
Universal Declaration on Legal Espionage and the Primacy of Open-Source Intelligence (OSINT)

Preamble

- **Recognizing** the inherent dignity and equal and inalienable rights of all members of the human family as the foundation of freedom, justice, and peace in the world, as proclaimed in the Universal Declaration of Human Rights and the International Covenants on Human Rights,
- **Affirming** that information in the public domain constitutes the collective property and wealth of humanity, essential for an informed citizenry and robust democratic discourse,
- **Declaring** that **Open-Source Intelligence (OSINT)** represents the ethical, lawful, and primary foundation of all modern intelligence practice, operating within the boundaries of privacy, freedom of expression, and the rule of law,
- **Emphasizing** that espionage derived from secret, coercive, or extralegal means, particularly those involving arbitrary interference with privacy, unlawful surveillance, or human rights violations, fundamentally undermines human dignity, democratic governance, state sovereignty, and the international rule of law,
- **Asserting** that only governments, acting under exceptional circumstances, subject to strict democratic supervision, and in full compliance with national and international legal frameworks, may employ non-OSINT intelligence practices,
- **Convinced** that adherence to these principles will foster greater trust, transparency, and stability in international relations, safeguarding individual liberties while ensuring collective security through responsible and legitimate intelligence practices,

We, the peoples of the world, proclaim this Universal Declaration on Legal Espionage.

Articles

Article 1. Definition of Legal Espionage

Legal espionage shall mean the collection, analysis, and dissemination of information **exclusively derived from publicly available, open sources**, including but not limited to media, academic research, public records, geospatial imagery, scientific publications, publicly shared data sets, and digital communications lawfully accessible. Such lawful accessibility explicitly excludes any means requiring covert methods, unauthorized access to private systems or data, deception regarding identity or intent that infringes upon rights, or violations of privacy as protected by international human rights law.

Article 2. Primacy of OSINT

OSINT shall be considered the ethical, lawful, and foundational methodology for all modern intelligence disciplines, including but not limited to Human Intelligence (HUMINT), Artificial Intelligence-assisted analysis, Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), and business intelligence. All intelligence gathering, regardless of methodology, must **prioritize and exhaust OSINT avenues** before considering other methods, and integrate OSINT findings to contextualize, validate, and ethically ground all other intelligence, ensuring consistency with human rights and the rule of law.

Article 3. Education and Accessibility

1. OSINT education, beginning with foundational principles, shall constitute the primary curriculum of all lawful intelligence training, both governmental and private. This education shall inherently include critical thinking, source validation, ethical considerations, data privacy best practices, and a comprehensive understanding of national and international legal boundaries, particularly concerning freedom of information and expression.
2. Access to OSINT knowledge and methodologies shall **never require a license, degree, or permit**, recognizing its foundational role in civic literacy, informed public discourse, and democratic oversight, consistent with the universal right to seek, receive, and impart information.
3. Public domain information is the collective wealth of humanity and shall remain available to all without prerequisite, free from undue restrictions, censorship, or monopolization by any single entity, private or governmental, in furtherance of the right to information.

Article 4. Illegitimacy of Non-OSINT Espionage by Non-Governmental Actors

1. Any espionage practice not rooted in OSINT, including but not limited to unauthorized

infiltration of systems or organizations, malicious hacking, physical surveillance infringing on privacy rights without legal mandate, or coercive questioning, shall be deemed **unlawful, unethical, and illegitimate for all individuals and**

non-governmental actors. Such acts constitute arbitrary interference with privacy (as per UDHR Article 12 and ICCPR Article 17) and attacks upon honor and reputation.

2. Such practices, when undertaken by individuals or non-governmental entities, shall be condemned as grave violations of human rights, privacy, democratic principles, and moral integrity, infringing upon the sovereignty of states and the security of individuals, and shall be subject to stringent legal prosecution under national and international law, including cybercrime conventions.

Article 5. Government Use of Non-OSINT Espionage

1. Governments may, under **exceptional circumstances** involving imminent and verifiable threats to national security, public safety, or international peace, employ non-OSINT espionage. Such activities shall be strictly limited in scope, duration, and target, and solely conducted through agents acting under the direct, explicit, and strict supervision of duly elected and accountable officials.
2. All such activities shall be subject to:
 - a. Rigorous constitutional and legal frameworks that define, constrain, and regularly review such powers, ensuring that any interference is lawful, necessary, and proportionate to a legitimate aim, in accordance with international human rights law;
 - b. Robust, independent, and transparent oversight mechanisms, including mandatory judicial authorization for specific operations and comprehensive legislative review, ensuring genuine accountability to the public and effective remedies for abuses;
 - c. Strict ethical standards consistent with democratic values, fundamental human rights, international humanitarian law (where applicable), and human dignity, minimizing collateral impact and unequivocally prohibiting torture, cruel, inhuman, or degrading treatment, and undue interference in the lives of innocent individuals or populations.
3. The **burden of proof for the necessity, proportionality, and legality** of non-OSINT espionage shall always rest unequivocally with the government employing it, and this proof must be reviewable by independent oversight bodies.

Article 6. Public Oversight and Transparency

1. States shall establish and empower **independent, transparent oversight bodies**, directly accountable to elected legislatures and the judiciary, to comprehensively review and regulate any non-OSINT espionage activities. These bodies shall have the authority to investigate, audit, and publicly report on intelligence practices, subject only to necessary and narrowly defined protections for operational security that do not compromise the integrity of oversight, thereby upholding the right to an effective

remedy (UDHR Article 8, ICCPR Article 2(3)).

2. Citizens shall have the right to demand accountability regarding the scope, methods, and justifications of intelligence practices, and states shall ensure accessible, effective, and timely mechanisms for public redress in cases of abuse, unlawful intelligence activities, or violations of privacy.

Article 7. Universality and Non-Discrimination

This Declaration affirms that OSINT-based intelligence is a right, a practice, and a safeguard of democracy for all peoples, and shall serve as the lawful and primary basis for intelligence work in the modern age. The principles herein shall apply universally, without discrimination based on nationality, ethnicity, religion, gender, sexual orientation, disability, or any other status, in accordance with fundamental human rights principles.

Article 8. International Cooperation and Mutual Assistance

1. States shall promote and facilitate international cooperation in OSINT gathering, analysis, and sharing, recognizing that global challenges require collaborative intelligence efforts rooted in public information and shared understanding, consistent with the UN Charter's call for international cooperation.
2. States shall establish robust mechanisms for mutual legal assistance in investigating and prosecuting violations of this Declaration, particularly concerning unlawful non-OSINT espionage conducted by individuals or non-governmental actors across borders.
3. Any intelligence cooperation between states that involves non-OSINT methods must adhere strictly to the principles of democratic oversight, human rights, international law, and the rule of law as outlined in Article 5, ensuring that the standards of the most protective state apply, thereby preventing circumvention of human rights obligations.

Article 9. Protection of OSINT Practitioners and Information Integrity

1. Individuals and organizations conducting lawful OSINT shall be **protected from harassment, intimidation, arbitrary detention, or retribution** by state or non-state actors for their work in gathering, analyzing, and disseminating publicly available information, in furtherance of the right to freedom of expression and to seek and receive information (UDHR Article 19, ICCPR Article 19).
2. States shall take proactive and transparent measures to combat disinformation, misinformation, and propaganda that intentionally seek to corrupt or manipulate the public information domain, thereby undermining the integrity and utility of OSINT.

However, such measures must be carefully balanced to protect freedom of speech, journalistic inquiry, and legitimate public discourse.

3. The principles of journalistic freedom, academic independence, and protection for whistleblowers, as vital components of a healthy public information domain, are paramount and therefore essential for the effective, ethical, and unimpeded practice of OSINT.

Article 10. Accountability and Redress for Violations

1. Any individual, governmental agent, or non-governmental entity found to be in violation of this Declaration, particularly through the engagement in illegitimate non-OSINT espionage or abuse of authorized non-OSINT powers, shall be **held fully accountable under national and international law, without impunity**, consistent with the principle of rule of law.
2. Victims of unlawful espionage or intelligence abuses shall have the **right to effective remedies**, including prompt and adequate compensation, public apologies where appropriate, and guarantees of non-repetition. States shall establish accessible, independent, and impartial judicial or quasi-judicial mechanisms for seeking such redress, as mandated by international human rights law.

Article 11. Adaptability to Technological Advancement

1. Recognizing the rapid and continuous evolution of technology, states commit to regularly reviewing and updating their intelligence practices, legal frameworks, and oversight mechanisms to ensure ongoing adherence to the principles of this Declaration. This includes careful consideration of new methods of data collection, processing, analysis, and the deployment of artificial intelligence, ensuring these developments respect privacy and human rights.
2. Technological developments in intelligence shall be guided by robust ethical considerations, human rights principles, and a commitment to democratic values, ensuring that tools and methods enhance, rather than undermine, the primacy of OSINT and individual liberties. **Independent ethical and human rights impact reviews of new intelligence technologies shall be mandatory.**

Article 12. Role of the Private Sector in Intelligence

1. Private entities engaged in intelligence gathering or analysis, including security companies, data brokers, and technological developers, shall be subject to the same ethical standards and legal restrictions regarding non-OSINT espionage as individuals

and non-governmental actors, as outlined in Article 4, recognizing their responsibility to respect human rights in accordance with the UN Guiding Principles on Business and Human Rights.

2. Governments contracting with or utilizing the services of private intelligence entities shall ensure that these entities adhere strictly to the principles of this Declaration, particularly concerning the primacy of OSINT and the limitations on non-OSINT practices. Governments remain ultimately accountable for the actions of their private sector partners in intelligence activities, upholding their duty to protect human rights.
3. Transparency regarding government contracts with private intelligence entities shall be encouraged to foster public trust and enable oversight, while respecting legitimate commercial confidentiality and narrowly defined operational security needs.

Article 13. Promotion and Implementation of National Frameworks

1. States commit to adopting legislative, administrative, and other measures necessary to give full effect to the rights and principles recognized in this Declaration within their national legal frameworks and policies. This includes the development of national OSINT guidelines, ethical codes, training programs, and comprehensive data protection regimes.
2. International, regional, and national human rights institutions, civil society organizations, and academic bodies are encouraged to promote and monitor the implementation of this Declaration, drawing on and contributing to international best practices in OSINT.
3. This Declaration shall be disseminated as widely as possible and promoted through education and public awareness campaigns, to ensure its principles are understood and respected by all.

Article 14. Relationship to Other International Instruments

Nothing in this Declaration shall be interpreted as diminishing or contradicting the obligations of states under existing international human rights law, international humanitarian law, international criminal law, or other relevant international legal instruments, but rather as reinforcing and elaborating upon those obligations in the context of modern intelligence practices.

Conclusion

We, the signatories and adherents to this Universal Declaration, solemnly reaffirm our unwavering commitment to an intelligence paradigm that champions transparency, ethics, and the international rule of law. By upholding the primacy of Open-Source Intelligence, grounded

in respect for human rights and democratic values, we envision a future where the pursuit of knowledge serves to strengthen freedom, protect human dignity, and foster a more secure, just, and cooperative world. We call upon all states, international organizations, and individuals to embrace and integrate these principles as a cornerstone of responsible governance and global citizenship in the indispensable information age.

Signed,

Marie-Soleil Seshat Landry, a Queen of the Universe.

spymaster@marielandryspyshop.com

www.marielandryspyshop.com