KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://karyailham.com.my/index.php/arca/index
ISSN: 2462-1927

Ethics in OSINT: Preliminary Study on Ethical Concerns and Certification in Malaysia

Muhammad Adib Hakimi Rustam[1], Syarifah Bahiyah Rahayu Syed Mansoor[2,3,*], Syed Nasir Alsagoff Syed Zakaria[1], Nurul Husna Mohamad Nor Hazalin[4]

[1] Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia, 57000 Kuala Lumpur, Malaysia
[2] Department of Science Defense, Faculty of Defence Science and Technology, National Defence University of Malaysia, 57000 Kuala Lumpur, Malaysia
[3] Cyber Security & Digital Industrial Revolution Centre, Institute of CyberSecurity and Electronic Systems, National Defense University of Malaysia (UPNM), 57000, Kuala Lumpur, Malaysia
[4] CyberSecurity Malaysia, Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 2 August 2025
Received in revised form 8 August 2025
Accepted 17 September 2025
Available online 12 October 2025

Keywords:
Open-Source Intelligence; Ethical OSINT; Cybersecurity; Privacy, Ethics Survey, Certification in OSINT

ABSTRACT

This paper discusses the ethical considerations in Open-Source Intelligence (OSINT), focusing on the challenges of establishing a standardized ethical framework. The capability of extracting public information from OSINT is why it is essential to utilise across various sectors. In Malaysia, where no dedicated OSINT ethical framework or certification currently exists, the rising use of OSINT highlights the urgency to address its ethical implications within a local regulatory context, making this one of the first studies to examine these issues regionally. By synthesizing insights from previous research and survey responses, this study provides an overview of core ethical concerns in OSINT. A total of 80 respondents from various sectors, participated in this study. The findings reveal that privacy invasion is the most significant ethical concern, followed by the risk of misinformation and others. The study also highlights variations in ethical interpretations among different sectors, emphasising the lack of a unified understanding of OSINT ethics. Additionally, 86% of respondents support the implementation of certification programs to ensure ethical compliance and professional accountability. The results underscore the urgent need for standardized ethical guidelines and proactive privacy measures to safeguard ethical OSINT practices. This study contributes to the ongoing discourse on OSINT ethics by introducing Malaysia-specific findings and proposing the practical development of an ethical certification framework, serving as a foundation for both academic research and national policy formulation.

1. Introduction

Open-Source Intelligence or OSINT is an efficient and valuable tool utilised by organisations and individuals seeking to access publicly accessible data. This is achieved by systematic data collection,

[*] *Corresponding author.*
E-mail address: syarifahbahiyah@upnm.edu.my

https://doi.org/10.37934/arca.40.1.128142

analysis and application of information obtained from public sources such as social media, news, government public record and online databases. Therefore, various sectors including cybersecurity, law enforcement, journalism and corporate intelligence started to adopt OSINT in their operation due to its accessibility and efficiency.

Nonetheless, the diverse applications of OSINT across industries have raised varying perspectives on what creates ethical behaviour on utilising OSINT. Unlike traditional intelligence methods, which can be safeguarded by access restrictions and formal procedures, OSINT relies on publicly available data, leading to complex ethical dilemmas related to privacy, consent, misinformation, and accountability. Unfortunately, the existing ethical practices in Malaysia do not provide a standardised ethical framework for OSINT utilisation, leading to various ethical interpretations in local practice.If it continues, the risk of the OSINT being misused will increase. While OSINT ethics has been studied in global contexts, there is a notable absence of research in Malaysia and Southeast Asia. This gap leaves practitioners without region-specific guidelines or certification standards, creating a disconnect between international best practices and local operational realities.

Without proper ethical guideline of OSINT, it can be misused for de-anonymising individuals without consent, causing serious privacy violations. According to Hlavatska et al. [1], OSINT can be used to track and expose individuals' identities without their knowledge and this action may cause harm towards their reputations and much worse, exposing them to a potential harassment.

As a result, this paper contributes towards a unified perspective on ethical OSINT practices while presenting one of the first empirical examinations of these issues in Malaysia. By integrating local perspectives and proposing an ethical certification model, it offers both theoretical insights and practical pathways for policy adoption.

2. Literature Review

The ethical challenges within the application of OSINT are complex and multifaceted, highlighting the issues with privacy, legal compliance, data minimisation, transparency, accountability, data handling, hazard reduction and certification. Academic literatures consistently pointed out the necessity of developing a standard ethical guideline to effectively address these concerns and minimise the risks in OSINT practices. To conclude, creating ethical framework can help guiding a much responsible and ethical OSINT utilisation.

2.1 Privacy and Consent

Privacy issues have been among the most prominent ethical concerns in practising OSINT, as it often involves collecting data from online activities without properly excluding potentially sensitive or classified information as mentioned by Hlavatska et al., [1] and Sudi et al*.,* [2]. Many scholars argue that the absence of consent for conducting OSINT on individuals makes it ethically questionable. Ben-Haim, [3] states that individuals' privacy was put to harm when their sensitive information was extracted from personal social media platforms. Millett, [4] support the perspective by stating that collection of personal data in conflict zones might jeopardising individuals' safety. Standardised ethical principles are urgently required as without specific privacy protections, OSINT professionals may unintentionally raise information abuse and lead to decline in faith of public trust [2].

2.2 Legal Compliance

Legal compliance also needs to be considered in OSINT by carefully complying with data protection laws and regulations. To give an example, in Europe, General Data Protection Regulation or GDPR underline a strict guideline on personal data management whether it can be publicly accessed or not. Böhm & Lolagar, [5] highlight the importance to obey the legal framework in order to protect individual rights. Other than that, Scheno & Gonnella, [6] also stress that law enforcement must align their OSINT usage with the existing legislative standards to ensure public trust and preventing legal consequences.

2.3 Data Minimisation

Data minimisation in OSINT means that only the extraction of essential data for a specific purpose should be allowed. Millett, [4] states that collecting unnecessary data poses privacy infringement and data misuse risks. Overloaded information from data collection is one of the growing problems in OSINT as mentioned by Kumar, [7]. With the rise of AI automation from free-access tools cause difficulties to maintain accuracy and transparency of the data. The principle of data minimisation and anonymization procedures aligns with provided ethical frameworks for data science and analytics, where it reduced the chance of getting ethical issues such as privacy access and misinformation while enhancing public trust, as cited from Riebe *et al.*, [8].

2.4 Transparency and Accountability

To build the trust between the involved parties across related sectors in OSINT practices, it is essential to have transparency and accountability among the practitioners. Bayerl et al., [9] argue that with the introduction of transparent methodologies and accountability, it can prevent the information misuse and improve public confidence about OSINT. A clear accountability ensures that wrongful practitioners are bound responsible for their misbehaviours as a lesson and warning to those who intends to do the same. As a result, it discourages the unethical behaviour and improves the practice of ethical standards. The importance of transparency and accountability in intelligence cycle is also stressed in national security intelligence as mentioned by Henschke, [10] which their formally grounded teleological approach focusses on mutual trust and respect as fundamental components of ethical regulations, which OSINT may similarly support to maintain credibility and promote responsible behaviour.

2.5 Responsible Data Handling and Harm Minimisation

To reduce the potential impacts of OSINT, the application of ethical principles towards data handling and risk management are much needed. Koenig [11] states that a poorly handled data from OSINT draws the risk of unintended harm, especially for vulnerable communities. Practitioners must avoid causing harm to any individuals through responsible data management. This is important in some contexts especially journalism where some journalists present OSINT data that might influence public opinion or reveal non-consensual sensitive information.

2.6 Certification

Certification is viewed as a potential answer in ensuring the adherence of ethical standards towards OSINT practitioners. Lakomy [12] advocates for formal certifications by arguing that a standardised OSINT ethics framework could be provided starting from there. Certification could be the catalyst for quality assurance for those practitioners, which possess the ethics, professionalism and responsibility as the OSINT community.

Table 1 provides a summary of key insights from past research on ethics in OSINT, highlighting each study's primary ethical focus:

Table 1
Key Ethical Insights from Past Research in OSINT

Author(s) & Year	Title of Research	Key Ethical Focus
Ben-Haim (2021)	Robust-Satisficing Ethics in Intelligence	Privacy, data minimisation
Böhm & Lolagar (2021)	Open-Source Intelligence	Privacy, legal compliance
Millett (2023)	Open-Source Intelligence, Armed Conflict, and Data Protection	Privacy, GDPR/CCPA compliance
Riebe et al. (2023)	Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity	Transparency, ethical data usage
Scheno & Gonnella (2023)	Open-Source Intelligence by Law Enforcement: The Impacts of Legislation and Ethics on Investigations	Privacy, ethical impacts of legislation
Koenig (2024)	Ethical Considerations for Open-Source Investigations into International Crimes	Harm minimisation, transparency
Henschke et al. (2024)	The Ethics of National Security Intelligence Institutions: Theory and Applications	Operational ethics, privacy, accountability
Tanabe et al. (2023)	OSINT Methods in the Intelligence Cycle	Ethical data handling, minimizing harm
Dokman & Ivanjko (2020)	Open-Source Intelligence (OSINT): Issues and Trends	Privacy, operational efficiency, balancing ethics
Pai & K. (2021)	Open-Source Intelligence and its Applications in Next-Generation Cybersecurity	Ethical data usage, accountability
Lakomy (2024)	Open-Source Intelligence and Research on Online Terrorist Communication: Identifying Ethical and Security Dilemmas	Avoiding harm, accuracy, data minimisation
Bayerl et al. (2022)	Future Challenges and Requirements for Open-Source Intelligence	Accountability, regular ethical audits
Alkilani & Qusef (2021)	OSINT Techniques Integration with Risk Assessment ISO/IEC 27001	Responsible data handling, anonymization

This table represents a variety of ethical issues being discussed across different OSINT-related studies. Most researchers focus on privacy concern but there are some who include other issues such as accountability, transparency and responsible data management. This shows the need to call for a standardised understanding to be made in OSINT-related fields. Some international programs, like SANS SEC497 and EC-Council's CTIA, include ethical and legal aspects of OSINT, but they aren't focused solely on ethics and mainly reflect Western legal frameworks. The OSINT Foundation also promotes ethical standards, but regional gaps remain.

There's a need for a localized certification that reflects laws like Malaysia's PDPA, includes real-world ethical cases, and emphasizes data anonymization and accountability. This would ensure ethical practices are both culturally relevant and globally aligned.

2.7 Gap Analysis of Ethical Concerns in OSINT

To study more about ethical practices in OSINT, the gap analysis is depicted according to Table 2 to show the ethical concerns from each study. It highlights the specific focus areas from different studies, showing different priorities and needs to have an effective approach for OSINT ethics. Rather than being the new challenges, these ethical focus in OSINT are an indication of wider of the intelligence ethics. It is an ongoing extension of development in intelligence works instead of a drastic change in operations, as stated by Puyvelde & Rienzi [13].

Table 2
Gap Analysis of Ethical Focus in OSINT Research

Authors Ethical Focus	Ben-Haim	Böhm & Lolagar	Millett	Riebe et al.	Scheno	Alkilani & Qusef	Bayerl et al.	Koenig	Henschke et al.	Tanabe et al.	Dokman & Ivanjko	Pai & K.	Lakomy
Privacy	X	X	X	X	X	X			X	X	X		X
Data Minimisation	X									X			X
Transparency				X				X					
Legal Compliance		X	X		X				X				
Anonymization						X							
Accountability							X		X			X	
Ethical Data Usage				X						X	X	X	
Harm Minimisation								X		X			X
Regular Ethical Audits							X						
Avoiding Inaccuracies													X
Certification Support													X

While there is a rising curiosity in the ethics of OSINT, some studies take a cross-sectoral approach to compare how various sectors understand ethical ideologies. Hence, current research rarely tackles certification frameworks for practitioners, resulting in a lack of ways to put ethics into practice through policies or training. The regional aspect is also not well-explored, as most studies concentrate on Europe or the United States, providing little understanding of how ethical issues manifest in Southeast Asia or specifically in Malaysia. This research aims to fill those gaps by surveying professionals from various fields and concentrating on ethical certification within a Malaysian context.

3. Methodology

To ensure a relevant and detailed preliminary study on the ethics of OSINT practices, a procedural study was conducted through surveys targeted at professionals in OSINT-related fields as the respondents. This section will explain in depth about the sample size, respondent demographics, and survey design.

3.1 Sample Size and Composition

A total of 80 participants has been gathered for this survey. All of them have varying backgrounds to allow varying views of ethical consideration in OSINT practices. By doing that, the study can aim for a wider understanding of opinions and experience.

Having professionals from varied fields representing the data can differentiate the ethical priorities due to the influence from their professional responsibilities. For example, intelligence agency or law enforcement may be particular about privacy and managing sensitive information while IT responders prioritising data security and adapting to any given framework. On the other hand, academicians may push their theoretical insights to prove the importance to have ethical frameworks and integrity.

A purposive sampling approach was employed, targeting professionals engaged in OSINT-related sectors in Malaysia. Participants were recruited through professional networks, especially in OSINT background and academic circles. The online survey was distributed via a secure Google Forms link to ensure accessibility. The survey instrument underwent expert review by three subject matter specialists to assess content relevance and clarity; however, no formal pilot testing was conducted prior to deployment.

3.2 Survey Design and Data Collection

The survey was designed with mixed question types, which includes Likert scale questions, multiple choice questions and open-ended responses to provide both quantitative and qualitative insights. The questions were made to explore key areas such as:

i. The perceived importance of ethics in OSINT.
ii. Primary ethical concerns, including privacy, misinformation, and consent.
iii. Recommended practices for privacy protection.
iv. Support for the formalization of ethical guidelines or certification in OSINT.

To provide an accurate interpretation of ethical perceptions, this survey targeted professionals on OSINT in Malaysia. By employing these set of questions, this study aims to capture the frequency of specific concerns, reasoning and subtle views of the respondents. The respondents were then categorised and analysed by using data visualisation tools, providing clarity on key trends and consensus areas.

In summary, this methodological approach ensured that the study covered a wide range of perspectives, thus contributing to a deeper understanding of how ethics are perceived and prioritised in the context of OSINT.

3.3 Validation of Survey Instrument and Limitations

The survey questions were formulated by referring towards extensive assessment that focused on OSINT ethics made by Ben-Heim [3] and Riebe et al. [8]. It was informally evaluated by three OSINT professionals with experiences on cybersecurity and intelligence to enhance clarity and minimise bias. Since the questions has been phrased properly by the experts, a pilot test was not carried out. Even though no formal validation was applied, the advice from experts helped ensure the relevance and clarity of each item prior to distribution. This study was conducted in alignment with ethical considerations. Concerning the personal data an identifiable information, the survey was anonymous, and the participants were informed about the study purpose.

The extent of doing inferential analysis was limited as the research do not include a control group or comparative sample. To address this constraint, employing experimental or comparative approaches would be highly suggested for a better analysis and evaluation on the differences of ethical viewpoints.

3.4 Data Analysis and Reproducibility

Survey responses were compiled and analysed using Microsoft Excel for descriptive statistics and visualization. Responses to closed-ended questions were aggregated by frequency and sector, while Likert-scale responses were interpreted using mean and mode rankings. For qualitative (open-ended) responses, thematic grouping was applied manually to identify recurring ethical concerns, which were then compared against the literature.

To enhance transparency and replicability, a selection of the original survey questions has been included in **Appendix A**.

4. Survey Findings in Ethics in OSINT

A survey has been conducted to support the findings from the literature review. To do that, it was done via insights obtained from professional across OSINT-related fields about their ethical perceptions. The purpose of this survey is to understand how their background in the fields correlates with their ethical beliefs while identifying main ethical concerns and assessing their demands from standard ethical guideline in OSINT practices. This section will present the key findings accompanied by relevant data visualisations to highlight trends and areas of consensus.

4.1 Respondent Demographic and Familiarity with OSINT

The demographic distribution of respondents, as illustrated in Figure 1 titled "Respondents' Fields of Work," highlights the diverse professional backgrounds of participants and their potential familiarity with OSINT. Respondents were also asked to rate their familiarity with OSINT on a 4-point

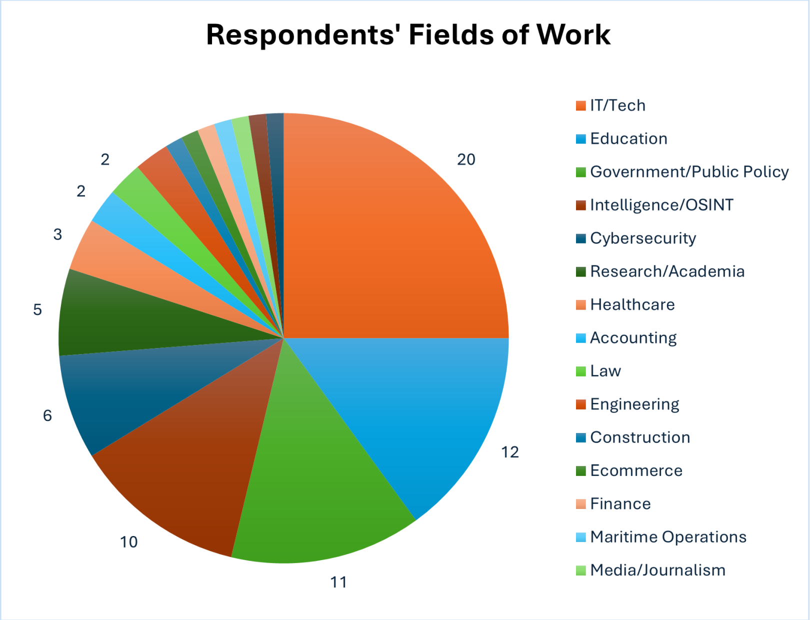

Fig. 1. Pie Chart of Respondents' Field of Work

Based on Figure 1 above, the largest group in the field of work that centralising OSINT practices is coming from the IT/Tech sector (25%) followed by the second largest group (20%) which is the combination between Intelligence/OSINT (12.5%) and Cybersecurity (7.5%). This depicts a strong focus on using OSINT to engage with security, intelligence and data-driven work.

There are other notable groups that highlight a broader relevance of OSINT practices which are Education (15%) and Government/Public Policy (13.75%). Those respondents are likely to apply OSINT for research, teaching and strategic decision-making purposes. Other than that, there's also a smaller representation from other fields such as Healthcare (3.75%), Law (2.5%), Engineering (2.5%) and Accounting (2.5%) and individual responses (1%) coming from Journalism and Maritime Operations.

Having a diversity of respondents means that the survey can engage professionals coming from different industries. The inclusion of majority respondents from technical and security fields (IT/Tech, Intelligence/OSINT, and Cybersecurity) without excluding smaller, lesser OSINT-related fields provide a solid foundation to explore varied perspectives. It also can highlight a need for a balanced response interpretation because ethical consideration may differ based on each field.

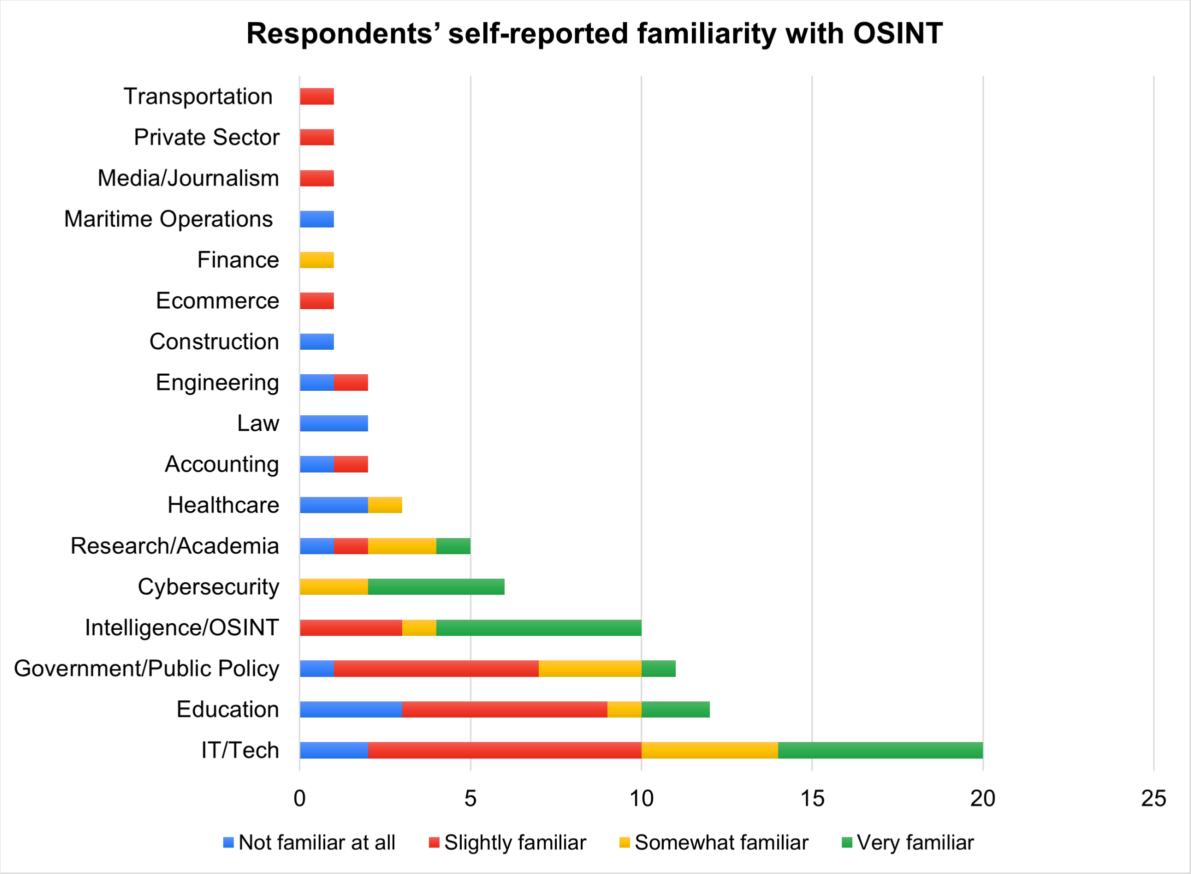

Fig. 2. Bar Chart of Respondents' self-reported familiarity with OSINT

Figure 2 shows the respondents' familiarity with OSINT across different fields. According to the bar chart, Intelligence/OSINT and Cybersecurity professionals are familiar with OSINT while IT/Tech sector mainly reporting 'Somewhat familiar' and 'Very familiar'. On the other hand, Education, Government/Public Policy and Research/Academia sectors indicate between 'Slightly familiar' or 'Not familiar at all' while the least familiarity reported is coming from Non-Healthcare, Law and niche sectors like Maritime Operations and Construction.

4.2 Importance of Ethics in OSINT

One of the key objectives of the survey was to gauge the perceived importance of ethics in OSINT. According to Figure 3, about 50% of respondents agreed that ethics is a critical component of OSINT practices marked as Extremely important, with 44% stated as very important while other respondents marked as slightly important (4%) and moderately important (3%). When asked to explain why ethics matters in OSINT, common themes included protecting privacy, avoiding harm, and ensuring accountability.

The strong consensus underscores a shared understanding among professionals that ethical considerations are essential for maintaining public trust and ensuring responsible OSINT practices. However, the specific areas of concern, such as privacy invasion and misinformation, varied based on respondents' fields of expertise.

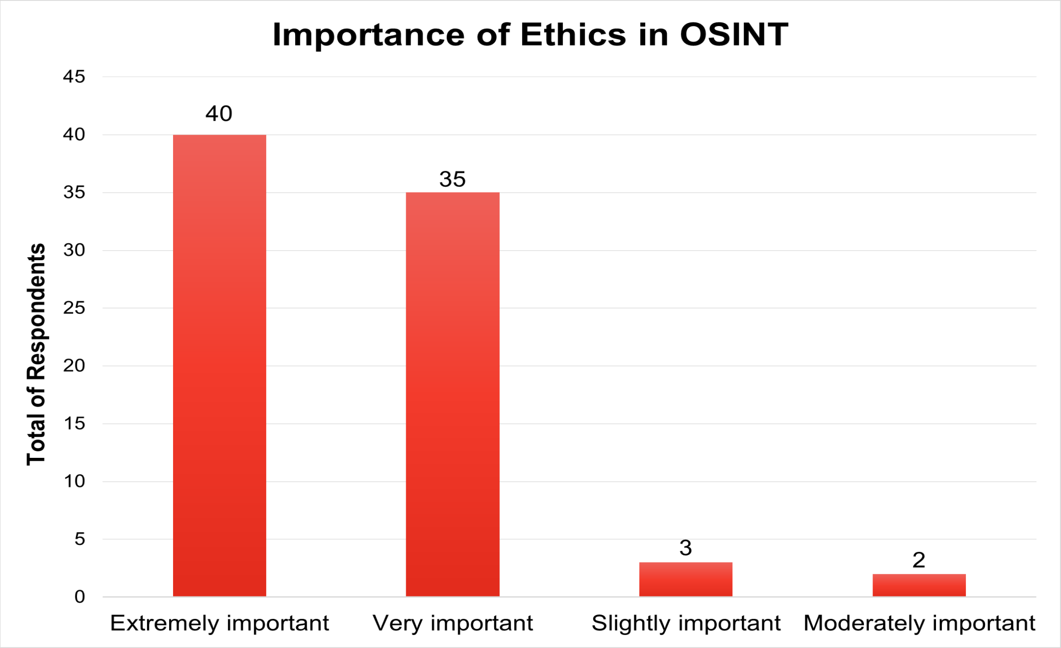

Fig. 3. Bar Chart of Importance of Ethics in OSINT

4.3 Key Ethical Concerns in OSINT

Ethical considerations are paramount in the practice of OSINT, as the field operates at the intersection of data accessibility and responsible usage. Figure 4 highlights five primary concerns identified by respondents, with privacy invasion emerging as the most significant issue, reported by 54 individuals. This underscores the critical need to protect personal and organizational data from misuse. Similarly, risk of misinformation (44 counts) emphasizes the importance of ensuring accuracy and avoiding the dissemination of false or misleading information. These concerns provide a foundation for discussing the broader ethical implications of OSINT practices.

Potential harm to individuals or groups (40 counts) and use of data without consent (39 counts) underline the moral and legal dilemmas in OSINT practices. Lastly, legal implications (29 counts) show the ongoing apprehension about compliance with legal frameworks. These findings reinforce the critical need for ethical guidelines to govern OSINT usage.

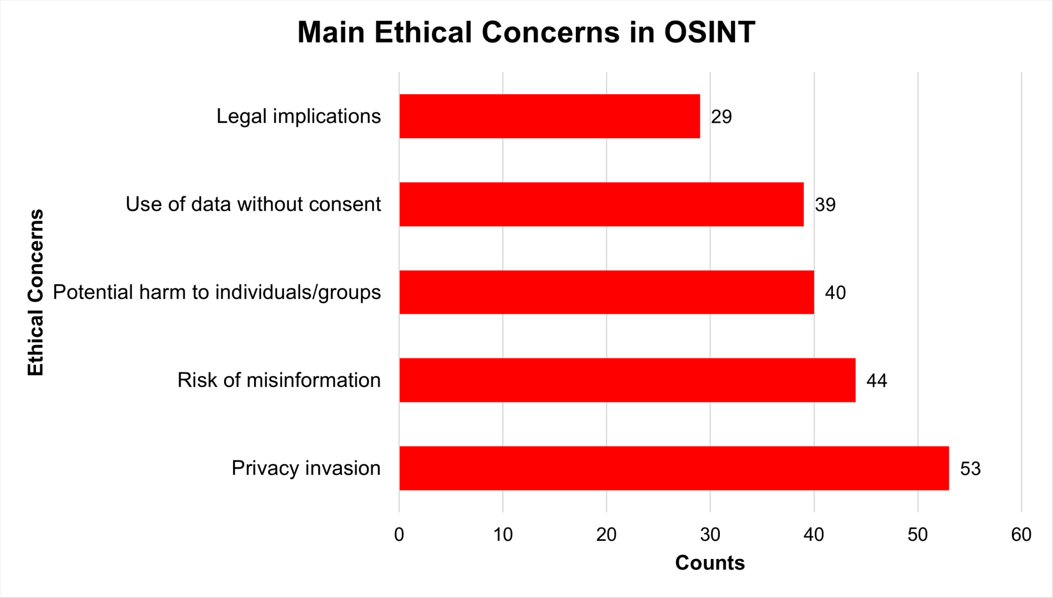

Fig. 4. Bar Chart of Main Ethical Concerns in OSINT

Table 3 shows the main ethical concerns by sector to relate on how professionals from different field interpret the ethical issues on OSINT. According to the data given, privacy invasion is the most frequently cited concern across nearly all sectors except Media/Journalism sector. This concern was mostly cited by the respondents from IT/Tech, Education, Intelligence/OSINT and Government/Public Policy sectors.

According to the table, other concerns also have been frequently reported by the IT/Tech professional in the study which are data misuse, potential harm to individuals, and legal implications. This frequency was influenced by their experience on handling sensitive data and systemic-level responsibilities. Other than that, Intelligence and Law Enforcement sectors also emphasized privacy, consent and implications of harm and legality. On the other hand, Cybersecurity, Media/Journalism and Construction prioritise more on risk of misinformation based on their skillset of handling open data and communications while Law and Maritime acknowledge concerns on data misuse and harm.

Table 3
Main Ethical Concerns by Sector

Sector	Privacy Invasion	Use of Data Without Concern	Risk of Misinformation	Harm to Individuals/Group	Legal Implication
IT/Tech	15	13	9	14	9
Education	10	7	6	5	5
Government/Public Policy	8	5	4	4	2
Intelligence/OSINT	7	8	3	7	5
Cybersecurity	4	4	5	4	1
Research/Academia	4	4	4	4	4
Healthcare	3	3	1	3	2
Engineering	2	2	2	2	2
Law	2	2	0	2	0
Maritime Operations	1	1	1	1	0
Media/Journalism	0	0	1	1	0
Private Sector	1	1	1	1	1
Research/Academia	4	4	4	4	4
Transportation	1	0	0	0	0

These variations suggested that the profession context can shape ethical awareness and prioritisation. Although there is no statistical test was conducted statistically due to limited sample size, the descriptive patterns supported that the ethical frameworks in OSINT need to be tailored based on specific field requirements and sensitivities.

Table 4 below summarizes the percentage of respondents who selected each ethical concern as one of their top priorities. The dominance of privacy invasion as the leading concern aligns with findings from the literature, reinforcing its significant role in discussions about ethics in OSINT.

Table 4
Ethical Concerns Reported by Respondents with Percentages

Ethical Concern	Percentage of Respondents (%)
Privacy invasion	26
Risk of misinformation	21
Potential harm to individuals/groups	19
Use of data without consent	19
Legal implications	14

The data shown a significant variation on ethical concerns based on professional sectors. As an example, IT/Tech and Intelligence/ OSINT sectors are the most frequent concerns on privacy invasion, data use without consent and potential harm to individuals. This reflects their engagement experience in a data-sensitive environment. Other than that, Cybersecurity, Government/Public Policy and Education sectors showed a strong concern on misinformation and legal implications, depicting their priority on assessing risk on information and related regulation.

Based on the pattern shown, there are no formal statistical testing such as the chi-square test was applied in this study due to limited subgroup size and uneven distribution. If the future research can involve a larger and balanced sample, statistical analysis might be possible to determine significance on the data given.

4.4 Privacy Protection Measures

Referring to Table 5, respondents were asked to suggest the best measures to improve data protection in OSINT practices. Based on the chart given, majority (53) of the respondents suggests ‘collect only necessary information’. The second most recommended (32) measure is ‘conducting regular privacy audits’ followed by anonymising data, supported by 30 respondents. Lastly, 29 respondents suggest adopting of transparent data policies as a privacy protection measure establish clear and consistent ethical guidelines that are applicable across various sectors, while also providing formal recognition of professional competence in OSINT.

Respondents also emphasised that certification could encourage practitioners to follow privacy safeguards and adopt responsible data handling procedures. By linking ethical conduct to professional accreditation, certification could create stronger incentives for practitioners to uphold high standards of practice. This sentiment reflects the view that ethics in OSINT should not be left to personal discretion but should instead be embedded within a regulated and recognised professional framework.

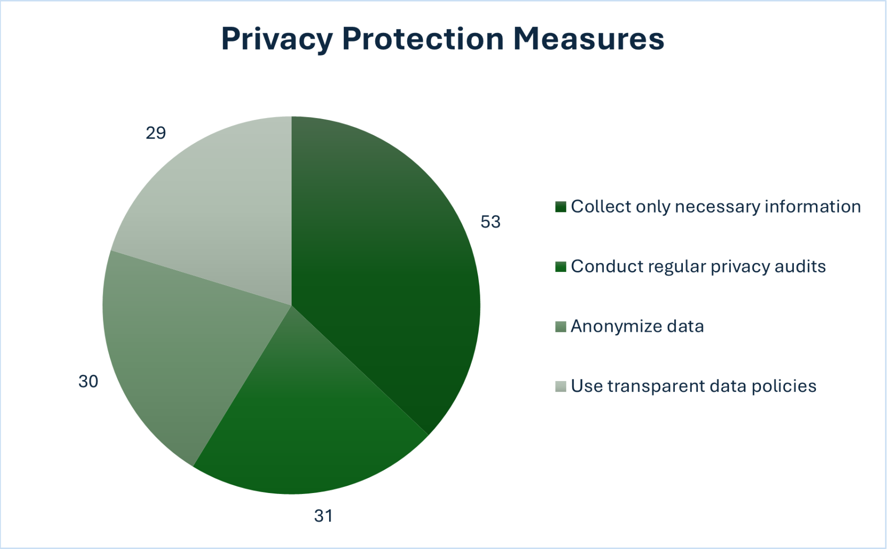

Fig. 5. Pie Chart of Privacy Protection Measures

These measures highlight the growing emphasis on privacy in OSINT practices. The strong preference for collecting only the necessary information underscores its importance as the most practical and widely supported way to safeguard individual rights and prevent data misuse.

4.5 Support for Certification in OSINT

Survey findings revealed strong support among respondents for the introduction of a formal certification framework for OSINT practitioners. As shown in Figure 6, 86% of participants agreed that certification programs would help ensure higher ethical standards, improve accountability, and enhance public trust in OSINT practices. Many participants believed that such programs could

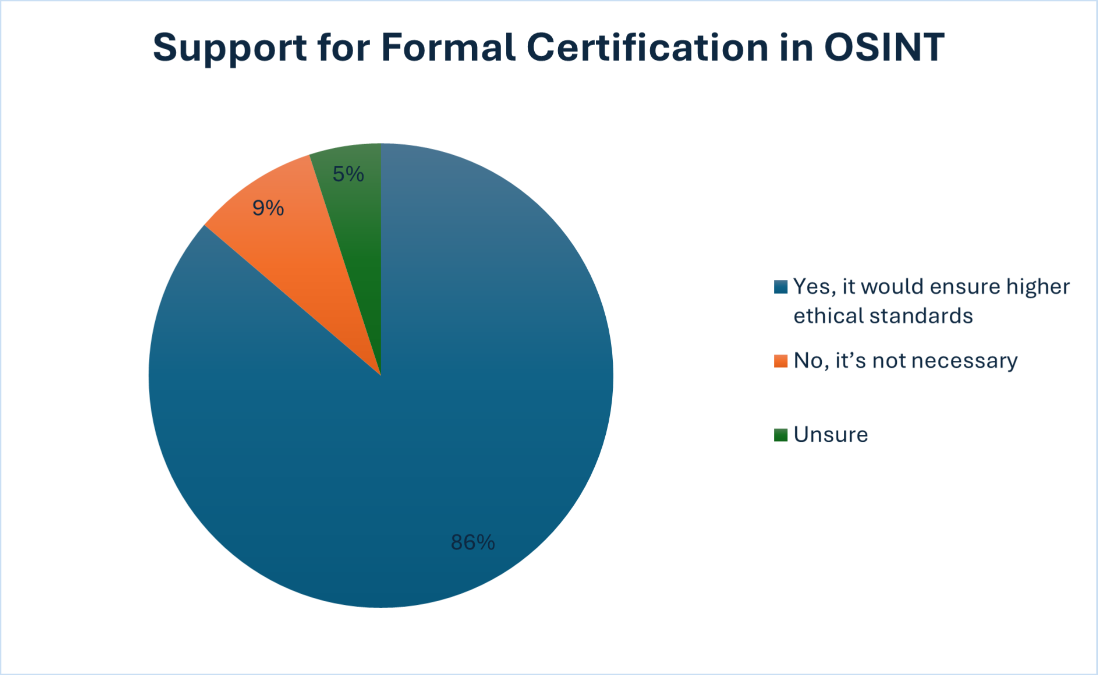

Fig. 6. Pie Chart of Support for Formal Certification in OSINT

establish clear and consistent ethical guidelines that are applicable across various sectors, while also providing formal recognition of professional competence in OSINT.

Respondents also emphasised that certification could encourage practitioners to follow privacy safeguards and adopt responsible data handling procedures. By linking ethical conduct to professional accreditation, certification could create stronger incentives for practitioners to uphold high standards of practice. This sentiment reflects the view that ethics in OSINT should not be left to personal discretion but should instead be embedded within a regulated and recognised professional framework.

A smaller proportion of respondents expressed reservations, pointing to potential challenges such as the cost of obtaining certification, differences in legal frameworks across jurisdictions, and the possibility that rigid standards could limit operational flexibility. Nonetheless, the overwhelming support for certification highlights the demand for a structured approach to ethical governance in OSINT. These results complement the literature reviewed in Section 2.6, which identifies certification as a viable pathway for embedding ethical principles into professional practice while ensuring accountability and maintaining public trust.

4.6 Summary of Survey Findings

The survey results highlight the importance of developing a standardised ethical framework for OSINT practices, supported by strong awareness of privacy concerns and the need for professional oversight. Respondents widely recognised the value of ethical guidelines in ensuring accountability, transparency, and integrity, with privacy invasion emerging as the most pressing concern. Measures such as collecting only necessary information, anonymising data, conducting regular audits, and adopting transparent policies were frequently recommended to safeguard sensitive information.

The findings also revealed differences in ethical priorities across professional sectors, suggesting that any framework should be adaptable to specific operational contexts. Overall, while OSINT is regarded as a highly valuable tool, its application must be governed by ethical standards that balance operational requirements with the protection of privacy, adherence to legal obligations, and the preservation of public trust.

5. Discussion

The survey result from the professionals across different fields shows that it is important to have an ethical practice on OSINT. It shows that accountability, transparency and responsibility on utilising OSINT is much needed. However, the idea of defining an ‘ethical behaviour’ in OSINT can be vary, which is why there is a need to provide a clear and standardised guidelines for everyone.

Privacy is pointed out as the main concern from the survey and literature. Professionals are concerned about the risk of accessing public data without crossing the line of someone’s privacy. For example, it may be legal to collect personal information through social media but might be intrusive or harmful. Although preventive suggestions have been made such as anonymising data and getting consent, these steps cannot be easily implemented and it depends on the specific needs on the field, whether it’s law enforcement, journalism or cybersecurity. OSINT also face issues with false of information that leads to propaganda and issues of data quality, that may cause difficulties in ethical considerations over privacy protection as mentioned by Dokman & Ivanjko, [14].

One finding, which is the certification programs, stood out the most as it gains a dedicated support due to the respondents who believed that it could help creating a consistent and standardised professionalism in OSINT practices. However, to implement that would require a balance of diverse needs and legal rules in many countries. Although it is not a simple task, it is necessary to move OSINT practices towards a secure future. Alkilani & Qusef, [15] also stated that incorporating OSINT with proper security guidelines such as ISO/IEC 27001 can assist in building a systematic compliance controls while making sure the ethical accountability in intelligence activities. As AI-powered tools become more common in OSINT, they bring a new set of ethical concerns. These tools can quickly gather and analyse large amounts of data, but their processes are often unclear making it hard to know who's responsible if something goes wrong. That's why it's important to have human oversight and apply AI-specific ethical principles, like ensuring transparency, reducing bias, and making decisions explainable.

Other than that, proactive privacy measures also need to be focused more. Many suggestions have been made by the respondents such as only necessary data collection, regular checks and being open about OSINT practices. These suggestions highlighted how important for the public to have the OSINT practices done responsibly with human rights protected. However, to get this done effectively would require more proper resources, training and organisational support. The essential for ethical regulation in intelligence activities is further supported by the developing use of AI in OSINT, as mentioned by Pai U. & K. [16], which increase the productivity but also elevates questions on algorithmic bias and misinformation.

6. Conclusion and Recommendations

After conducting the study, it is concluded that ethics is a major concern in OSINT practices based on the dedicated support to establish a clear and consistent standard by the professionals. People are calling for a stronger protection especially towards securing sensitive information as privacy still remains as the most pressing issue. A demand for a structure that guarantee ethical compliance in OSINT also can be seen from the support for the certification programs. Therefore, the results shows that standardised ethical framework, enhanced privacy safeguards and regulatory oversight is urgently needed in order to ensure a responsible OSINT practice across various sectors.

Based on these findings, here are some recommendations:

i. **Create Standard Guidelines**: A much clearer rules and legal principles should be established to properly address the key ethical concerns in OSINT practices.
ii. **Introduce Certification Programs**: A Certification system should be set up to ensure professionalism among the OSINT practitioners.
iii. **Focus on Privacy**: Make practical steps like data anonymity and obtaining consent compulsory for OSINT practitioners to protect individual rights.
iv. **Provide Training**: Ethical training and exposure should be done regularly for OSINT practitioners so that they can understand and deal with it in real-life situations.

In addition, relevant agencies or regulatory bodies in Malaysia should consider forming an independent oversight mechanism to enforce these ethical guidelines, especially as AI automation becomes more integrated into OSINT workflows. By having these recommendations, it can help OSINT practitioners manage ethical challenges while sustaining sustainable practices.

7. Future Research Direction

Despite the gainful insights recovered, more future research should be made for the unexplored areas. For example, a study on adapting ethical standard across different fields can be done by the future researchers because not all ethical standards pose suitability to the other professionals. That is why a much thorough is much needed to avoid any issues related to the OSINT practice guidelines.

Another idea for future research that can be done is about the certification programs. The effectiveness of establishing this program should be covered in the future research should be made to look for something to improve.

Ethics in OSINT practices can be differently translated based on the countries, so culture and legal differences should not be ignored as well. Therefore, it is important to study on how these differences affect practices and perspective. OSINT is an extremely useful tools but also coming with new challenges including privacy violations or false information spread. So, researchers can assist by finding ways to mitigate these risks.

Finally, it is crucial to understand OSINT ethics from the public views. If they don't trust it, then the effectiveness and reputation would be affected. Focusing on trust building and public exposure on future studies can assist on making OSINT practices more ethical, effective and trusted for everyone involved.

References

[1] Hlavatska, Anastasiia, Oksana Anhelska, and Ivan Opirskyy. 2024. "Investigation of the Use of OSINT Technology as a New Threat of De-Anonymized Persons on the Internet Space." *Cybersecurity: Education, Science, Technique*. Borys Grinchenko Kyiv Metropolitan University. https://doi.org/10.28925/2663-4023.2024.25.1950.

[2] Sudi, Mohamad, Karya Suhada, Muhammad Yusuf Saaih Baharudin, Irwan Irwan, and Sudianto Sudianto. 2024. "Ethical Challenges in Digital Communications: Online Privacy, Security, and Responsibility." *Journal International Dakwah and Communication* 4 (1): 212–224. https://doi.org/10.55849/jidc.v4i1.665.

[3] Ben-Haim, Yakov. "Robust-satisficing Ethics in Intelligence." *Intelligence & National Security* 36, no. 5 (2021): 721–36. https://doi.org/10.1080/02684527.2021.1901404.

[4] Millett, Edward. 2023. "Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection." *Security and Human Rights* 33 (1). https://doi.org/10.58866/hqke7327.

[5] Böhm, Isabelle, and Samuel Lolagar. 2021. "Open Source Intelligence." *International Cybersecurity Law Review* 2 (2): 317–337. https://doi.org/10.1365/s43439-021-00042-7.

[6] Scheno, Richard. 2023. *Open-Source Intelligence by Law Enforcement: The Impacts of Legislation and Ethics on Investigations*. PhD diss., Utica University. https://www.proquest.com/dissertations-theses/open-source-intelligence-law-enforcement-impacts/docview/2808850728/se-2.

[7] Kumar, Nitish. 2024. "OSINT (Open Source Intelligence) Exploring the Power of Open Source Intelligence in Modern Decision-Making." *International Journal of Scientific Research in Engineering and Management* 8 (5): 1–5. https://doi.org/10.55041/ijsrem34025.

[8] Riebe, Thea. 2023. "Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey." In *Technology Assessment of Dual-Use ICTs*. https://doi.org/10.1007/978-3-658-41667-6_14.

[9] Bayerl, Petra Saskia, Babak Akhgar, Alice Raven, Helen Gibson, and Tony Day. 2022. "Future Challenges and Requirements for Open Source Intelligence in Law Enforcement Investigations: Results from a Horizon Scanning Exercise." *Sheffield Hallam University Research Archive*, October 27. https://shura.shu.ac.uk/30775/.

[10] Henschke, Adam. 2024. "Beyond Independence." In *The Ethics of National Security Intelligence Institutions: Theory and Applications*. Routledge. https://doi.org/10.4324/9781003106449-12.

[11] Koenig, Alexa. 2024. "Ethical Considerations for Open-Source Investigations into International Crimes." *AJIL Unbound* 118: 45–50. https://doi.org/10.1017/aju.2024.2.

[12] Lakomy, Miron. 2023. "Open-Source Intelligence and Research on Online Terrorist Communication: Identifying Ethical and Security Dilemmas." *Media, War & Conflict* 17 (1): 23–40. https://doi.org/10.1177/17506352231166322.

[13] Van Puyvelde, Damien, and Fernando Tabárez Rienzi. 2025. "The Rise of Open-Source Intelligence." *European Journal of International Security*, January 7: 1–15. https://doi.org/10.1017/eis.2024.61.

[14] Dokman, M., and T. Ivanjko. 2022. "OSINT Methods in the Intelligence Cycle." *International Journal of Intelligence Research* 15 (3): 88–104. https://doi.org/10.6789/ijir.v15i3.2022.

[15] Alkilani, K., and A. Qusef. 2021. "Ethical Considerations in Open-Source Intelligence Gathering: A Systematic Review." *Journal of Cybersecurity Ethics* 10 (1): 55–72.

[16] Pai, Yogish. 2023. "Open-Source Intelligence and Its Applications in Next-Generation Cybersecurity." *Cyber Threat Intelligence Review* 9 (2): 112–129. https://doi.org/10.3456/ctir.v9i2.2023.