

Universal Declaration of Open-Source Intelligence (OSINT)

Marie Seshat Landry
Marie Landry's Spy Shop
www.marielandryceo.com
ceo@marielandryceo.com

April 2, 2025

Preamble

Recognizing the transformative power of Open-Source Intelligence (OSINT) in fostering transparency, accountability, and informed decision-making, we declare the following principles to ensure the ethical, responsible, and effective use of OSINT. This declaration seeks to establish a global standard that respects fundamental rights, promotes security, and upholds integrity in the collection, analysis, and dissemination of publicly available information.

Article 1: Definition of OSINT

OSINT is the systematic collection, analysis, and dissemination of publicly available information from diverse sources, including but not limited to media, social networks, government reports, academic research, and publicly accessible databases, for the purpose of generating actionable intelligence while respecting legal and ethical standards.

Article 2: Fundamental Principles

1. **Legality** – OSINT activities must comply with national and international laws, avoiding unauthorized access to private or classified information.
2. **Ethical Conduct** – Practitioners must adhere to ethical guidelines that promote transparency, honesty, and non-manipulation of data.
3. **Accountability** – Individuals and organizations engaged in OSINT must ensure responsible use and mitigate risks of misuse.
4. **Privacy and Human Rights** – OSINT practices must respect individuals' rights to privacy and avoid unnecessary harm, discrimination, or persecution.
5. **Transparency and Integrity** – OSINT findings must be reported accurately, with clear source attribution and verification of authenticity.

6. **Non-Malicious Intent** – OSINT should not be used for purposes that contribute to harm, misinformation, or repression of fundamental freedoms.

Article 3: Responsible Use and Oversight

1. **Verification and Fact-Checking** – OSINT practitioners must prioritize accuracy by cross-referencing multiple sources and validating information before dissemination.
2. **Data Protection and Anonymity** – Personal and sensitive data must be handled responsibly to prevent misuse or exploitation.
3. **Security and Risk Awareness** – Users of OSINT must be aware of potential threats, including misinformation, digital surveillance, and cyber risks.
4. **Ethical Training and Education** – Governments, organizations, and independent practitioners should promote training on ethical OSINT practices.
5. **Public Interest and Journalism** – OSINT should be leveraged to support investigative journalism, public safety, and human rights advocacy while safeguarding journalistic integrity.

Article 4: Implementation and Global Cooperation

1. **International Collaboration** – Governments, institutions, and civil society should collaborate to establish best practices and policies for OSINT.
2. **Open Access and Knowledge Sharing** – OSINT methodologies should be shared to strengthen public awareness, security, and accountability.
3. **Preventing Misuse** – Mechanisms should be in place to detect and mitigate the misuse of OSINT for disinformation, harassment, or unethical surveillance.
4. **Adaptability and Evolution** – Given the rapid technological changes, OSINT principles must evolve to address new challenges and threats in the digital age.

Conclusion

This Universal Declaration of OSINT serves as a foundation for ethical, transparent, and responsible intelligence gathering. It is a call for individuals, institutions, and nations to uphold these principles, ensuring that OSINT remains a tool for knowledge, accountability, and the greater good of society.