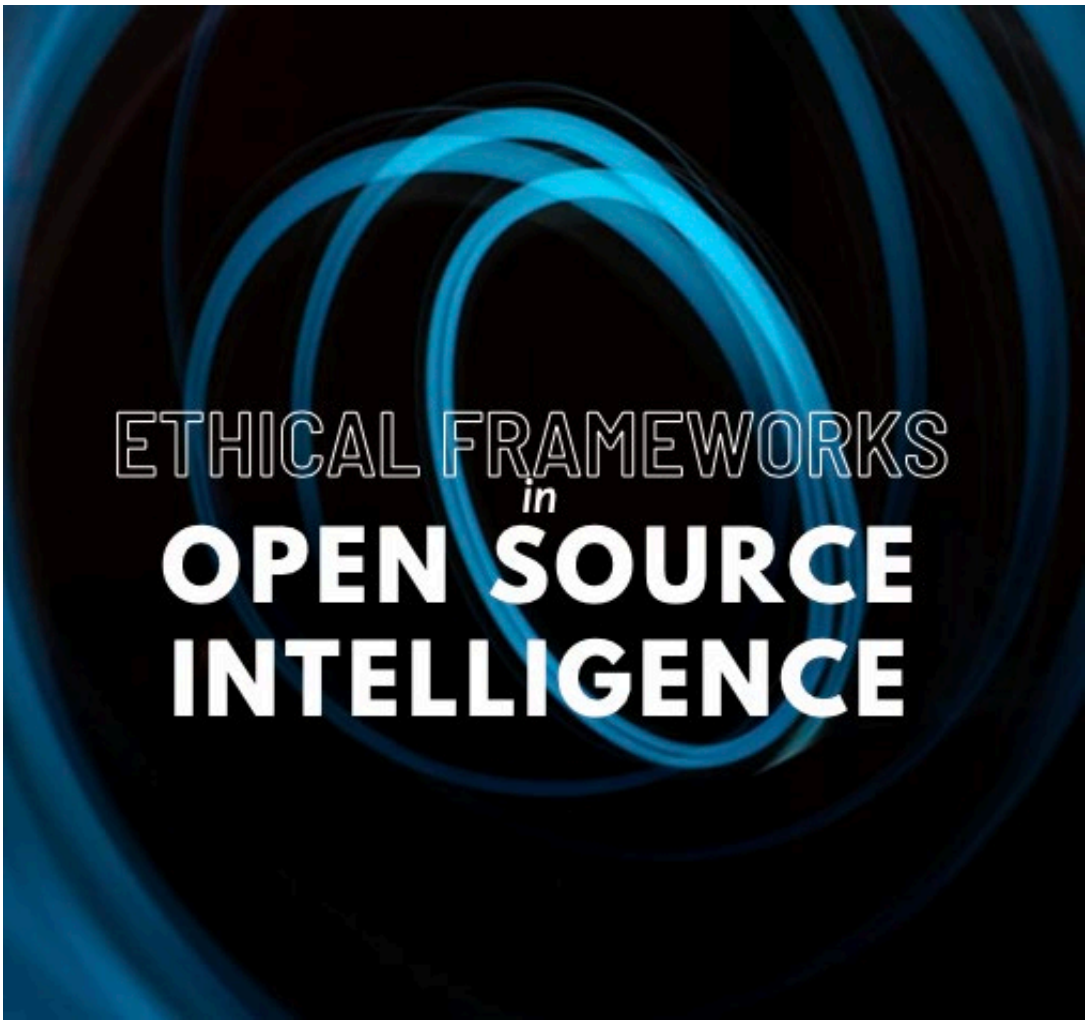
2022
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM



DISCLAIMER STATEMENT: *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.*

Member	Organization
Brittany Krilov	National Insurance Crime Bureau (NICB)
Ryan Gough	Secure Community Network
Patricia Kickland	Hawaii State Fusion Center
Melissa Pisaniello	New Jersey State Police
Katherine Wolfe	QVC
Danielle Fiumefreddo Waters	Bank of America
William Nasuti	
Chianna Mirtaheri	Snap Inc.
Rosangie (Angie) Paiz	The Walt Disney Company
Shani Spivak, champion	***FBI (Champion Agency)***

Table of Contents

Ethical Frameworks in Open-Source Intelligence

Introduction

Open-Source Intelligence is used today by a variety of experts in many different fields. The resulting findings that are gathered can provide critical information for investigations, intelligence and more. This paper focuses on the ethical guidelines that surround these Open-Source intelligence findings as well as the potential need there might be for the future.

Definition of Open-Source Intelligence

According to the U.S. government, open-source intelligence (OSINT) is defined as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[1] Some scholars have defined OSINT as "intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature."[2]

While interviewing OSINT experts, many agreed there is no clear definition of OSINT, but that it is important to define it in any framework involving OSINT research. For the purposes of this white paper, we will define OSINT as publicly available information and sources, including but not limited to, public data such as government reports, court cases and hearings, demographics, utilities records, etc.; professional and academic literature such as scholarly articles, conferences, professional associations, etc.; and any information obtained from the media such as the internet, news articles, television, podcasts, etc.

As per the case *U.S. v. Mereglido*, where the government stated that expectation of privacy "is not absolute" when referencing social media,[3] we will include social media in our definition of OSINT under information obtained from the media. We will define social media as websites and applications that enable users to create and share open-source content or participate in social commentary.

History of OSINT

The first use of OSINT predates August of 1939. The British government requested the British Broadcasting Corporation (BBC) launch a civilian OSINT service analyzing foreign print journalism and radio broadcasting. It produced a foreign broadcast compilation titled Digest of Foreign Broadcasts, renamed in May of 1947 to the Summary of World Broadcasts (SWB), now known as BBC Monitoring.

On February 26, 1941, U.S. President F.D. Roosevelt created the Foreign Broadcast Monitoring Service (FBMS) to translate and analyze propaganda messages against the United States and transmitted through shortwave radio broadcasts. The FBMS published its first transcription report on November 18, 1941, and its first analytical report, dated December 6, 1941. [7] There was a demand for services from the FBMS after the Japanese attack on Pearl Harbor. In 1947, FBMS was renamed the Foreign Broadcast Intelligence Service (FBIS) and placed under the Central Intelligence Agency.[7] From 1947-1948 the BBC and FMBS established an official partnership under the agreement on the full exchange of information. Also, in 1948, the research arm of the U.S. Library of Congress was based out of the Aeronautical Research Unit to provide customized research and analytical services using the vast holdings of the library. It is now known as the Federal Research Division (FRD). [4]

OSINT began as a tactic for military intelligence and has expanded to business, politics, and law enforcement intelligence. Large organizations are using OSINT strategically, and academics are researching techniques to work with OSINT. Law enforcement agencies use OSINT to anticipate national security threats such as international terrorism.[19] Although the chances are slim that a terrorist will post their selected target location online, these measures help monitor violent extremist views.[20] Following the September 11, 2001, terrorist attacks there was a realization that outdated need-to-know standards for information sharing constricted its flow during the Cold War and needed to change. There was a need for a formal information-sharing procedure, making information itself as shareable as possible.[8] As a result, the U.S. Patriot Act and Homeland Security Act were enacted. On October 26, 2001, The U.S. Patriot Act eliminated legal barriers to information sharing between law enforcement and intelligence agencies. It prevented the abuse of authority by providing a private offense cause of action against government officials who improperly reveal sensitive information.[9] The Patriot Act was intended to "deter and punish terrorist acts in the United States and worldwide" and "enhance law enforcement investigatory tools.'[10] The Homeland Security Act created the Department of Homeland Security (DHS) by combining 22 existing agencies and 170,000 federal employees into a new cabinet-level department.[11]

In December 2004, President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act into legislation addressing the issues of intelligence failure. The Intelligence Reform and Terrorism Prevention Act created a Director of National Intelligence (DNI) and ordered him or her and their Office

of the Director of National Intelligence (ODNI) to improve intelligence analysis in the wake of two major perceived U.S. intelligence failures: al-Qaeda's attacks of September 11, 2001, and the National Intelligence Estimate (NIE) on Iraqi weapons of mass destruction (WMD) of September 2002.[12] [4]

Changes in OSINT

Before the development of the Internet, OSINT was gathered from foreign print and broadcast media, radio, television, and other streams of electronically available products. The development of the Internet opened the door to multiple new streams of publicly available information to collect. Now, open sources of information consist of the following general categories:

- Traditional media sources (television, radio, newspapers, books, magazines)
- Commercial online premium sources
- Other niche commercial online sources [14]
- Gray literature (limited edition locally available information)
- Overt human experts
- Commercial imagery and geospatial information (maps and commercial imagery products)
- The Internet and the world wide web (forums, blogs, social networking sites, video-sharing sites like YouTube.com, wikis, WHOIS records of registered domain names, metadata, and digital files, dark web resources, geolocation data, I.P. addresses, people search engines and anything that can be found online) [15]
- Specialized journals, academic publications, dissertations, conference proceedings, company profiles, annual reports, company news, employee profiles, and resumes
- Photos and videos, including metadata

The Internet created the opportunity to gather information desired at faster speeds, whether the content was displayed in a foreign language or from another country. Receiving information today is within a click of a mouse.[16]

Open-source intelligence overlaps many information disciplines. Geospatial intelligence (GEOINT) can now be classified as OSINT due to commercial satellites that are now able to provide an overhead imagery capability on a par with the capacity historically provided only by classified collection platforms.[16] OSINT can also be classified as human intelligence (HUMINT). OSINT can also be classified as signals intelligence (SIGINT). Social media data collection (SOCMINT) provides insights and perspectives of an individual. Social media data collection may involve the electronic collection of many records that are sifted using technical means to identify interactions or communications of critical interest.[13]

With the growth of the Internet came social media and social networking, which is comprised of all the online forums that link internet users through retrievable listings or websites (Facebook, LinkedIn), blogs

(WordPress, BlogSpot), Twitter, Tumblr, Instagram, and video hosting (YouTube, daily motion), and collaborative or search tools.[17] Facebook and Twitter have collectively been the most used social media platforms. Social media and social networking have become the preferred communication outlet over email.

Uses of OSINT

Open-source intelligence is used today in a wide variety of fields for a variety of uses. Currently, both public and private sectors utilize OSINT for anything from researching a subject on Facebook to identifying war crimes across the globe.

Public Sectors- Government/LE

According to the Human Rights Center, "Digital open-source information has, however, been used in a largely ad hoc manner as human rights organizations, intergovernmental bodies, investigative mechanisms, and courts have at times struggled to adapt their working practices to include new digital methods of fact-finding and analysis."[21]

Federal government bodies utilize OSINT for a variety of purposes including tracking organized crime, national security concerns, counterterrorism, cybersecurity cyber-attacks, and domestic and foreign public views. Utilizing OSINT along with closed source intelligence allows agencies to collect detailed information for analysis.

Local law enforcement officers utilize OSINT as part of criminal investigations, identifying potential crimes, protecting citizens from sexual crimes, abuse, identity theft, fraud crimes, and more. Per Steve Adams at SkopeNow, "OSINT enables law enforcement agencies to piece together information from a wide range of sources, building a detailed picture of criminals, organized crime networks, trafficking, the illegal trade of goods, and much more."[22]

Meanwhile, the emergence of international criminal courts and investigative mechanisms, as well as national war crimes units, has further heightened the need for common standards for capturing, preserving, and analyzing open-source information that can be introduced as evidence in criminal trials.[23]

In recent news, OSINT has been used by government and law enforcement officials to learn about potential subjects in crimes such as the Boston marathon, the Capital attack, the war in the Ukraine and the Highland Park shooting. Officials can see recent photos, locations, videos, occupations, political affiliations and more. This intelligence has provided insight into criminals' lives and ideas that may have led to those different crimes.

Private Sectors

Private sectors use OSINT for reasons such as business intelligence, marketing, journalism, medical and insurance fraud, and even auto thefts. Some private sectors also assist law enforcement in investigations and can utilize open-source information to help in their research on a particular subject, person, or incident. Griffin Glynn, the founder of Hatless Investigations uses OSINT for a variety of reasons. He currently uses OSINT to assist other companies and task forces in their investigations.

"OSINT solutions are also useful in procurement, particularly with corruption investigations, compliance and due diligence checkups, and social media monitoring of key people and organizations."[24]

Joseph Stephenson is currently the Director of Digital Intelligence for Intertel. He uses OSINT for products they currently have and will soon have in the market. They utilize OSINT to see if a patient received injury prior to a workers' compensation claim and utilize social media to see where clients might have been at the time of a reported automobile theft.

Ethical Challenges in OSINT

The word ethics is defined as "a set of moral principles: a theory or system of moral values."[25] However, applying this definition is far more complicated as moral principles and values can vary across time, geographical spaces, and applications.[26] As it relates to social media, ethics must be considered as they apply to legal rights, expectations of privacy, and benefits to society.

Currently, there are not nationally or internationally accepted guidelines for how social media intelligence is collected, analyzed, and obtained.[27] Applicable legislation and generally accepted ethical use of social media intelligence takes vastly different forms in the public sector compared to the private sector.

After speaking to multiple experts in the field of social media intelligence, it has become clear that the ethical boundaries defining this relatively new source of information are constantly changing and evolving. However, one consistent defining ethical boundary across sectors is the idea that intelligence gathered from open sources, such as social media must be done in a way that does not violate existing privacy laws, must not be used in a malicious manner, and must be done only when necessary.

Current Ethical Frameworks for OSINT

Though used as a current OSINT framework, legal statutes are not the same as ethical frameworks as the law is reflective of the rules and regulations set by the current authoritative body, while ethics are the accepted moral values and principles adopted by one's society. Based on current findings from academic publishing and subject matter experts (SME), there remains a limited understanding of universally

accepted ethical frameworks used by both the public and private sectors. From the perspective of the public sector, federal and/or state law governs how OSINT frameworks are applied for government entities. These statutes vary from how information is collected to what information is legally protected from public agencies from collecting. Additional obstacles are created when it comes to the classification of the intelligence report and the appropriate audience who may access this information. Though also bound to legal implementations, private sector entities experience less restrictive statutes when collecting and developing intelligence through OSINT. However, how OSINT is collected and shared varies widely between private organizations. Despite the overall inconsistency of how ethics are implemented in OSINT, the private and public sectors may find common ground through the application of their organization's mission statement, as a means of providing employees with an ethical foundation to guide their practices.

According to American author John C. Maxwell, a mission statement should complement an organization's code of ethics and inspire employees to work toward a common goal or make decisions that are in line with the organization's values. In theory, both private and public sectors' framework for security practices, such as the practice of OSINT, should align or be rooted within the organization's code of ethics and mission. However, not all mission statements keep security considerations in mind. As the organization's goal remains the focal point for all operations, OSINT frameworks that provide a constructed set of ethical implementations might not be considered by key decision-makers. Without a standard policy or framework in place specific to security practices, intelligence analysts and investigators may unknowingly pursue unethical routes to propel their organization's mission or goal.

The Fourth Amendment

The Fourth amendment to the Constitution gives people the right to protection against unreasonable searches and seizures. It states that it is "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[28]

As with defining the word and applications of "ethics", this amendment has long been the subject of various interpretations and legal challenges to what constitutes a "reasonable" search or seizure. In general, it is understood that a "reasonable" search or seizure is one in which law enforcement agents have probable cause to search or seize a person, place, or thing. However, it should be noted that the right to privacy is not specifically mentioned or protected by an amendment in the constitution.

There have been four landmark cases decided upon by the US Supreme Court regarding the Fourth amendment.[28]

- Weeks v. United States, 1914: this case established that in order for a search by law enforcement to be legal, probable cause must be established and used to gain a search warrant.
- New Jersey v. T.L.O., 1985: this case determined that the right to privacy in a school was limited in the extent to which safety and security were maintained. The court determined that privacy had to be weighed with the concern for safety of others within the school.
- Vernonia School District v. Acton, 1995: this case reinforced the New Jersey V. T.L.O. decision by stating that drug testing policies in schools were within the school's right to perform to ensure the safety of students.
- Safford Unified School District v. Redding, 2009: this case determined that strip searches of a student at school was illegal, and the privacy of the student outweighed the need to search the student in this case.

Jurisdictional Differences

Legal frameworks for OSINT and social media may vary depending on jurisdiction. For example, unlike the U.S. Constitution, multiple state constitutions have provisions explicitly referring to privacy.[30] Some states, such as California, have stand-alone privacy provisions.[31] Other states, such as South Carolina, explicitly mention privacy within provisions that are otherwise similar to the Fourth Amendment to the U.S. Constitution.[32] Some states, like Hawai'i, do both.[33]

Recently, some states have been amending their constitutions to explicitly include electronic data and communications. These amendments are located within the search and seizure provisions of the state constitutions. Missouri was the first state to include electronic communications or data in its constitution.[34] Michigan followed suit in 2020.[35] A similar amendment will be on the ballot for Montana voters during the November 8, 2022 elections.[36] The Michigan and Missouri provisions specifically govern "access" to electronic data and communications.

- Michigan (Section 11): The person, houses, papers, possessions, electronic data, and electronic communications of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things or to access electronic data or electronic communications shall issue without describing them, nor without probable cause, supported by oath or affirmation. The provisions of this section shall not be construed to bar from evidence in any criminal proceeding any narcotic drug, firearm, bomb, explosive or any other dangerous weapon, seized by a peace officer outside the curtilage of any dwelling house in this state.
- Missouri (I Section 15): Unreasonable search and seizure prohibited — contents and basis of warrants. — That the people shall be secure in their persons, papers, homes, effects, and electronic communications and data, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, or access electronic data or communication, shall

issue without describing the place to be searched, or the person or thing to be seized, or the data or communication to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation.

Conclusion

While the roots of OSINT date back to the late 1930s, the mediums through which open-source intelligence is gathered has vastly changed over time as technology has evolved. At its core, the goal of OSINT has remained the same – to collect information, analyze it, and turn it into useable intelligence. However, the birth of the digital age has raised a new grey area in terms of what can be ethically obtained from the numerous sources of OSINT. Across various interviews and in-depth research, it became clear that while there is no one set of rules defines ethics in OSINT, the federal and state government has established laws that help to guide the research. Different agencies and companies all work under different sets of guidelines defined by their governing organizations. While these rules may differ in wording and nuances, it is generally accepted that information gained from OSINT must be obtained in a way that does not violate existing privacy laws, must not be used in a malicious manner, and must be done only as a necessary means to an end.

Acknowledgements

The AEP "Ethical Frameworks in Open-Source Intelligence" Team gratefully acknowledges the following individuals for providing their time and expertise in the course of our research:

- Steve Beltz, Director of Learning & Development, National Insurance Crime Bureau (NICB)
- Joseph Stephenson, Director of Digital Intelligence, Intertel
- Griffin Glynn, President, and Founder of Hatless Investigations Group

References

1 Website; Public Law 109-163, National Defense Authorization Act for Fiscal Year 2006, Sec. 931, Department of Defense Strategy for Open-Source Intelligence, January 6, 2006. https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-subchapI-sec403-5.htm#:~:text=%E2%80%9C(1)%20Open%2Dsource,addressing%20a%20specific%20intelligence%20requirement.

2 Website; Rajamäki, J., Sarlio-Siintola, S., and Simola, J., 'The Ethics of Open-Source Intelligence Applied by Maritime law Enforcement Authorities', Laurea, 2018, https://www.theseus.fi/bitstream/handle/10024/152174/Rajamaki_Sarlio-Siintola_Simola.pdf;jsessionid=9EE1A1113A8E9E4901E322736B4255EA?sequence=1

3 Website; U.S. v. Mereglido, 2012 WL 3264501, 2012, https://www.boscolegal.org/resources/social-media-case-law/#62bf2142ae526

4 Schaurer, F. and Störger, J., 'Guide to the Study of Intelligence. The Evolution of the Open Source Intelligence (OSINT)', The Intelligencer,2011, https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

5 Princeton Listening Center, 'Finding Aid' , *Center for Study of Intelligence,* 2010 https://books.google.com/books?id=nmm02WSOKgEC&pg=PA36&lpg=PA36&dq=Princeton+Listening+Center,+Online+Records,+1939%E2%80%931941,+%E2%80%9CFinding+Aid,%E2%80%9D&source=bl&ots=jslCeLf3wo&sig=ACfU3U27UvaiGjfMRgH7AK9TeJ-cOaRebQ&hl=en&sa=X&ved=2ahUKEwi7tsW3yb_5AhWLnWoFHcJcCcEQ6AF6BAgCEAM#v=onepage&q&f=false

6 Roop, J., 'Foreign Broadcast Information Service, History, Part I: 1941–1947', *Central Intelligence Agency*, 1969 https://apps.dtic.mil/sti/pdfs/ADA510770.pdf (declassified, 2009); Rotheray, B., 'New Risks of Crisis-Fresh Perspectives from Open Source', *BBC*, 2001, https://www.yumpu.com/en/document/read/37068591/open-source-intelligence-the-challenge-for-nato-ossnet

7 Leetaru,K., 'The Scope of FBIS and BBC Open-Source Media Coverage, 1979– 2008 (U)', *CIA*, 2010, https://www.cia.gov/static/e4cd771e0aecd4492cd7e1be1e43fd76/The-Scope-of-FBIS.pdf

8 Jones, C., 'Intelligence Reform: The Logic of Information Sharing', Research Gate, 2007, https://www.researchgate.net/profile/Calvert-Jones/publication/232833253_Intelligence_reform_The_logic_of_information_sharing/links/5b997664458515310583e40a/Intelligence-reform-The-logic-of-information-sharing.pdf

9. McCarthy, M., 'USA Patriot Act, 39 HARV. J. oN Legis', 435 (2002).

10 Shaw, L., 'The USA Patriot Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, and the False Dichotomy between Protecting National Security and Preserving Grand Jury Secrecy', *Seton Hall Law Review*, vol. 35, no. 2, 2005, p.495-576. HeinOnline.

11 Brook, D., and King, C., 'Civil Service Reform as National Security', Public Administration Review 67 '(3): 397-405, 2007

12. Gentry, J., 'Has the ODNI Improved U.S. Intelligence Analysis? International Journal of Intelligence and CounterIntelligence', 28:4, 637-661, DOI: 10.1080/08850607.2015.1050937, 2015

13 Tomislav, I., 'Open Source Intelligence (OSINT): Issues and Trends', *Research Gate*, 2019, https://www.researchgate.net/profile/Tomislav-Ivanjko

2/publication/340301223_Open_Source_Intelligence_OSINT_issues_and_trends/links/5ecb93f2a6fdcc90d6971499/Open-Source-Intelligence-OSINT-issues-and-trends.pdf
14 Steele, R,, 'Open Source Intelligence', in Loch K. Johnson (ed.), *Handbook of Intelligence Studies*, (London: Routledge, 2009), pp. 129–47.
15 Hassan, N., and Hijazi, R.. 'Open Source Intelligence Methods and Tools', *Apress Media LLC*. ISBN-13 (pbk): 978-1-4842-3212-5 ISBN-13 (electronic): 978-1-4842-3213-2. 15-18, 2018.
16 Williams, H. and Blum, I., 'Defining second generation open-source intelligence (OSINT) for the defense enterprise', *RAND Corp.,* Santa Monica, CA, USA, Tech. Rep. RR-1964-OSD, 2018, doi: 10.7249/RR1964.
17 Ansari F, Akhlaq M, Rauf A (2013) Social networks and web security: Implications on open-source intelligence. In Information Assurance (NCIA), 2013 2nd National Conference on IEEE pp: 79-82.
18 NATO, Open-Source Intelligence Handbook, 2001
https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook
19 Gonçalves, J., et. al, 'Systematic Literature Review to Investigate the Application of Open-Source Intelligence (OSINT) with Artificial Intelligence', *Journal of Applied Security Research* (2020), 1–25
20 Eijkman, Q., and Weggemans, D., 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?', *Security & Human Rights,* 23(4), 285-296, 2013
21 Human Rights Center, Berkley Protocol on Digital Open Source Investigations', *UN Human Rights Center*, New York and Geneva, United Nations Publications, 2022, https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf
22 Adams, Steve, 'OSINT for Law Enforcement', *Skopenow*, https://www.skopenow.com/news/osint-for-law-enforcement
23 Human Rights Center, 'Berkley Protocol on Digital Open-Source Investigations', *UN Human Rights Center*, New York and Geneva, United Nations Publications, 2022, https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf
24 Popel, John, 'OSINT: The New Big Thing in B2B Business', *Forbes*,
https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/01/26/osint-the-new-big-thing-in-b2b-business/?sh=1bce26eb7b7e
25 "ethic." Merriam-Webster.com. 2022. https://www.merriam-webster.com/dictionary/ethic
26 Velasquez, M., Andre, C., Shanks, T., Meyer, M., 'What is Ethics', *Markkula Center for Applied Ethics*,
https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/what-is-ethics/
27 Tropotei, T., and Deac, I., 'Social Media in Intelligence Analysis', *Strategic Impact*, vol. 2019, no. 72+73, 2019, pp. 69–78.,
https://doi.org/https://media.proquest.com/media/hms/PFT/1/povxD?_s=DKE3txRWMdnTChspZiqhw3j5Ly8%3D
28 US Constitution of the United States, 'Fourth Amendment', *Congress,*
https://constitution.congress.gov/constitution/amendment-4/
29 Judicial Learning Center, 'Your 4th Amendment Rights', *Judicial Learning Center,* 2019
https://judiciallearningcenter.org/your-4th-amendment-rights/
30 National Conference of State Legislatures, 'Privacy Protections in State Constitutions, *National Conference of State Legislatures,* 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx
31 California Legislative Information, 'Article I declaration of Rights{Section 1- Sec 32],
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=SECTION%201.&article=I
32 California Legislative Information, 'Article I Declaration of Rights', *California Legislative Information*,
https://www.scstatehouse.gov/scconstitution/A01.pdf

33 Hawaii State Legislature, 'State Constitution', *Legislative Reference Bureau*, 2022, https://lrb.hawaii.gov/constitution#articlei

34 Revisor of Missouri, 'I Section 15. Unreasonable search and seizure prohibited', *Revisor of Missouri,* 2014, https://revisor.mo.gov/main/OneSection.aspx?section=I++++15&bid=31715&constit=y

35 Michigan Legislature, 'Constitution of Michigan of 1963', *Michigan Legislature*, http://www.legislature.mi.gov/(S(w2irceen3gq5lc5vaoucqfik))/mileg.aspx?page=getObject&objectName=mcl-Article-I-11

36Ballotpedia, 'Montana C-48, Search Warrant for Electronic Data Amendment (2022)', Ballotpedia, https://ballotpedia.org/Montana_C-48,_Search_Warrant_for_Electronic_Data_Amendment_(2022)