



Online Data Privacy Ethical Guidelines based on Islamic Perspectives

**Ahmad Faiqun Nawwar Rofiq, Md Saidur Rahman, Ahmad Yusuf Shaikh,
Mamadou Bobo Barry, Akram M Zeki**

Faculty of Information and Communication Technology, International Islamic University
Malaysia

akramzeki@iium.edu.my

Abstract

In today's digital age, online data privacy is a critical concern, particularly as it intersects with ethical and cultural values. However, most organizations don't have any clear frameworks for online data privacy especially based on Islamic perspective. Islamic perspectives offer unique insights into privacy which could provide a robust ethical foundation for managing online data. This research aims to establish Ethical Frameworks for organizations operating in the Muslim community to protect personal information and uphold Islamic values. The results of this study highlight the urgent requirement of data privacy standards that are sensitive to culture and ethics for the concerned organizations and communities under Islamic influence. The increasing rate of digitization of collection and use of personal data brings a lot of challenges with respect to its use in ethical framework, a few of whom are not satisfactorily covered by the existing global frameworks. This study proposes the applicability of Islamic precepts in bridging this gap by providing a host of guidelines driven by the values of trust (Amanah), privacy (hifz al-'ird), public benefits (maslaha), and proportionality.

Keywords: Privacy, Data, Islam, Ethics, Frameworks,

1. Introduction

In the digital age, online data privacy is a critical concern, particularly as it intersects with ethical and cultural values. However, most organizations don't have any clear frameworks for online data privacy especially based on Islamic perspective. Islamic perspectives offer unique insights into privacy which could provide a robust ethical foundation for managing online data. This research aims to establish Ethical Frameworks for organizations operating in the Muslim community to protect personal information and uphold Islamic values.

The significance of this research lies in its attempt to bridge the gap between online data privacy and Islamic perspectives on ethical thought. While much research has been dedicated to online data privacy from a technical, legal, and ethical perspective, there are still few studies that define the frameworks of online data privacy in the context of Islamic principles and values. The relevance of this research is underscored by the fact that Islam plays a central role in the lives of about two billion people worldwide, and the principles articulated in Islamic ethics and jurisprudence have the potential to influence how organizations can use our data.

2. Objective

The objective of this study is to establish Online Data Privacy Ethical Guidelines based on Islamic Perspective for organizations in the Muslim community to protect personal information and uphold Islamic values.

This study aims to answer two main questions:

1. What are the key challenges in establishing data privacy frameworks based on Islamic ethics, and how can these challenges be addressed?
2. What specific ethical guidelines can be derived from Islamic teachings to protect online data privacy for individuals and organizations?

3. Methods

To answer the research questions, a qualitative research methodology with descriptive analysis and case study will be used. It aims to extract three things, First, analysing the organization's privacy policy using Google and Apple as case studies. Secondly, analysing journals, articles and academic papers related to online data privacy and finally analysing insights from Islamic texts, legal documents, and ethical writings relevant to online data privacy. A comprehensive selection of primary sources, including the Quran, Hadith, and classical Islamic jurisprudence texts, will be analysed to extract relevant principles and guidelines.

4. Results

A qualitative analysis of Google and Apple data privacy policy found that each company has their own distinct approaches to user data protection. The privacy guidelines established by Google, place a strong emphasis on transparency by giving users tools to govern their data, like privacy settings and preferences, as well as explicit information on data collection and usage. In order to adhere to its privacy policies, the organization conducts data minimization by gathering only necessary data, implements robust data protection measures including encryption and security audits, and limits third-party access. Meanwhile, Apple privacy policies prioritize user data minimization by only collecting the information that is required and refraining from using user profiles for marketing purposes. It uses end-to-end encryption to guarantee that no one, not even Apple, can access users' private information. Apple gives customers control over aspects like app permissions and tracking, prioritizes user consent for data collection, and incorporates privacy by design into its products. With its App Tracking Transparency feature, Apple further encourages transparency by giving consumers the ability to efficiently control third-party data access. Although both companies share a commitment to privacy, neither of them used any Islamic values in their privacy guidelines.

Based on qualitative analysis of journals, articles, and academic papers on online data privacy, the authors found that personal data privacy is crucial in this digital era, because organizations and companies can easily obtain, preserve, and transfer personal information. Data collecting, which is usually done through techniques such as cookies and embedded scripts, allows companies to personalize services and advertisements based on the user's online behavior, but it is often done without proper disclosure and user consent. Data sharing and selling to other parties, such as advertising and analytics businesses, can occur without the user's awareness, raising worries about the misuse of personal information. As data security breaches including leaks, identity theft, and online fraud become more widespread, so does the demand for personal data protection solutions. This has become a problem because most companies and organizations worldwide do not incorporate ethical frameworks based on Islamic views into their privacy policies, necessitating the development of a clear ethical framework on online data privacy based on Islamic perspectives that companies and organizations can incorporate into their privacy policies.

The qualitative analysis of the Islamic texts, legal documents and ethical writings revealed some major challenges with establishing data privacy frameworks based on Islamic ethics, particularly due to a lack of direct references regarding digital issues in classical Islamic jurisprudence. Islamic ethics can provide some guiding principles that can be adapted to contemporary data privacy issues, such as Amanah (trust), hifz al-'ird (protection of privacy), and maslaha (public interest). Islamic writings also emphasize the importance of personal privacy and protecting sensitive information. For example, in the Quran and Hadith, there are references to protecting the privacy of individuals, including their homes and personal affairs. These references highlight the significance of privacy and confidentiality, which should be applied to customer online data privacy by the companies. Preemptive measures should be taken to protect the privacy of customer data based on Islamic values.

5. Discussion

To establish Online Data Privacy Ethical Guidelines based on Islamic Perspective for organizations in the Muslim community to protect personal information and uphold Islamic values we need to answer the two research questions based on the analysis that has been conducted.

6. Challenges in Implementing Islamic Data Privacy Frameworks

1. Interpretation of Islamic Ethics in the Digital Era: The greatest challenge to establishing data privacy frameworks based on Islamic ethics is applying these principles to the most recent technologies. Digital data collection, amongst other things, was never mentioned by classical Islamic jurisprudence; this presents a void in the application of immediate ethical guidelines. Some scholars, like Al-Qaradawi (2009), feel that *ijtihad*, or independent reasoning, might help re-interpret Islamic ethics in the light of the digital era; however, according to Zaman (2014), there is no single methodology unified among scholars, hence the inconsistent applications across various Islamic traditions.

2. Balancing Individual Privacy and Societal Interests: Islamic ethics views an individual's right to privacy as one of the most sacrosanct, but it has provisions for derogation of this right where the public interest—so to say, national security or public health—requires it. The principle of “*la darar wa la dirar*” (no harm and no reciprocating harm) permits privacy to be compromised when necessary to prevent greater harm (Al-Shatibi, 1997). However, as Hassan (2011) highlights, such exceptions should be narrowly defined and strictly regulated to avoid misuse. The challenge lies in maintaining a balance between individual privacy and societal welfare while preventing unnecessary encroachment on privacy.

3. Consent and Informed Autonomy in Data Collection: Islamic ethics give paramount importance to consent, particularly when the question of personal dignity and wealth is involved in data. Many contemporary collecting practices are opaque and uninformative about how the data is collected, kept, or used, therefore not allowing users to be autonomous over it. The Hadith says, “None of you truly believes until he wishes for his brother what he wishes for himself” (Sahih al-Bukhari); fairness and transparency in all dealings, including data collection, is needed. Ali (2019) posits that organizations have to make users comprehend how their data is utilized and that their consent is given out of their free will.

7. Addressing Challenges: Solutions and Recommendations

1. Flexible, Adaptive Interpretations of Islamic Ethics: In this respect, applying Islamic ethics to the digital challenge requires an ongoing dialogue involving the participation of Islamic scholars, legal experts, and technologists. The principles of Islamic ethics may be adapted to

modern challenges by using *ijtihad*. According to Sadeq (2022), the blending of Islamic jurisprudence with current legal systems will establish adaptive and pertinent data privacy policies that reflect both ethical contemplation and technological development.

2. **Transparency and Consent Mechanisms:** A solution to the challenge of consent is developing clear, transparent consent processes. Islamic ethics requires transparency regarding the purpose of personal information, ensuring such consent has been given voluntarily and with due knowledge. Frameworks should, therefore, be developed where usage of data is clearly expressed and obtained with explicit, unambiguous consent. As Al-Qaradawi (2009) mentions, transparency will ensure *Amanah* between a person and the handlers of his data.

3. **Proportionality in Data Collection and Surveillance:** Islamic ethics advocate proportionality in all moves, actions, data collection, and surveillance. Surveillance and data collection should occur only when the situation calls for it. In that regard, the information collected must be minimum and purpose-specific. According to Al-Ghazali (2005), harm is to be minimized; this means data collection should be proportionate to the issue at hand. Such ethical considerations can help in developing methods of surveillance respectful of privacy and sensitive to legitimate public concerns.

4. **Strengthening Legal Frameworks for Data Protection:** Data protection laws can be enhanced in Muslim-majority countries by leveraging Islamic legal principles, including *Amanah* (trust) and *maslaha* (public interest). These principles thus lay the bedrock for legal frameworks that identify clearly defined rules regarding data ownership, access, and retention. Nashit (2018) argues that such frameworks should hold data controllers accountable for privacy breaches, while allowing exceptions when data sharing is genuinely necessary for public welfare. Strengthening legal protections can help balance individual privacy with broader societal benefits.

The establishment of a data privacy framework that is underlain by Islamic ethics poses both challenges and opportunities. Of prime importance are three challenges-interpretation of traditional Islamic principles, treading the thin line between individual privacy and public interest, and informed consent in data collection. Yet, such challenges can be addressed with flexibility in interpretation of Islamic ethics in relation to information, consent transparency, and proportionality in data collection, along with enhancement of legal frameworks for data protection. It means that aligning data privacy policy with Islamic ethical principles will create a system that respects both individual rights and the public good in the digital era.

8. The ethical guidelines can be derived from Islamic teachings to protect online data privacy for individuals and organizations.

There are several ethical principles derived from Islamic teachings regarding the protection of online data privacy at both the individual and organizational levels. These ethical principles spread from Quran, Hadith, and Islamic jurisprudence can be applied to guide that personal data should be accorded respect, transparency, and integrity. The basis and specific ethical guidelines are enumerated below:

1. Right to Privacy, Huqooq al-'Ibad

Islamic Teaching: Privacy is an indispensable right under Islam; the Quran stresses and demands respect for other people's privacy:

يَا أَيُّهَا الَّذِينَ ءَامَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ٢٧

O believers! Do not enter any house other than your own until you have asked for permission and greeted its occupants. This is best for you, so perhaps you will be mindful. (Quran, 24:27).

Ethical Guideline: Unless with explicit consent, personal data of an individual should not be accessed or used but with his expressed permission. The data shall not be transferred or disclosed without due authorization of the person.

2. Transparency and Informed Consent - Shura and Amanah

Islamic Teaching: transparency and mutual consent in the process are integral to Islamic ethics. The Prophet Muhammad SAW had said, "The believer is the one from whom people are safe regarding their blood and wealth" (Sahih Muslim). Secondly, there exists the concept of Amanah that projects that persons handling other people's data have been entrusted with its care.

Ethical Guideline: An organization should ensure that it provides all the clear and transparent details about the collection, processing, and usage of personal information. It must obtain informed consent freely and without coercion from an individual before collecting the data.

3. Minimization of Data Collection-Qasd and Proportionality

Islamic Teaching: Islam encourages moderation in all matters. The Quran admonishes:

يَا أَهْلَ الْكِتَابِ لَا تَغْلُوا فِي دِينِكُمْ وَلَا تَقُولُوا عَلَى اللَّهِ إِلَّا الْحَقَّ

O People of the Book! Do not go to extremes regarding your faith; say nothing about Allah except the truth.... 4:171

And this can be applied to data collection, encouraging minimalism.

Ethical Guideline: Data collection should not be done except when extremely necessary, and the volume of data that is to be collected must be related to the purpose it is serving. Organizations must avoid requesting excessive or unnecessary personal information.

4. Confidentiality (Sitr)

Islamic Teaching: Islam gives immense importance to maintaining confidentiality. Muhammad (PBUH) is reported to have said, "Whoever conceals the faults of a Muslim, Allah will conceal his faults on the Day of Judgment" (Sahih Muslim).

Ethical Guideline: Every organization has an ethical obligation to maintain the data of individuals in confidence and safeguard it from unauthorized access. Any breach of confidentiality is viewed as a violation of the trust granted to the data handler and is against any ethical conduct in Islam.

5. Prohibition of Harm (La Darar)

Islamic Teaching: The maxim "la darar wa la dirar" actually signifies no harm and no reciprocating harm in Islamic principles. This prohibits every action that may cause another harm. The unauthorized use of personal data leads to different harms such as identity theft or reputational damage.

Ethical Guideline: Organizations should not harm individuals with their data handling practices. Data must be processed in a secure manner whereby protective measures against breaches, leakages, and misuses are taken to avoid exposing any individual to harm.

These ethical guidelines from Islamic teachings give a wide perspective on online data privacy. The principle of privacy, transparency, consent, confidentiality, and prohibition of harm, while organisations are executing the best practices of data protection in conformity with Islamic ethical standards to protect the dignity and rights of individuals in the digital age.

9. Conclusion

This research underscores the relevance of Islamic ethics in addressing data privacy challenges. By developing an ethical framework based on Islamic principles, this study seeks to fill the existing gap in culturally specific approaches to data privacy. The findings provide an avenue for policymakers, organizations, and individuals to incorporate religious and moral considerations into data privacy practices, contributing a meaningful, faith-based perspective to the global conversation on digital ethics. The results of this study highlight the urgent requirement of data privacy standards that are sensitive to culture and ethics for the concerned organizations and communities under Islamic influence. The increasing rate of digitization of collection and use of personal's data brings a lot of challenges with respect to its use in ethical framework, a few of whom are not satisfactorily covered by the existing global frameworks. This study proposes the applicability of Islamic precepts in bridging this gap by providing a host of guidelines driven by the values of trust (Amanah), privacy (hifz al-'ird), public benefits (maslaha), and proportionality. On the other hand, Islamic ethics may provide organizations with robust but benign frameworks that emphasize transparency, consent, confidentiality, and minimization of harm in relations to Muslim communities, thus enabling organizations to operate with regard to data privacy principles. Such principles do not only coincide with the modern ethical view but also offer a culturally pertinent response to the problems of digital privacy. The research agrees with the criticisms about the application of classical Islamic law to modern technology issues that relate directly to the lack of direct mappings of such issues. However, it contends even so that there is space for the application of Muslim ethical principles to current issues through critical reasoning known as *ijtihad*. This strategy makes it possible

References

- [1] D. Suwondo, "The legal protection of personal data in Islamic perspective," *International Journal of Law Reconstruction*, vol. 7, no. 2, pp. 221, 2023.
- [2] K. Komaruddin, A. S. Utama, E. Sudarmanto, and Sugiono, "Islamic perspectives on cybersecurity and data privacy: legal and ethical implications," *West Science Law and Human Rights*, vol. 1, no. 04, pp. 166-172, 2023.
- [3] N. Md Norwawi, N. H. Mohd Alwi, R. Ismail, F. Wahid, and N. M. Alkaenay, "Promoting Islamic ethics on privacy in digital social networks for user data protection and trust," *Ulum Islamiyyah Journal*, vol. 13, Special Edition, pp. 115-127, 2014.
- [4] M. Lubis and M. Kartiwi, "Privacy and trust in the Islamic perspective: implication of the digital age," in *Proceedings of the 5th International Conference on Information and Communication Technology for the Muslim World*, 2013.
- [5] A. Al-Ghazali, *Al-Mustasfa min 'Ilm al-Usul (The Essentials of Islamic Jurisprudence)*. Beirut: Dar al-Ma'arif, 2005.
- [6] Y. Al-Qaradawi, *The Lawful and the Prohibited in Islam*. Kuala Lumpur: Islamic Book Trust, 2009.
- [7] I. Al-Shatibi, *Al-Muwafaqat (The Concurrence of the Aims of Sharia)*. Beirut: Dar al-Ma'arif, 1997.
- [8] R. Hassan, "Privacy in Islam: The Challenge of Balancing Public and Private Interests," *Islamic Law and Society*, vol. 18, no. 1, pp. 42-59, 2011.
- [9] M. Nashit, "The Role of Islamic Legal Principles in Shaping Modern Data Protection Frameworks," *Journal of Islamic Law and Technology*, vol. 12, no. 3, pp. 89-102, 2018.

- [10] A. Sadeq, "Islamic Ethics and Data Privacy: Adapting Principles to Modern Technology," *Journal of Islamic Ethics*, vol. 10, no. 4, pp. 201-215, 2022.
- [11] M. Zaman, "Ijtihad in the Digital Age: Islamic Ethics and the Internet," *Journal of Islamic Thought and Practice*, vol. 14, no. 2, pp. 78-91, 2014.
- [12] S. Sadeq, "Reinterpreting Islamic Ethics for the Digital Age," *Islamic Studies Review*, vol. 40, no. 3, pp. 43-58, 2022.
- [13] M. Zaman, "The Role of Ijtihad in Islamic Ethics and Technology," *Journal of Islamic Ethics*, vol. 9, no. 1, pp. 78-95, 2014.
- [14] M. Ali, "Islamic Data Privacy: Ethical Challenges and Solutions," *Journal of Islamic Ethics in Technology*, vol. 5, no. 2, pp. 107-123, 2019.
- [15] F. Khan, "The Concept of Privacy in Islamic Jurisprudence and its Relevance to Modern Data Protection Laws," *Islamic Studies Review*, vol. 22, no. 1, pp. 45-60, 2018.
- [16] Apple, "Privacy," *Apple.com*. [Online]. Available: <https://www.apple.com/privacy/>. [Accessed: 5-Dec-2024].
- [17] Google, "Policies," *Google.com*. [Online]. Available: <https://policies.google.com/>. [Accessed: 5-Dec-2024].