical availability, or silence about the matter, cannot

[19] Al-Ṭabarī, *Jāmiʿ al-bayān*, commentary on Qur'an 49:12, explanation of backbiting; al-Saʿdī, *Taysīr al-karīm al-raḥmān*, commentary on Qur'an 49:12.

settle whether that transformation is permissible. Where meaningful refusal is unavailable, the institution must defend another source of authority and its limits. The wider horizon of human honour also constrains treatment after access. Suspicion of wrongdoing may support a focused inquiry, yet it leaves unrelated exposure or degrading treatment unjustified. These are contemporary implications of the textual findings, and their adequacy depends on the stated connections between protected affairs, institutional capacity, and consequences.

Digital operations make these shifts in authority consequential. Inferring a sensitive attribute can reveal information absent from any single input, while biometric matching turns an image into a claim of identity that may support action. Kosinski, Stillwell, and Graepel show that sensitive inference from disclosed traces is possible. Buolamwini and Gebru examine commercial gender classification, while the NIST demographic reports concern face recognition and its error differentials. These studies address different tasks, so they cannot support a universal claim about accuracy. They share an evaluative demand, however: identify what a system purports to know, and what evidence warrants acting on that claim. An alert is therefore distinct from permission to investigate, and an investigation is distinct from proof of wrongdoing. The moral burden changes once information becomes a classification on which an institution acts.[20]

Stage-specific justification gives this burden a practical form through five established principles. Legitimate purpose identifies the protected interest and the competent authority. Necessity tests the proposed interference against workable alternatives. Proportionality examines its scope, sensitivity, duration, incidental burdens, and expected protective benefit. Human dignity constrains how persons are treated, including those properly suspected. Accountability locates responsibility for reasons, review, and repair. These principles constrain one another without compensating for failure. Accurate documentation cannot legitimate an improper objective, consent cannot supply missing evidential reliability, and a necessary inquiry does not make gratuitous disclosure justified. Renewing justification means reassessing the relevant reasons when an operation changes its object or consequences. It does not mean repeating authorisation for routine acts within a defensible limit.

The six stages in Table 1 specify where those reasons become necessary. Authorisation and collection concern the grounds and extent of access. Inference concerns what the evidence can establish. Retention and disclosure concern continuing custody and exposure. Remedy concerns the ability to challenge and correct the exercise of power. Their relationship is recursive: a failed attribution may require correction, deletion, and review of the original authorisation. Retention and remedy have especially indirect textual grounds. They follow from entrusted responsibility and human standing, not from an

[20] Kosinski, Stillwell, and Graepel, "Private Traits and Attributes," 5802–5; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): 77, https://proceedings.mlr.press/v81/buolamwini18a.html; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test Part 3: Demographic Effects*, NISTIR 8280 (2019), executive summary, https://doi.org/10.6028/NIST.IR.8280; Patrick Grother, *Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials*, NISTIR 8429 (2022), abstract and sec. 1, https://doi.org/10.6028/NIST.IR.8429.

explicit scriptural procedure. An evidential hold may protect a subject's ability to challenge an inquiry after operational copies are no longer needed. The justification must therefore distinguish preserving a minimal record for redress from maintaining a reusable personal dossier.

Table 1. Qur'an-informed grounds and institutional decision burdens

Stage	Interpretive resource	Justification required	Consequence of failure
Authorization	49:12; 24:27–28; 4:58	Identify the task, evidence, competent authorizer, scope, and independent review. Purpose and accountability govern entry.	Refuse a speculative objective or unbounded authority.
Collection	24:27–29 by bounded analogy	Compare feasible alternatives; delimit targets, fields, and time. Necessity and proportionality govern access.	Reject avoidable intrusion; narrow excessive capture.
Inference	49:12; dignity horizon of 17:70	Justify the attribute sought, its relevance, reliability, and consequences. Distinguish a lead from an adverse judgment.	Withhold unreliable classification or unsupported sanctions.
Retention	4:58 as continuing trust	State expiry and access controls; separately justify an evidential hold for proceedings or challenge.	Delete or segregate when the task ends; reject indefinite storage.
Disclosure	49:12 on exposure; 4:58	Justify each recipient, purpose, and necessary content. Dignity limits exposure despite legitimate acquisition.	Redact unrelated material; refuse unauthorized transfer.
Remedy	4:58 and 17:70 as ethical grounds	Provide independent challenge, correction, and proportionate repair; justify any delay in notice.	Suspend harmful use; correct records and downstream decisions.

Sources: The six stages and their procedural requirements are the article's normative construction. Verse references identify interpretive resources

The framework distinguishes protective monitoring from institutional expansion by asking whether the reason for one operation supports the next. Continuous facial identification across teaching spaces to enforce attendance would require a case for necessity beyond the legitimate attendance objective, since less intrusive registers or targeted checks may adequately serve that task. A restricted laboratory, by contrast, may justify credential checks and a short entrance log where the danger, the alternatives, and the review arrangements support that limited operation. Converting the log into a map of personal associations changes both what is sought and what is exposed. The original safety rationale remains relevant, but its adequacy must be demonstrated for the additional use. These hypothetical contrasts show how the model assesses changes in informational authority even where an institution's declared purpose stays constant.

Contributions to Privacy and Islamic Ethics

Contextual integrity explains why information flows must be assessed beyond the availability of their inputs. The present reconstruction places an institution's claim of authority within that assessment. Who seeks access? What operation is proposed? What protected relationship is altered? Its Qur'anic grounds make the limitation of permission

intelligible through the position of the person whose affairs are exposed and the responsibility of the holder. An organisational expectation of monitoring cannot by itself satisfy those reasons. The added value is an explicit interpretive warrant for evaluating institutional claims. It is not a competing taxonomy of flows. It connects the contextual question of appropriate use with the obligation of an institution to explain the authority it exercises at a particular transition.[21]

Wachter and Mittelstadt's reasonable-inference proposal marks a close point of convergence. Their demands for the acceptability, relevance, and reliability of high-risk inference already separate collection from justified classification. The Qur'an-informed model places that separation within a wider relationship between restraint in seeking knowledge and responsibility for its custody and exposure. Citron and Solove's account of dispersed and prospective privacy harms further explains why evaluation cannot wait for a readily individualised loss. The present argument adds an ethical ground to that position. The relationship established by a search into concealed affairs can itself require justification, apart from proving a measurable injury. This emphasis supplements consequence-sensitive assessment by making the warrant for seeking and using knowledge an independent object of scrutiny.[22]

Lifecycle governance offers institutional means for sustaining that scrutiny. NIST's framework distributes governance and risk assessment across the system lifecycle. Raji and colleagues connect internal audit artefacts with decisions about deployment and remediation. Both approaches already concern the acceptability of uses as well as documentation. The Qur'an-informed reconstruction contributes a substantive rationale against which such processes can be assessed. It gives an account of why the object of access, the standing of the subject, and entrusted responsibilities constrain permission. Its distinctions among information operations can help locate the point at which a claimed purpose stops justifying an interference. The comparison therefore joins an interpretive account of authority with the organisational capacity to record, review, and revise its exercise.[23]

Data-protection law draws a similar distinction in legally specified form. Purpose limitation, minimisation, storage limitation, accountability, and rights of challenge assign different obligations to different uses. The European Data Protection Board treats disclosure as separate processing that requires its own basis, while its consent guidance addresses how power and conditionality affect apparent agreement. The domestic-entry findings add a related moral emphasis: refusal must have practical force if permission is to carry justificatory weight. An institution unable to accommodate refusal must defend a different authority, rather than redescribe compulsion as consent. These legal

[21] Nissenbaum, "Privacy as Contextual Integrity," abstract and introductory argument.
[22] Wachter and Mittelstadt, "Right to Reasonable Inferences," 495; Citron and Solove, "Privacy Harms," 793–94.
[23] NIST, *AI RMF 1.0*, secs. 1.2 and 5; Raji et al., "Closing the AI Accountability Gap," secs. 4–5.

comparisons clarify the operational significance of the argument. Their jurisdictional scope and legal force are distinct from the ethical reasons reconstructed here.[24]

For Islamic ethics, the contribution lies in making the connection between interpretation and institutional obligation inspectable. Lum'ah and colleagues establish the digital relevance of suspicion, intrusion, and exposure. Mustapha and Malkan identify overlapping AI safeguards. This article specifies how the selected interpretive resources support distinct burdens at consequential changes of use. Ghaly's account of AI-mediated work offers a parallel method for examining the relationships that technological change reorganises. Here the reconstructed relationship is between the person made knowable and the institution claiming authority over that knowledge. The ethical content reaches beyond a list of principles. It identifies why particular reasons are owed, which actions they must support, and what follows when they fail. The contribution is an integration of interpretive grounds and institutional judgement within the scholarship examined.[25]

Protective Inquiry under Uncertain Evidence

Consider a hypothetical university that receives a message naming a student, a laboratory containing dangerous materials, and a time for an attack. The recipient provides the original message, but the apparent sender disputes authorship. Protecting the intended victim and others is a legitimate purpose. The accused person's privacy and protection against wrongful attribution are also substantial interests. The case cannot be resolved by requiring consent to all investigation, since asking permission may defeat protection. Nor can it be resolved by treating the seriousness of the threatened harm as proof of the sender's identity. The competing claims concern different persons and different uncertainties. The model requires the institution to explain why this evidence warrants this interference. Invoking safety or privacy as a decisive label is not enough.

The first question is whether the threat warrants access beyond immediate protective measures. Checking provenance, securing the laboratory, supporting the recipient, and assessing access to dangerous materials may reduce the danger without searching private communications. Those steps may still leave a serious, unresolved risk. Corroboration can then support a focused request under competent authority, limited to the relevant account, event, and time window. A demand for every student's communication would go beyond what the stipulated facts justify. If the allegation is only an unsubstantiated rumour or an unexplained model score, intrusive access should be refused pending better grounds. The judgement changes with the quality of the evidence and the adequacy of alternatives, not simply with the institution's insistence that safety matters.

Even justified access leaves attribution unsettled. Account activity may reflect shared devices, impersonation, or compromised credentials, and contrary testimony can defeat the apparent connection to the student. A temporary protective measure may require a

[24] European Parliament and Council, Regulation (EU) 2016/679, arts. 5–6, 12–22, and 35; European Data Protection Board, *Guidelines 05/2020*, secs. 3.1–3.1.4; European Data Protection Board, *Guidelines 3/2019*, secs. 3–4 and 8.

[25] Lum'ah, Musafa'ah, and Mahbub, "Paradigm of Digital Privacy," 241–44; Mustapha and Malkan@Molkan, "AI Surveillance," abstract; Ghaly, "What Makes Work 'Good'," secs. 1 and 3.

different evidential threshold from a disciplinary judgement, but urgency must not turn precaution into a conclusive accusation. Dignity here requires uncertainty to remain visible in both reasoning and treatment. If a matching or profiling system is used, its relevance and reliability must be supported for the actual task and setting. This separates a reason to investigate a possible threat from a reason to impose a lasting adverse judgement on an identified person.

The same distinction shapes what may happen to the material gathered. Unrelated communications should be excluded from investigative use and deleted or segregated as appropriate. Relevant evidence may be preserved on a specified basis for proceedings or challenge. A minimal audit record can support redress without preserving a continuing personal dossier. Protective disclosure should be confined to recipients with a justified role and to content necessary for that role. If attribution proves wrong, correction must reach both the record and the decisions made from it, followed by review of restrictions and proportionate repair. Notice may be delayed while disclosure would undermine protection, but continued delay requires independent scrutiny and a stopping condition. These choices preserve the differences among retention, disclosure, and remedy without treating them as isolated administrative tasks.

Urgency makes the conflict harder without removing it. Where delay itself threatens grave harm, limited access before independent authorisation may be defensible, provided contemporaneous reasons are recorded and prompt retrospective review can terminate it. This exception follows from the competing protective responsibilities in the case, and its justification must still answer to the privacy interest it overrides. Informant protection creates a further tension. Identifying the source may endanger a vulnerable recipient, while withholding it can make an accusation difficult to contest. Confidential examination by an independent reviewer can reduce that conflict without eliminating it. Where adequate challenge is impossible, the institution should limit the weight and consequences assigned to the contested evidence. The framework locates the unresolved burden and constrains action in response. Procedural form cannot supply the missing evidence.

These tensions also define the reach of the analogy. Classical discussions of searching concealed faults differ from metadata analysis, public CCTV, and machine inference. The extension is strongest where intimate communications are penetrated, and it requires additional reasons where public traces are combined into a sensitive classification. Anonymous traffic counting may lack that protected object altogether. Foreseeable capacity for exposure can matter even where the operator declares no intention to uncover faults, but the assessment must identify the affairs revealed and the power enabled. This keeps *tajassus* analytically connected to its interpretive object, while allowing a contemporary institution's design and uses to be judged beyond its professed intention.

The framework's wider application across religious and social categories draws on the human horizon of 17:70 and the demand for just entrusted judgement. It goes beyond the believer-centred formulations found in parts of the corpus, through an explicit normative argument. Reza's distinction between moral resources and institutional history remains relevant here: interpretive grounds provide reasons for safeguards, not evidence that those

safeguards operated consistently. The selective corpus also leaves a comprehensive jurisprudence of criminal evidence, intelligence, and emergency powers outside this inquiry. The result is a specified ethical account whose strength lies in making authority answerable at changes of use. Whether institutions apply it consistently, and whether affected persons obtain effective redress, are questions of implementation that the textual and normative evidence cannot determine.[26]

Conclusion

The textual analysis distinguishes suspicion from entitlement to investigate, identifies permission and consequential refusal as conditions of protected access, and connects human honour with the discharge of entrusted responsibility. The pairing of inquiry with backbiting further separates acquiring information from exposing it. Knowing a matter does not settle whether communicating it is justified. These findings locate the ethical problem in relationships among judgement, access, and responsibility, not in observation alone. They supply the interpretive grounds for evaluating what an institution is entitled to do with the knowledge it acquires.

The conceptual contribution is a Qur'an-informed account of stage-specific institutional justification. Reasons for authorisation, collection, inference, retention, disclosure, and remedy must address the distinct interests and consequences involved. Legitimate purpose, necessity, proportionality, dignity, and accountability constrain these reasons without substituting for one another. In dialogue with contextual integrity, reasonable inferences, privacy harms, and lifecycle governance, the model makes explicit why an initial permission remains limited when informational power changes its object. For Qur'anic studies, the contribution lies in tracing the movement from particular exegetical distinctions to an institutional ethical argument. For Islamic ethics, it specifies the responsibilities that continue after access has been justified.

The safety investigation shows how this account can defend focused inquiry while restricting uncertain attribution, excessive collection, unrelated exposure, and continued custody. Protecting potential victims and respecting the investigated person require differentiated judgements, not a single verdict on surveillance as a whole. The conclusions remain bounded by the selective exegetical corpus and by contextual normative reasoning. This study did not establish institutional effectiveness. Within those limits, the argument makes a substantive demand on surveillance governance: each consequential use must remain answerable to reasons appropriate to that act, and the person subjected to it keeps claims that justified access alone cannot extinguish.

Declarations

Use of Artificial Intelligence (AI). The authors used ChatGPT/Codex (OpenAI) as a technical aid for language editing, structural refinement of the manuscript, and reformulation of sentences. The tool did not generate any research data. The authors reviewed and independently verified all references, substantive descriptions, and

[26] Reza, "Islam's Fourth Amendment," abstract.

interpretations in the manuscript. AI is not listed as an author. The authors bear full responsibility for the accuracy, originality, academic integrity, and final content of the manuscript.

Funding. This research received no specific grant from any public, commercial, or not-for-profit funding agency.

Conflict of Interest. The authors have no conflicts of interest to declare regarding the research, authorship, or publication of this manuscript.

Bibliography

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." Proceedings of Machine Learning Research 81 (2018): 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html.

Citron, Danielle Keats, and Daniel J. Solove. "Privacy Harms." Boston University Law Review 102 (2022): 793–863. https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

Cohen, Julie E. "What Privacy Is For." Harvard Law Review 126, no. 7 (2013): 1904–33. https://harvardlawreview.org/print/vol-126/what-privacy-is-for/.

European Data Protection Board. Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1. May 13, 2020. https://www.edpb.europa.eu/system/files/documents/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Board. Guidelines 3/2019 on Processing of Personal Data through Video Devices. Version 2.1. February 26, 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

European Parliament and Council of the European Union. Regulation (EU) 2016/679 of April 27, 2016 (General Data Protection Regulation). Official Journal of the European Union L 119 (May 4, 2016): 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/.

Ghaly, Mohammed. "What Makes Work 'Good' in the Age of Artificial Intelligence (AI)? Islamic Perspectives on AI-Mediated Work Ethics." Journal of Ethics 28 (2024): 429–53. https://doi.org/10.1007/s10892-023-09456-3.

Grother, Patrick. Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials. NISTIR 8429. 2022. https://doi.org/10.6028/NIST.IR.8429.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. Face Recognition Vendor Test Part 3: Demographic Effects. NISTIR 8280. 2019. https://doi.org/10.6028/NIST.IR.8280.

Haggerty, Kevin D., and Richard V. Ericson. "The Surveillant Assemblage." British Journal of Sociology 51, no. 4 (2000): 605–22. https://doi.org/10.1080/00071310020015280.

Ibn Kathīr, Abū al-Fidāʾ Ismāʿīl ibn ʿUmar. Tafsīr al-Qurʾān al-ʿaẓīm. Arabic electronic commentary on Qur'an 24:27–29. King Saud University. https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya27.html; https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya28.html; https://quran.ksu.edu.sa/tafseer/katheer/sura24-aya29.html.

Jobin, Anna, Marcello Ienca, and Effy Vayena. "The Global Landscape of AI Ethics Guidelines." Nature Machine Intelligence 1 (2019): 389–99. https://doi.org/10.1038/s42256-019-0088-2.

Kosinski, Michal, David Stillwell, and Thore Graepel. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." Proceedings of the National Academy of Sciences 110, no. 15 (2013): 5802–5. https://doi.org/10.1073/pnas.1218772110.

Lum'ah, Diana Durrotul, Suqiyah Musafa'ah, and Muhammad Ihsan Mahbub. "The Paradigm of Digital Privacy in Indonesian Tafsir: A Study of Tafsir Al-Azhar on QS. Al-Hujurāt (49): 12 in the Age of Information." MUSHAF: Jurnal Tafsir Berwawasan Keindonesiaan 5, no. 2 (2025): 235–49. https://doi.org/10.33650/mushaf.v5i2.11148.

Mittelstadt, Brent. "Principles Alone Cannot Guarantee Ethical AI." Nature Machine Intelligence 1 (2019): 501–7. https://doi.org/10.1038/s42256-019-0114-4.

Mustapha, Ramlan, and Siti Norma Aisyah Malkan. "AI Surveillance, Privacy (Ḥifẓ *al-ʿIrḍ*), and Human Dignity in Islamic Jurisprudence." International Journal of Islamic Theology & Civilization 4, no. 1 (2026): 11–28. https://doi.org/10.5281/zenodo.18295050.

National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. January 2023. https://doi.org/10.6028/NIST.AI.100-1.

Nissenbaum, Helen. "Privacy as Contextual Integrity." Washington Law Review 79, no. 1 (2004): 119–58. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

Office of the United Nations High Commissioner for Human Rights. The Right to Privacy in the Digital Age. A/HRC/51/17. August 4, 2022. https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

Qurṭubī, Abū ʿAbd Allāh Muḥammad ibn Aḥmad al-. Al-Jāmiʿ li-aḥkām al-Qurʾān. Arabic electronic commentary on Qur'an 49:12. King Saud University. https://quran.ksu.edu.sa/tafseer/qortobi/sura49-aya12.html.

Raji, Inioluwa Deborah, Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes. "Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing." arXiv, January 3, 2020. https://arxiv.org/abs/2001.00973.

Reza, Sadiq. "Islam's Fourth Amendment: Search and Seizure in Islamic Doctrine and Muslim Practice." Georgetown Journal of International Law 40, no. 3 (2009): 703–806. https://scholarship.law.bu.edu/faculty_scholarship/2581/.

Richards, Neil M. "The Dangers of Surveillance." Harvard Law Review 126, no. 7 (2013): 1934–65. https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/.

Saʿdī, ʿAbd al-Raḥmān ibn Nāṣir al-. Taysīr al-karīm al-raḥmān. Arabic electronic commentary on Qur'an 49:12, 24:27, 17:70, and 4:58. King Saud University. https://quran.ksu.edu.sa/tafseer/saadi/sura49-aya12.html; https://quran.ksu.edu.sa/tafseer/saadi/sura24-aya27.html; https://quran.ksu.edu.sa/tafseer/saadi/sura17-aya70.html; https://quran.ksu.edu.sa/tafseer/saadi/sura4-aya58.html.

Solove, Daniel J. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154, no. 3 (2006): 477–564. https://scholarship.law.gwu.edu/faculty_publications/921/.

Ṭabarī, Abū Jaʿfar Muḥammad ibn Jarīr al-. Jāmiʿ al-bayān. Arabic electronic commentary on Qur'an 49:12 and 24:27–28. King Saud University.

https://quran.ksu.edu.sa/tafseer/tabary/sura49-aya12.html;
https://quran.ksu.edu.sa/tafseer/tabary/sura24-aya27.html;
https://quran.ksu.edu.sa/tafseer/tabary/sura24-aya28.html.

UNESCO. Recommendation on the Ethics of Artificial Intelligence. November 23, 2021. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence.

Wachter, Sandra, and Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." Columbia Business Law Review 2019, no. 2 (2019): 494–620. https://doi.org/10.7916/cblr.v2019i2.3424.