

Universal Declaration of the Legality and Ethical Practice of Open Source Intelligence (OSINT)

Marie Seshat Landry

March 27, 2025

Preamble

Recognizing that the digital transformation of society has rendered vast quantities of information ubiquitously accessible through public and commercial channels; Acknowledging that intelligence derived exclusively from such publicly and commercially available sources—commonly known as Open Source Intelligence (OSINT)—constitutes an indispensable tool for understanding and navigating our complex world; Affirming the fundamental right of states, international organizations, intelligence professionals, law enforcement agencies, businesses, researchers, journalists, civil society organizations, and independent investigators to lawfully collect, analyze, process, and disseminate such information; Grounded in established principles of national and international law, including freedoms of speech, expression, and access to information [1], and cognizant of necessary limitations prescribed by law for the protection of rights such as privacy [2, 3]; Drawing upon existing legal frameworks and best practices demonstrated globally—from the constitutional protections in the United States [4] and Canada [5] to the comprehensive data protection regulations in the European Union [2] and the United Kingdom [6], and further informed by guidelines within national intelligence communities (e.g., the U.S. Intelligence Community OSINT Strategy 2024-2026 [7] and related directives like ICD 301 [8]); This declaration proclaims that OSINT, when conducted responsibly and ethically, is a lawful, legitimate, and essential activity for a wide array of stakeholders engaged in security, governance, commerce, research, and public interest activities. It distinguishes OSINT clearly from clandestine surveillance and intrusive data collection methods which operate under distinct and stricter legal regimes [9].

1 Article 1 – Definition and Scope of OSINT

1.1 1.1. Definition

Open Source Intelligence (OSINT) is defined as intelligence produced from data and information that is publicly available or commercially obtainable upon request or purchase, collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

1.2 1.2. Source Types

Publicly available information includes, but is not limited to:

1. Content from mass media (print newspapers, magazines, radio, television).
2. Information available via the public internet, including websites, blogs, discussion forums, social media platforms (public profiles and content), public government data portals, public

records (court filings, property records, corporate registrations), mapping and geographic data services.

3. Content accessible on the deep and dark web that does not require circumventing authentication, encryption, or access controls intended to protect privacy or confidentiality.
4. Commercially available information, including data brokerage services, commercial imagery (satellite, aerial), subscription databases, market research reports, and financial data feeds, obtainable legally through purchase or subscription.
5. Academic and grey literature, such as conference proceedings, pre-prints, theses, dissertations, reports by NGOs, industry journals, patents, and technical papers.
6. Observations of public places, events, or activities, including public speeches, debates, and legislative sessions.

1.3 1.3. Exclusions

OSINT, by definition, excludes intelligence derived from:

1. Clandestine surveillance or espionage involving non-public intrusions (e.g., illegal hacking, wiretapping, physical trespass).
2. Human Intelligence (HUMINT) obtained through clandestine recruitment or coercive means.
3. Signals Intelligence (SIGINT) involving the non-consensual interception of private communications.
4. Geospatial Intelligence (GEOINT) derived from classified satellite or aerial reconnaissance systems not available commercially or publicly.
5. Measurement and Signature Intelligence (MASINT) derived from specialized, often classified, technical sensors.

1.4 1.4. Nature of Activity

OSINT primarily involves the *discovery, collection, validation, analysis, synthesis, and dissemination* of information that any member of the public could theoretically access, locate, and observe, albeit potentially requiring specific skills, tools, or resources (including financial payment for commercially available data) [10].

2 Article 2 – Presumption of Legality and Foundational Principles

2.1 2.1. Fundamental Legality

The collection, analysis, processing, and utilization of information conforming to the definition of OSINT in Article 1 are hereby declared to be presumptively lawful activities under prevailing national and international legal norms. This legality is rooted in fundamental rights concerning freedom of expression, the right to seek, receive, and impart information [1, 11], and the general principle that information placed in the public domain or made commercially available without expectation of privacy is generally permissible to access and use.

2.2 2.2. Distinction from Regulated Surveillance

OSINT activities, focusing solely on publicly and commercially available information, are fundamentally distinct from activities like electronic surveillance, covert physical surveillance, com-

pelled disclosure of private data, or computer network intrusions, which are typically subject to specific and stringent legal authorization requirements (e.g., warrants, judicial oversight) precisely because they infringe upon reasonable expectations of privacy or involve unauthorized access [9, 12].

2.3 2.3. Legal Boundaries and Compliance

The presumption of legality is contingent upon OSINT activities being conducted in full compliance with all applicable laws within the relevant jurisdiction(s). This includes, but is not limited to:

1. **Data Protection and Privacy Laws:** Adherence to regulations governing the processing of personal data, such as the EU/UK General Data Protection Regulation (GDPR) [2, 6], the California Consumer Privacy Act (CCPA) [3], Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) [13], and similar statutes worldwide. This requires OSINT practitioners processing personal data to have a lawful basis, respect data subject rights (access, rectification, erasure), adhere to principles of purpose limitation, data minimization, and security, and conduct data protection impact assessments where appropriate.
2. **Copyright and Intellectual Property Laws:** Respecting limitations on the reproduction and use of copyrighted materials.
3. **Computer Fraud and Abuse Laws:** Abstaining from unauthorized access, scraping in violation of robust technical measures intended to prevent such access, or actions that intentionally damage or impair computer systems [12]. Note that the legal status of violating website Terms of Service during scraping remains subject to jurisdictional interpretation and debate [15].
4. **National Security Legislation:** Compliance with laws regarding the handling of classified information, export controls, or specific prohibitions on collecting certain types of data (even if publicly available) related to critical infrastructure or defense matters in some jurisdictions.
5. **Sector-Specific Regulations:** Adherence to rules governing data use in specific sectors like finance or healthcare, where applicable.

2.4 2.4. Basis in Public Nature

The legality fundamentally derives from the source of the information – its public or commercial availability – negating the requirement for intrusive methods that trigger higher legal thresholds for justification and authorization.

3 Article 3 – Scope and Recognized Applications

OSINT is recognized as a fundamental, lawful, and often indispensable tool across diverse domains:

3.1 3.1. National and International Security

Supporting intelligence analysis, threat assessments (terrorism, proliferation, cyber threats), geopolitical monitoring, sanctions enforcement, verification of arms control treaties, early warning systems, counter-intelligence, and informing diplomatic strategy [7, 10]. The NATO OSINT Handbook provides extensive context for its military and security applications [16].

3.2 3.2. Law Enforcement and Crime Prevention

Assisting in investigations (identifying suspects, witnesses, networks), tracking criminal activities (trafficking, financial crime, extremism), preventing crime through situational awareness, and supporting prosecution with publicly corroborated evidence.

3.3 3.3. Espionage and Statecraft

Providing foundational intelligence, contextual understanding for other intelligence disciplines (INTs), identifying potential targets or leads, supporting operational planning, and enabling state-level strategic decision-making [8]. OSINT offers a low-risk, high-yield initial layer for intelligence gathering.

3.4 3.4. Business and Competitive Intelligence

Facilitating market analysis, competitor tracking, supply chain risk management, cybersecurity threat intelligence, merger and acquisition due diligence, reputational risk assessment, financial market prediction, and identification of innovation trends.

3.5 3.5. Academic Research and Scientific Inquiry

Enabling research in social sciences, political science, international relations, conflict studies, public health, economics, and technology by providing access to vast datasets on human behavior, societal trends, global events, and scientific developments.

3.6 3.6. Journalism, Public Interest Investigations, and Transparency

Powering investigative journalism (e.g., Bellingcat's methodology [17]), monitoring human rights violations, tracking environmental changes, verifying claims made by state and non-state actors, promoting government accountability, monitoring elections, and combating disinformation and misinformation [18].

3.7 3.7. Emergency Management and Humanitarian Aid

Providing situational awareness during natural disasters or crises, mapping affected populations, identifying infrastructure damage, monitoring displacement, and coordinating relief efforts.

4 Article 4 – Ethical and Legal Obligations of Practitioners

4.1 4.1. Primacy of Law and Ethics

All individuals and organizations engaged in OSINT collection, analysis, processing, and dissemination (hereafter "practitioners") bear the responsibility to conduct their activities lawfully and ethically, demonstrating respect for human rights and fundamental freedoms.

4.2 4.2. Compliance Culture

Practitioners must foster a culture of compliance, ensuring awareness of and adherence to all relevant legal frameworks mentioned in Article 2.3, including international humanitarian law where applicable (e.g., concerning protected persons in conflict zones).

4.3 4.3. Data Protection by Design and Default

When processing personal data obtained through OSINT, practitioners must integrate data protection principles from the outset, including:

1. Lawfulness, Fairness, and Transparency: Processing data only when a lawful basis under relevant data protection law exists (e.g., legitimate interests, public task, consent where appropriate) and being transparent about processing activities where feasible and required.
2. Purpose Limitation: Collecting and processing personal data only for specified, explicit, and legitimate purposes.
3. Data Minimization: Collecting and retaining only the personal data that is adequate, relevant, and limited to what is necessary for the intended purpose.
4. Accuracy: Taking reasonable steps to ensure the accuracy of personal data and rectifying inaccuracies.
5. Storage Limitation: Retaining personal data in an identifiable form only for as long as necessary.
6. Integrity and Confidentiality: Implementing appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or destruction.
7. Accountability: Being able to demonstrate compliance with these principles [2, 6].

4.4 4.4. Ethical Considerations Beyond Law

Practitioners should adhere to recognized ethical principles, including:

1. Proportionality: Ensuring that OSINT activities, particularly those involving personal data, are proportionate to the legitimate aim pursued.
2. Avoidance of Harm: Taking reasonable steps to foresee and mitigate potential negative impacts of OSINT activities on individuals and groups, particularly vulnerable populations. This includes careful consideration before publishing sensitive personal information, even if publicly available.
3. Objectivity and Bias Mitigation: Striving for objective analysis, acknowledging potential biases in data sources and analytical methods (including algorithmic bias), and representing findings accurately.
4. Source Vetting and Information Validity: Employing critical evaluation techniques to assess the reliability and credibility of sources and information, cross-referencing where possible, and clearly indicating confidence levels.
5. Responsible Disclosure: Considering the potential consequences of disseminating OSINT findings and adopting responsible disclosure practices, particularly where findings could endanger individuals or compromise legitimate security interests.
6. Respect for Platform Terms of Service: While recognizing the evolving legal landscape [15], practitioners should be mindful of website/platform Terms of Service (ToS) and the potential legal and ethical implications of violating them, particularly concerning automated scraping methods.

4.5 4.5. Guidance Adherence

Practitioners, particularly within government and regulated industries, should adhere to relevant internal policies, codes of conduct, and professional standards, such as those developed by

intelligence oversight bodies [19] or professional associations.

5 Article 5 – Transparency, Oversight, and Accountability

5.1 5.1. Principle of Appropriate Transparency

While acknowledging that the specific nature and targets of some OSINT activities, particularly in national security and law enforcement, may require confidentiality, the overall practice of OSINT, especially by public bodies, should operate within a framework of appropriate transparency and accountability to maintain public trust.

5.2 5.2. Oversight Mechanisms

OSINT activities conducted by state actors should be subject to robust and independent oversight mechanisms (e.g., parliamentary committees, inspector generals, judicial review where applicable) commensurate with the potential impact on rights and freedoms. Oversight should verify legal compliance, ethical propriety, necessity, and proportionality [19].

5.3 5.3. Accountability Frameworks

Organizations conducting OSINT should implement internal accountability measures, including clear policies and procedures, training programs on legal and ethical obligations, mechanisms for recording significant OSINT activities (audit trails), and designated points of responsibility for compliance.

5.4 5.4. Redress Mechanisms

Where feasible and appropriate, individuals potentially affected by unlawful or unethical OSINT practices should have access to effective redress mechanisms.

5.5 5.5. Promoting Best Practices

Governments, industry bodies, academic institutions, and civil society organizations are encouraged to collaboratively develop and promote standardized best practices, ethical guidelines, and training curricula for OSINT practitioners to foster responsible conduct across the field [20].

6 Article 6 – International Cooperation and Harmonization

6.1 6.1. Need for Cooperation

Given the inherently transnational nature of publicly available information and the global scope of challenges addressed by OSINT (e.g., terrorism, cybercrime, disinformation), international cooperation among states and relevant organizations is essential.

6.2 6.2. Areas for Collaboration

Nations and international organizations are urged to cooperate in:

1. Harmonizing legal and ethical standards for OSINT to the extent possible, reducing legal fragmentation and promoting a common understanding of responsible practices.
2. Sharing best practices, methodologies, and training resources related to lawful and ethical OSINT collection and analysis.

3. Facilitating lawful cross-border sharing of OSINT relevant to shared security threats or public interest objectives, consistent with data protection laws and human rights obligations.
4. Establishing platforms for ongoing dialogue between governments, industry, academia, and civil society on emerging OSINT challenges and opportunities.
5. Collaborating on technical standards for data discovery, access, and exchange where appropriate.

6.3 6.3. Building Trust

Enhanced international cooperation based on shared adherence to legal and ethical principles will foster greater trust, improve collective security and understanding, and support a more resilient global information ecosystem.

7 Article 7 – Adaptability and Continuous Evolution

7.1 7.1. Dynamic Environment

The technological landscape, the nature of publicly available information, societal norms regarding privacy, and the legal/regulatory environment are constantly evolving. Artificial intelligence, machine learning, the Internet of Things (IoT), synthetic media (deepfakes), and new communication platforms continuously reshape the OSINT domain.

7.2 7.2. Living Document

This declaration is intended as a living document. The principles and articles herein should be subject to periodic review and potential amendment through multi-stakeholder consultations to ensure they remain relevant, effective, and responsive to emerging technologies, challenges (such as countering sophisticated disinformation or balancing AI-driven analysis with human rights), and evolving legal and ethical paradigms.

7.3 7.3. Anticipatory Governance

Stakeholders are encouraged to engage in ongoing dialogue and research to anticipate future developments and proactively address their implications for the legal and ethical practice of OSINT.

8 Article 8 – No Specific OSINT License Requirement

8.1 8.1. Reaffirmation

It is hereby declared that no special, government-issued, or privately mandated "OSINT license" or certification shall be required as a precondition for engaging in the fundamental activities of collecting, analyzing, or disseminating information falling under the definition of OSINT (Article 1).

8.2 8.2. Justification

OSINT fundamentally involves accessing information that is already available to the public or commercially obtainable through lawful means. Imposing a licensing requirement on the act of observing, researching, or analyzing such information would constitute an undue burden and potentially infringe upon fundamental rights to freedom of expression and access to information

[1, 11], akin to requiring a license to read newspapers, browse the public internet, or conduct library research.

8.3 8.3. Distinction from Regulated Professions

This principle does not preclude licensing requirements for specific professions that *utilize* OSINT as one tool among others (e.g., private investigators engaging in broader surveillance activities, lawyers advising clients, financial analysts providing investment advice), where licensing serves to regulate the *overall professional conduct* and protect the public from specific harms related to specialized services or fiduciary duties extending beyond the mere use of public information.

8.4 8.4. Regulation Through General Law

The legality and propriety of OSINT activities are adequately governed by existing general laws (data protection, privacy, copyright, computer fraud, national security) and the ethical obligations outlined in Article 4. Compliance with these established legal and ethical frameworks, rather than a bespoke OSINT license, constitutes the appropriate regulatory mechanism.

Conclusion

This Universal Declaration affirms the fundamental legality and indispensable nature of Open Source Intelligence when conducted within the bounds of established law and ethical principles. By defining OSINT, distinguishing it from intrusive surveillance, grounding its legality in fundamental rights while mandating compliance with existing legal obligations (especially concerning privacy and data protection), and explicitly rejecting the need for specific OSINT licensing, this Declaration aims to provide clarity and support for the responsible use of OSINT worldwide. It advocates for a future where OSINT is universally recognized as a legitimate tool, practiced ethically and transparently under robust oversight, contributing significantly to informed decision-making, enhanced security, commercial innovation, academic discovery, journalistic integrity, and the broader public interest in an increasingly complex and information-rich global environment.

References

- [1] Universal Declaration of Human Rights (UDHR), Article 19. UN General Assembly, 1948.
- [2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR).
- [3] California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act (CPRA).
- [4] First Amendment to the Constitution of the United States.
- [5] Canadian Charter of Rights and Freedoms, Section 2(b), Part I of the Constitution Act, 1982.
- [6] Data Protection Act 2018 (United Kingdom), implementing the UK GDPR.
- [7] Office of the Director of National Intelligence (ODNI). *U.S. Intelligence Community Open Source Intelligence Strategy 2024-2026*. Washington, D.C. (Refer to official publication if available).

- [8] Office of the Director of National Intelligence (ODNI). *Intelligence Community Directive (ICD) 301: National Open Source Enterprise*. (Refer to the current version).
- [9] European Convention on Human Rights (ECHR), Article 8 (Right to respect for private and family life). Council of Europe, 1950.
- [10] U.S. Department of Defense. *DoD Manual 3305.10: Open Source Intelligence (OSINT) Lifecycle*. (Refer to the current version).
- [11] International Covenant on Civil and Political Rights (ICCPR), Article 19. UN General Assembly, 1966.
- [12] Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. (United States).
- [13] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5. (Canada).
- [14] Convention on Cybercrime (Budapest Convention). CETS No.185. Council of Europe, 2001.
- [15] Reference to ongoing legal discussions, e.g., *LinkedIn Corp. v. hiQ Labs, Inc.*, 938 F.3d 985 (9th Cir. 2019) and subsequent related decisions or developments regarding CFAA and Terms of Service violations.
- [16] North Atlantic Treaty Organization (NATO). *NATO Open Source Intelligence Handbook* (or related doctrine like AJP-2.1, Intelligence Procedures). (Refer to latest unclassified versions if available).
- [17] Bellingcat. Methodology resources and publications available via their website. Represents investigative practice. (Example: <https://www.bellingcat.com/>)
- [18] Ethical Journalism Network (EJN). Guidelines and principles regarding ethical reporting. (Example: <https://ethicaljournalismnetwork.org/>) a
- [19] General principles derived from the mandates and reports of established intelligence oversight bodies, e.g., Inspector Generals within Intelligence Communities, Parliamentary oversight committees like the UK's Intelligence and Security Committee.
- [20] Concept reference to community-driven resources like the "OSINT Framework" (<https://osintframework.com/>) which aggregates tools and resources, indicative of practitioner community practices. This is distinct from a formal standards body.