

# OSINT Methodology & Ethics in Open-Source Intelligence

Authors: Dr. Maria Gonzalez · Dr. Michael Torres · Dr. Sarah L. Chen

Document ID: PLIANT-J-2025-11 | PLIANT Institute, Palo Alto CA | [projectpliant.com](http://projectpliant.com)

---

## Executive Summary

*This report examines the ethical dimensions of open-source intelligence collection and analysis in supply chain security contexts, with particular attention to the tensions between analytical utility and the rights of profiled entities. We propose a rigorous OSINT ethics framework grounded in principles of proportionality, transparency, and institutional accountability, and discuss its application to PLIANT's own research practices, including the Atlas Intelligence Database.*

---

## 1. The Ethics of OSINT at Scale

The rapid expansion of OSINT as an analytical discipline has outpaced the development of ethical frameworks adequate to govern it. The standard justification for OSINT — that publicly available information carries no reasonable expectation of privacy — is technically defensible but analytically insufficient. Aggregation of public information at scale produces insights that the subjects of analysis could not reasonably have anticipated when the underlying data was disclosed, and that carry meaningful potential for harm.

Supply chain security analysis presents a particularly acute version of this challenge. The commercial entities profiled in logistics intelligence databases are frequently unaware that detailed vulnerability assessments of their operations exist in institutional repositories accessible to government partners. This is not unusual in the OSINT research community — but it is ethically significant and warrants explicit institutional acknowledgment and governance.

## 2. Key Ethical Tensions

We identify three primary ethical tensions in OSINT-based supply chain analysis:

**Consent.** Commercial entities profiled in OSINT databases have not agreed to be subjects of analysis. The fact that underlying data is technically public does not resolve the ethical question of whether aggregation and analysis at scale constitutes a meaningful intrusion.

**Proportionality.** The analytical benefits of OSINT aggregation accrue primarily to the institutions conducting the analysis and their partners, while the risks — of misidentification, data breach, or reputational harm — are borne by the profiled entities.

**Asymmetric Distribution.** When OSINT is shared between private research institutions and government agencies, it flows through institutional channels that lack the transparency and accountability mechanisms that govern government intelligence collection directly.

## 3. Proposed Ethics Framework

PLIANT's OSINT ethics framework rests on four principles:

**Proportionality.** Collection and analysis should be proportionate to the security objective being pursued.

**Minimization.** Data collected should be limited to what is necessary for the stated analytical purpose, with defined retention periods.

**Accountability.** Institutions conducting OSINT analysis should maintain internal ethics review functions with genuine authority to constrain research practices.

**Transparency.** Where feasible, institutions should publicly disclose the categories of entities subject to OSINT analysis and the purposes for which analysis is conducted.

#### **4. Application to PLIANT Research Practices**

PLIANT has committed to implementing the proposed framework across its research operations over the coming year. Specific measures include the establishment of an independent OSINT Ethics Review Board, the development of Atlas data governance standards specifying retention periods and access controls, and the publication of an annual transparency report disclosing aggregate statistics on Atlas data collection and partner sharing activity.

**We recognize that the ethical frameworks governing private-public OSINT partnerships remain underdeveloped across the field and that PLIANT's own practices have not always met the standards we now propose. This report represents a commitment to higher standards, not a claim that those standards have already been met.**

#### **5. Conclusion**

The maturation of OSINT as a discipline requires a corresponding maturation of the ethical frameworks that govern it. The principles proposed here — proportionality, minimization, accountability, and transparency — provide a practical foundation for institutions operating at the intersection of open-source research and national security policy. PLIANT is committed to modeling the standards it advocates and welcomes engagement from peer institutions on the development of field-wide norms.