Balancing national security and privacy: examining the use of commercially available information in OSINT practices

Oerlemans, J.; Langenhuijzen, S.

International Journal of Intelligence and CounterIntelligence

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/ujic20

Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices

Jan-Jaap Oerlemans & Sander Langenhuijzen

To cite this article: Jan-Jaap Oerlemans & Sander Langenhuijzen (2025) Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices, International Journal of Intelligence and CounterIntelligence, 38:2, 579-597, DOI: 10.1080/08850607.2024.2387850

To link to this article: https://doi.org/10.1080/08850607.2024.2387850

Published online: 12 Sep 2024.

International Journal of Intelligence and CounterIntelligence, 38: 579–597, 2025
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2024.2387850

Routledge
Taylor & Francis Group

JAN-JAAP OERLEMANS AND
SANDER LANGENHUIJZEN

Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices

Jan-Jaap Oerlemans is an Endowed Professor of Intelligence and Law at the Willem Pompe Institute for Criminal Law and Criminology, Utrecht University. He is also an Assistant Professor of Criminal Law at the Institute for Criminal Law & Criminology at Leiden University. Until 2024, he was a Senior Researcher at the Dutch Review Committee on the Intelligence and Security Services. The author can be contacted at j.j.oerlemans@uu.nl.

Sander Langenhuijzen is a Legal Advisor at the Netherlands Ministry of Defence. Until 2024, he was a Researcher at the Dutch Review Committee on the Intelligence and Security Services. The author can be contacted at sjw.langenhuijzen@mindef.nl.

The views expressed in this article are those of the authors and do not necessarily reflect the views of Government of the Netherlands.

Abstract: Open source intelligence (OSINT) researchers utilize specialized tools to access vast amounts of data from multiple sources simultaneously. These tools, equipped with (paid) modules, allow users to tap into aggregated data sets containing commercially available information, such as location data from mobile phone users. The utilization of commercially available information from OSINT tools by intelligence and security services impacts fundamental rights and freedoms; more specifically, the right to personal data protection. Drawing from prior experience working on this topic within a Dutch oversight committee on the intelligence and security services and international developments in OSINT practice, insights are provided on this new OSINT practice and the responses of oversight authorities. Rather than advocating for a categorical ban, a more refined approach to process commercially available information from OSINT tools is suggested. Building on the work of a Dutch oversight authority and the work of the U.S. Office of the Director of National Intelligence, four recommendations are provided to intelligence and security services to responsibly handle commercially available information in OSINT practices.

In today's digital age, open source intelligence (OSINT) is a vital tool to collect information concerning national security threats. For example, video footage laid bare evidence for the usage of chemical weapons in Syria by the al-Assad regime.[1] And battlefield movements of Russian troops were tracked through social media posts[2] and commercial satellite imagery[3] following the invasion of Ukraine. At the same time, OSINT is seen as a threat to national security. For example, the Chinese government reportedly used stolen data to expose American intelligence operatives in Africa and Europe,[4] and a leak from a food delivery app disclosed personal data from presumedly Russian intelligence personnel.[5] Advertising technology, too, can expose intelligence and security personnel and political leaders to blackmail and hacking, thereby undermining the security of their organizations and institutions.[6]

The utilization of commercially available information from OSINT tools by intelligence and security services is critically examined, considering its impact on the right to personal data protection. The analysis builds on prior work of a Dutch oversight committee on the intelligence and security services and the U.S. Office of the Director of National Intelligence. This analysis is limited to the use of commercially available data in the context of OSINT tools. The use of commercially available data in other contexts, such as in cybersecurity or the financial sector, may warrant further research.[7]

First, international developments in OSINT practice are examined, specifically concerning the collection and processing of commercially available information. Second, the impact of this OSINT practice on fundamental rights

and freedoms is analyzed, specifically in light of the right to privacy and data protection. Finally, an evaluation and regulatory suggestions for this emerging OSINT practice are provided, in order to establish a legal framework for intelligence and security services to responsibly handle commercially available information in OSINT practices.

OSINT AND COMMERCIALLY AVAILABLE INFORMATION

What Is OSINT?

OSINT can be defined as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[8] Some key ways in which OSINT is utilized are early warning, intelligence gathering, counterterrorism, geospatial analysis, (counter)influence operations, and cybersecurity.

OSINT encompasses data from social media, websites, news articles, blogs, and public records. In the current age, however, it can also include leaked data and commercially available location data. OSINT practitioners employ various tools and techniques, including web scraping, data mining, social network analysis, and geospatial mapping, to collect and analyze information.[9]

The question often arises whether the collection and processing of commercially available information can still be viewed as "publicly available information" and an OSINT practice. In 2020, U.S. attorney general procedures stated that "information is publicly available only if it is [...] generally available to the public" and "commercial acquisitions of data may be so tailored and specialized for government use, and unavailable to a similarly situated private-sector purchaser, that the data cannot be considered publicly available."[10] In contrast, the Europol regulation explicitly states that "Europol may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers."[11]

Ultimately, what definition is used for OSINT and commercially available information is irrelevant. Modern OSINT and the acquisition and subsequent processing of commercially available information are inextricably linked. This OSINT practice warrants public attention from a legal point of view, because it significantly interferes with the right to privacy and may lead to data protection risks.

OSINT Tools

Gathering information through OSINT goes back to as early as halfway the nineteenth century in the United States and early twentieth century in Europe.[12] In recent years, a significant development took place with the

creation and utilization of specialist (commercial) tools for OSINT. These tools aid intelligence services in consulting various open sources, including social media, such as Facebook and X (previously Twitter). Examples of these OSINT tools are SpiderFoot, Recon-ng, Maltego, and Shodan.[13]

Tools for OSINT offer two major advantages over standard open source investigations using a web browser. The first is ease of use; a single search using an automated OSINT tool can query hundreds of sources simultaneously. The tool can then provide a visual representation of the results.[14]

The second major advantage to the services of using such tools is that they give access to data sources provided by the tool's vendor on a commercial basis. These tools enable their users to use paid modules, or "plug-ins," to access more data, including aggregated data sets. Vendors can aggregate these data sets as a single searchable source (a "composite data set"), which in some instances may contain billions of data points.[15]

The revenue model of these companies specializing in OSINT tools is based on offering these paid modules.[16] The Dutch Review Committee on Intelligence and Security Services refers to this automated processing of data and use of these tools as "automated OSINT."[17] The report of the oversight body shows how OSINT tools and the use commercially available information are inextricably linked.

Commercially Available Information and National Security

Commercially available information within the context of OSINT refers to data sets offered by companies, often through paid modules in their OSINT tools. These data sets sometimes contain data "scraped" from the internet, meaning the data are automatically collected from publicly accessible sources based on prefixed parameters.[18]

Next to scraped historical data, such data sets could include information about cryptocurrency transactions, leaked data sets, and advertisement data. Advertisement data can also include location data. Information about users generated by the providers of apps or websites (e.g., via cookies or adverts) are often sold to or exchanged with other parties. These data—also called advertisement intelligence—can end up in a commercial data set, which may be searched through a web browser or using a tool for automated OSINT.[19] The commercial parties selling (aggregated) data sets to their customers often use data brokers to acquire the data. Data brokers, a multibillion-dollar market,[20] collect and store billions of data elements covering nearly every consumer.[21] Examples of major data brokers are Accenture, LexisNexis, and Oracle (Datalogix).[22]

Most of the clients of these "data brokers" are marketing firms, hedge funds, real estate companies, and other data brokers. But a handful of companies sell information to law enforcement agencies and intelligence

agencies.[23] Examples of service providers offering commercially available information are Venntel, Anomaly Six, and Babel Street.[24] The "Electronic Frontier Foundation" visualized the practice of the use of commercially available information by governmental organizations in the infographic shown in Figure 1.

OSINT and Commercially Available Information to Protect National Security

Intelligence and security services can use OSINT tools and commercially available information to *protect* national security. Intelligence and security services collect this information about targets that may threaten national security. These targets are, for example, jihadists or right-wing extremists that may be involved in planning a terrorist attack. Other targets could be individuals from other intelligence and security services (foreign intelligence officers). Personal data about these targets will be acquired and processed for (counter)espionage purposes. The significance of OSINT for the intelligence domain also becomes clear in the United States' first OSINT Strategy, aptly titled "The INT of First Resort: Unlocking the Value of OSINT" (released in March 2024).[25]

OSINT tools can be used to quickly collect personal information about individuals on a variety of online sources, such as websites indexed by an array of search engines, social media services, and publicly available information on internet forums. Many individuals also inadvertently post identifying information, including location data, on social media services, which may then be used by intelligence and security services.[26] For example, Pastor-Galindo et al. show that ISIS fighters in Syria and Iraq have been tracked down through geotagged photos they unintentionally posted on Instagram or Twitter.[27] This type of information can also end up as commercially available information in advertising data.[28]

OSINT and Commercially Available Information as a Threat to National Security

Commercially available information can, however, also pose a *threat* to national security due to its potential for exploitation by adversaries. This view is particularly prevalent in the United States. Adversaries, too, collect information about their own targets and foreign troop movements.[29] For example, it has been reported that China maintains a large system to gather data on social media users, from platforms such as TikTok, X, and Facebook.[30]

Following news reports that previously focused on U.S. governmental authorities making use of commercially available information,[31] it seems that the political debate in the United States shifted from a privacy concern to a

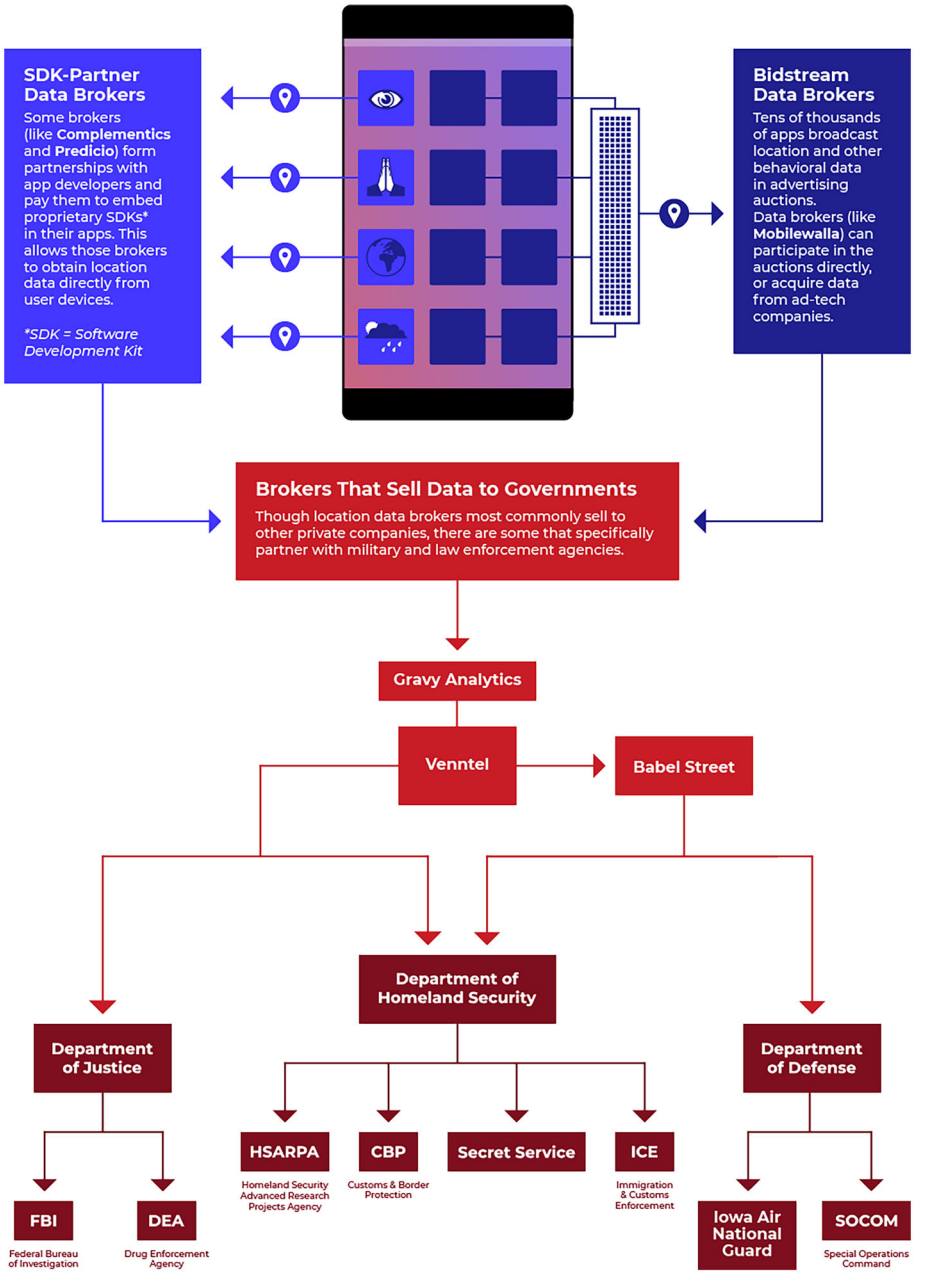

Figure 1. Brokers that sell data to governments. Electronic Frontier Foundation, "How the Federal Government Buys Our Cell Phone Location Data" (13 June 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

national security concern.[32] This resulted in a presidential Executive Order, issued on 28 February 2024, in order to protect Americans' sensitive personal data from exploitation by "countries of concern."[33]

The order builds on previous measures, and empowers the attorney general and secretary of homeland security to regulate data transfers and propose security measures. This includes prohibiting or restricting large-scale data transfers and implementing safeguards against activities that could give foreign entities access to sensitive data. While an important step to countering risks involving the data brokers industry, this executive order is no panacea. Time will tell which legislation is ultimately adopted to regulate data brokering in the United States.

THE RIGHT TO PRIVACY, OSINT, AND COMMERCIALLY AVAILABLE INFORMATION

In order to identify how the use of OSINT tools and commercially available data by intelligence and security services should be regulated, this intelligence method is tested in light of the right to privacy in Article 8 of the European Convention on Human Rights (ECHR).[34]

Commercially Available Information and the Right to Privacy

Within the intelligence domain, OSINT is frequently described as "the source of first resort."[35] Intelligence and law enforcement agencies often use terms such as "open source" and "publicly available information" to gather information with few or no legal requirements. However, it is essential to consider that information labeled as "open source" or "publicly available" may not, in reality, be readily accessible to the public. The use of modern OSINT techniques raises concerns regarding privacy, civil liberties, and the potential for abuse.

From a European legal point of view, it is clear that collecting and processing data with OSINT tools interfere with the right to privacy as protected in Article 8 of the ECHR.[36] The European Court of Human Rights (ECtHR) made clear in case law that storing and processing personal data by intelligence and security services and law enforcement authorities interferes with the right to private life as protected in Article 8 of the ECHR.[37] As a consequence, this privacy interference can only be justified when certain criteria are met. These will be explained in the next section.

Criteria to Justify an Interference to the Right to Privacy

Art. 8(2) of the ECHR states that such a privacy interference is legitimate when the following three conditions are met: (1) a legitimate aim is available,

(2) the interference is "in accordance with the law," and (3) the interference is "necessary in a democratic society."

A legitimate aim to collect and process the data is the protection of national security. In practice, states rarely encounter problems in arguing and demonstrating that a "legitimate aim is pursued" when intelligence methods are used that interfere with the right to privacy to protect national security.

States must then argue the use of the intelligence method is "in accordance with the law." The ECtHR uses a broad interpretation of the term "law." According to the ECtHR, the law concerns both (1) written law, including published guidelines for the application of investigative methods, and (2) unwritten law, such as settled case law.[38] In its case law, the ECtHR has stipulated that the regulation of investigative methods must fulfill the following three requirements in order to be considered "in accordance with the law": (1) accessibility, (2) foreseeability, and (3) a certain quality of the law.[39] Accessible law means that the statutory law, case law, or guidelines must be publicly available. Secret guidelines are thus not considered as accessible law.[40] The foreseeability requirement stipulates that both (a) the scope of the power conferred on the competent authorities and (b) the manner in which the intelligence method is exercised must be clear to the individuals involved. In other words, the national law must be clear, foreseeable, and adequately accessible.

Intelligence methods cannot be regulated "in terms of an unfettered power" that is conferred on law enforcement authorities.[41] The ECtHR can require a "certain quality of the law," relating to (1) the level of detail of the regulations and (2) the minimum procedural safeguards that must be implemented in the domestic legal frameworks of contracting states to the ECHR. These detailed regulations and procedural safeguards in domestic law aim to counterbalance the risk of abuse of power by the government.[42] What level of detail in regulations and minimum procedural safeguards the ECtHR requires will depend on the intensity of the investigation and interference with the right to privacy.[43] The ECtHR typically takes into account the circumstances of the case, such as the nature, scope, and duration of the possible measures; the grounds required for ordering them; the authorities competent to authorize, carry out, and supervise them; and the kind of remedy provided by the national law.[44]

Privacy Interference in the Current OSINT Practice

There is no case law available in relation to the collection and processing of publicly available information and commercially available information in an OSINT practice. Therefore, it is unknown what level of detail in regulations and procedural safeguards the ECtHR will require in this context. Moreover, the practices around OSINT are differently regulated around law

enforcement authorities and intelligence and security services.[45] Nevertheless, the criteria for privacy interferences and their mechanisms remain the same. Therefore, these criteria are used to identify how OSINT tools and the collection of commercially available information can be regulated.

In general, statutory law or guidelines should make clear whether intelligence and security services can make use of OSINT tools and commercially available information for their tasks. This will fulfill the criteria of "accessible and foreseeable law." The "quality of the law" and required procedural safeguards are more difficult to determine. States could think of the requirement of authorization by an independent authority or judge to acquire commercially available information as a procedural safeguard. The necessity to collect the data, proportionality and subsidiarity, must be justified in a written document, which will then be assessed by an independent authority. This may reduce the risk abuse of this type of data by intelligence and security services. In addition, data protection principles must be applied when processing personal information in order to protect the right to privacy of the individuals involved.

When OSINT tools are used and commercially available information is collected and processed, the privacy interference is significant and may require additional regulations and procedural safeguards. The following factors may be helpful in determining the gravity of the privacy interference and need for additional safeguards. These factors are (a) the type of data, (b) the scale of the data collected and subsequently stored, and (c) its subsequent analysis.[46]

For example, the interference with the right to privacy is minimal when data is copied from news articles and the publicly accessible parts of social media services. The interference with the right to privacy can be significant when location data and leaked data sets are processed.[47] It is clear, including from European case law on the processing of location data by the intelligence and security services, that the processing of location data seriously interferes with the right to protection of personal data and privacy.[48] Location data allow determination of the profile and routine of life, the place where one stays and for how long one stays in a given place.[49] Location data can also be sensitive when combined with other data, such as the type of app from which they are collected. For example, media reports suggest that third parties or data brokers harvested data from popular apps, such as Muslim Pro and Muslim Mingle, which were sold to both commercial parties and government agencies, including the U.S. military.[50]

There is no case law available on the gravity of the privacy interference when leaked data sets are collected and processed by intelligence and security services or law enforcement services. However, the scale of the data sets can be significant and the collection and making nonpublic data available and

trading stolen data are criminalized in many states, including the Netherlands. This is indicative for how this type of information is viewed in light of the right to privacy.[51]

The subsequent analysis of the collected data is also a factor in determining the gravity of the interference with the right to privacy and need for additional safeguards. In case law relating to bulk interception, the ECtHR also made clear it finds the privacy interference most significant in the analysis phase.[52] It is clear that—at a minimum—data protection principles should be applied as safeguards.[53] This means that a necessity and proportionality test should be conducted when storing personal data in a file about a target, the data should be adequately protected, and the data should be retained for a limited duration.[54] Note that these safeguards can only be effective when they are applied in practice and can be scrutinized (ex post) by an independent and effective authority.

USE AND RESTRICTIONS OF COMMERCIALLY AVAILABLE INFORMATION IN PRACTICE

In order to illustrate further the use and restrictions of OSINT tools and commercially available information by intelligence and security services in practice, this section analyzes a report of the Dutch Review Committee on the Intelligence and Security Services and a report of the U.S. Office of the Director of National Intelligence (ODNI).

Dutch Report on "Automated OSINT"

In September 2022, the Dutch Review Committee on the Intelligence and Security Services published their report, titled "Automated OSINT," about the use of OSINT tools and commercially available information in English.[55]

The Dutch Review Committee on the Intelligence and Security Services found that both intelligence and security services in the Netherlands utilized OSINT tools and commercially available information. The General Intelligence and Security Service only incidentally made use of these OSINT tools, in order to collect information about targets that threaten the national security of the Netherlands. The Military Intelligence and Security Service made frequent use of OSINT tools and commercially available information. The tools for automated OSINT were deployed by a specialist department of the Military Intelligence and Security Service and its use is a standard component of the intelligence process of the employees specialized in OSINT.[56]

In the Dutch legal framework, OSINT can be carried out based on a general legal basis for intelligence and security services to collect intelligence for the protection of national security. In case a "more or less complete view"

of certain aspects of an individual's private life will be obtained, a special investigatory power must be used for the systematic collection of personal data from publicly accessible information sources.[57]

In addition, the data processing using tools for automated OSINT by the services must comply with the general provisions regarding data processing within the Dutch Intelligence and Security Services Act. These include a necessity and proportionality test to process data, and a test of reliability of the data. The Dutch Review Committee found it especially important this test is conducted *before* such an OSINT tool is deployed and the services gain insight into how the tool functions, with what underlying data sources. Prior knowledge of the working (functionalities) and underlying sources of the tools is necessary to be able to conduct the proportionality assessment.

In short, the Dutch Review Committee found that the Dutch intelligence and security services checked which operational value these OSINT tools had and, in doing so, assessed the requirements of purpose and necessity. However, they failed to examine adequately the impact on the fundamental rights of the data subjects. A "data protection impact assessment" will aid in identifying compliancy risks and should lead to measures to respect these data protection regulations. The assessment may lead to a decision of intelligence and security services not to use certain functionalities of OSINT tools or not to copy certain results presented by these tools. In addition, the intelligence and security services could restrict the use of OSINT tools and commercially available information to certain (trained) employees, which can in turn rely on clear policies, procedures, and work instructions for their work.[58]

U.S. Report on Commercially Available Information (CAI)

On 27 January 2022, the ODNI published a report regarding the Intelligence Community (IC)'s handling of CAI.[59] In its report, a Senior Advisory Group Panel found that commercially available information is both a powerful tool for intelligence and sensitive for individual privacy and civil liberties. They are not in favor of a categorical ban on using commercially available information. However, considering the "privacy and civil liberties concerns and possible legislation restricting access to CAI," "the intelligence community should develop a thoughtful and balanced approach in this area."[60]

In short, the panel came to similar recommendations as the Dutch oversight body, stating that the IC must first understand how it processes commercially available information before it can make improvements.[61] This is very similar to a data protection impact assessment. One can only assess and mitigate risks when you "know your data."

Most notably, the panel recommends the IC should first develop a multilayered process to catalog commercially available information with attention to procurement contracts, data flows, and data use. Second, based on the knowledge gained from that process, the IC should develop a set of standards and procedures for commercially available information. To set up these standards and procedures, the following are necessary: (1) to identify the need/value for the mission analysis (a necessity test); (2) explain how they propose to use it; (3) analyze the vendor and data quality; (4) apply and evaluate acquisition mechanics; (5) attention to data security; (6) a legal review; (7) auditing the use of commercially available information; and (8) periodic reevaluation.[62]

The panel also provides helpful suggestions as safeguards when processing commercially available information. These are: (1) data minimization approaches and techniques, including ability to acquire commercially available information via access to data at the vendor rather than ingestion of data in bulk; (2) limits on retention, access, querying, other use, and the dissemination of commercially available information; and (3) possible requirements for special training of relevant personnel and auditing of queries and other uses of commercially available information.[63]

In May 2024, the U.S. IC followed up on these recommendations of the panel with the release of the "Policy Framework for Commercially Available Information." This framework encompasses many aspects mentioned above. It first establishes "general principles governing the access to and collection and processing of all CAI," for example, to determine the method(s) through which the CAI was generated and aggregated, and to assess the integrity and quality of CAI they access or collect. Second, it lays out a framework to govern the access to and collection and processing of certain sensitive forms of CAI.

CAI is considered "sensitive" if it is both purchased or made available by a commercial entity, and—briefly put—includes a "substantial volume" of personally identifiable information from U.S. persons, or a "greater than de minimis volume" of sensitive data (e.g., political opinion and sexual orientation), or capturing sensitive activities ("activities that over an extended period of time establish a pattern of life"). For these sensitive forms of CAI, enhanced safeguards are introduced. These can include applying privacy-enhancing techniques, such as filtering or anonymizing data, or implementing procedures to restrict access to the data. The framework also commits to provide a report to the public every two years regarding the access to and collection, processing, and safeguarding of sensitive CAI.

In short, the measures in the framework contribute to responsible intelligence gathering. The framework, however, also grants agencies significant discretion to determine whether such information is sensitive and merits enhanced safeguards.[64]

CONCLUSION

OSINT goes further than gathering articles on news websites or publicly accessible data on social media services. OSINT tools enable intelligence and security services to query hundreds of sources simultaneously and provide a visual representation of the results. In addition, OSINT tools can provide access to commercially available information. These data sets are in turn provided by (largely unregulated) data brokers and made available to law enforcement authorities and intelligence and security services.

News reports, a report of the Dutch Review Committee on Intelligence and Security Services, and a report and framework of the ODNI, show intelligence and security services make use of OSINT tools and commercially available information in practice. In the United States, news reports led to a public debate on how commercially available information poses a threat to privacy, but it is, on a political level, mainly perceived as a threat to national security.

The aim was to clarify how intelligence professionals can legitimately use commercially available information to protect national security and provide practical suggestions to intelligence and security services to handle the information responsibly. Therefore, legal requirements derived from the right to privacy were identified and two reports about the processing of commercially available information by intelligence and security services were analyzed. This analysis leads to the conclusion that states need to balance national security and privacy and take the following four steps to responsibly collect and process commercially available information:

1. Prior to using OSINT tools or acquiring commercially available information, intelligence and security services must be aware: (a) *how* data are processed, (b) *what* data are processed, and (c) *why* the data are processed, in order to identify risks of abuse of these data. In other words, intelligence and security services should first assess their impact in a data protection impact assessment and take measures to mitigate risks.
2. The IC should set up standards and procedures and implement safeguards, such as identifying the need for and value of the use of these data (while balancing this with the impact on fundamental rights), analyze the vendor and data quality, apply acquisition mechanics (such as procurement procedures), and periodically evaluate these standards. Then, intelligence and security services should implement safeguards when processing commercially available information, such as data minimization approaches and techniques, as well as limits on retention, access, querying, other use, and the dissemination of commercially available information.
3. OSINT practitioners must be appropriately educated and brought up to speed with the "do's and don'ts" with OSINT tools. Intelligence and security

services should periodically evaluate their policy and guidelines and review their practices.
4. An independent and effective oversight authority should scrutinize whether legislation and internal policies are respected.

These steps will help to ensure the safeguards are implemented to prevent the abuse of personal information in modern OSINT practices.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

REFERENCES

[1] Amnesty International, "How Open Source Evidence Took a Lead Role in the Response to the Douma Chemical Weapons Attack," 23 April 2023, https://www.amnesty.org/en/latest/news/2018/04/how-open-source-evidence-took-a-lead-role-in-the-response-to-the-douma-chemical-weapons-attack/
[2] Jack Hewson, "A Private Company Is Using Social Media to Track Down Russian Soldiers," *Foreign Policy,* 2 March 2023, https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/
[3] Doina Chiacu, "Russian Convoy of Ground Forces, Tanks Moving toward Kyiv, Maxar Says," *Reuters,* 27 February 2022, https://www.reuters.com/world/europe/russian-convoy-ground-forces-fuel-tanks-moving-toward-kyiv-maxar-2022-02-27/
[4] Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," *Foreign Policy,* 21 December 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/
[5] Aric Toler, "Food Delivery Leak Unmasks Russian Security Agents," *Bellingcat*, 1 April 2022, https://www.bellingcat.com/news/rest-of-world/2022/04/01/food-delivery-leak-unmasks-russian-security-agents/
[6] Johnny Ryan and Wolfie Christl, "Europe's Hidden Security Crisis: How Data about European Defence Personnel and Political Leaders Flows to Foreign States and Non-State Actors" (Irish Council for Civil Liberties, 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf
[7] See, for example, J. D. Work, "Evaluating Commercial Cyber Intelligence Activity," *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 2 (2020), pp. 278–308.
[8] U.S. Office of the Director of National Intelligence, "U.S. National Intelligence, An Overview 2011," https://www.govinfo.gov/content/pkg/GOVPUB-PREX28-PURL-gpo19700/pdf/GOVPUB-PREX28-PURL-gpo19700.pdf
[9] See, for example, Heather J. Williams and Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise" (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf
[10] U.S. Office of the Director of National Intelligence, "Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive

Order 12333," https://www.intelligence.gov/assets/documents/702%20Documents/declassified/AGGs/ODNI%20guidelines%20as%20approved%20by%20AG%2012.23.20_OCR.pdf

[11] See Article 25(4) of the Council decision of 6 April 2009 establishing the Europol Police Office (2009/371/JHA), Official Journal of European Union L 121/37.

[12] Ludo Block, "The Long History of OSINT," *Journal of Intelligence History*, Vol. 23, No. 2 (2023), pp. 95–109.

[13] Javier Pastor-Galindo, Pantaleone Nespoli, Felix Gómez Mármol, and Gregorio Martínez Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," *IEEE Access*, Vol. 8 (2020), pp. 10282–10304.

[14] See, for example, Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, 16 November 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," *New York Times*, 22 January 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html

[15] Dutch Review Committee on Intelligence and Security Services, "Automated OSINT: Tools and Sources for Open Source Investigation" (Report No. 74, 2022), https://english.ctivd.nl/binaries/ctivd-eng/documenten/review-reports/2022/09/19/index/CTIVD+NR74+Toezichtsrapport+ENG.pdf, p. 3.

[16] A critique of broker fees can be found in Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 2 (2007), pp. 240–257.

[17] Dutch Review Committee on Intelligence and Security Services, "Automated OSINT," p. 3.

[18] The collection of internet data and relationship with OSINT was acknowledged as early as 1995 (see Scientific & Technical Intelligence Committee Open Source Subcommittee records, October 1991–1995 (Freedom of Information Act document, released 8 February 2022), https://www.cia.gov/readingroom/document/06798974) See Robert David Steele, "The Open Source Program: Missing in Action," *International Journal of Intelligence and CounterIntelligence*, Vol. 21, No. 3 (2008), pp. 609–619 for a critique of these "Internet scraping" activities.

[19] Paul Vines, Franziska Roesner, and Tadayoshi Kohno, "Exploring ADINT: Using Ad Targeting for Surveillance on a Budget -or- How Alice Can Buy Ads to Track Bob," In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society, ACM* (2017), 153–164. See also, Dutch Review Committee on Intelligence and Security Services, "Automated OSINT."

[20] Transparency Market Research, "Data Brokers Market," 2022, https://www.transparencymarketresearch.com/data-brokers-market.html

[21] U.S. Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)," https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014, p. 43.

[22] U.S. Office of the Director of National Intelligence, "ODNI Senior Advisory Group Panel Declassified Report on Commercially Available Information" (January 2022, declassified June 2023), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

[23] Thorsten Wetzling, and Charlotte Dietrich, "Disproportionate Use of Commercially and Publicly Available Data: Europe's Next Frontier of Intelligence Reform?" (Stiftung Neue Verantwortung, 2022), https://www.stiftung-nv.de/sites/default/files/snv_commercially_available_data.pdf.pdf

[24] Bennett Cyphers, "How the Federal Government Buys Our Cell Phone Location Data," Electronic Frontier Foundation, 13 June 2022, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

[25] U.S. Office of the Director of National Intelligence, "The IC OSINT Strategy 2024–2026" (March 2024), https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

[26] Vines et al., "Exploring ADINT," pp. 153–164.

[27] Pastor-Galindo et al., "The Not Yet Exploited Goldmine of OSINT," p. 31.

[28] For example, Ryan and Christl refer to a category of data listed as "Government—Intelligence and Counterterrorism" offered by data brokers, with data "observed from social sharing, search page visits and click-backs on shared pages." Ryan and Christl, "Europe's Hidden Security Crisis," pp. 11–12.

[29] See, for example, Byron Tau, "The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots," *Wall Street Journal*, 26 April 2021, https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402; Michael Kans, "Data Brokers and National Security," *Lawfare*, 29 April 2021, https://www.lawfaremedia.org/article/data-brokers-and-national-security

[30] Cate Cadell, "China Harvests Masses of Data on Western Targets, Documents Show," *Washington Post*, 31 December 2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html; Brian Fung, "Lawmakers Say TikTok Is a National Security Threat, but Evidence Remains Unclear," *CNN*, 21 March 2023, https://edition.cnn.com/2023/03/21/tech/tiktok-national-security-concerns/index.html

[31] See, for example, Cox, "How the U.S. Military Buys Location Data from Ordinary Apps"; Tau, "The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots"; Thomas Claburn, "Federal Agencies Buying Americans' Internet Data Challenged by US Senators," *The Register*, 22 September 2022, https://www.theregister.com/2022/09/22/federal_agencies_american_data/

[32] Justin Sherman, "The Open Data Market and Risks to National Security," *Lawfare*, 3 February 2022, https://www.lawfaremedia.org/article/open-data-market-and-risks-national-security; Thomas Claburn, "You Can Buy Personal Info of US Military Staff from Data Brokers for Just 12 Cents a Pop," *The Register*, 7 November 2023, https://www.theregister.com/2023/11/07/data_brokers_military_data/

[33] "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," Executive Order

14117 of 28 February 2024, U.S. Federal Register, https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related

[34] The ECHR is selected as a treaty to analyze the privacy interference. The Charter of Fundamental Rights of the European Union may also be relevant, especially because it explicitly protects the right to data protection in Article 8. However, the European Union has left national security as "the sole responsibility of each Member State" (Article 4(2) of the Treaty on European Union) and there is little case law available from the Court of Justice of the European Union (CJEU) and applicable to the national security domain, with a notable exception of CJEU 6 October 2020, C-511/18, C-512 and C520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net and Others*).

[35] "Forward," *Open Source Intelligence: Professional Handbook* (Washington, DC: Joint Military Intelligence Training Center, 1996). See also the previously mentioned first U.S. OSINT Strategy, "The INT of First Resort: Unlocking the Value of OSINT," U.S. Office of the Director of National Intelligence, "The IC OSINT Strategy 2024–2026" (March 2024), https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

[36] See, with regard to the law enforcement domain: Bert-Jaap Koops, "Police Investigations in Internet Open Sources: Procedural-Law Issues," *Computer Law & Security Review*, Vol. 29, No. 6 (2013), pp. 654–665; Jan-Jaap Oerlemans, "Investigating Cybercrime" (PhD dissertation) (Leiden: Amsterdam University Press 2017), pp. 95–102. The outcome of this legal analysis will not be different in a national security context.

[37] See, for example, ECtHR 4 May 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, § 43 (*Rotaru v. Romania*) and ECtHR 6 June 2006, appl. no. 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200, § 72 (*Segerstedt-Wiberg and others v. Sweden*).

[38] See, for example, ECtHR 24 April 1990, appl. no. 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185, §28 (*Kruslin v. France*) and app. no 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584, § 28–29 (*Huvig v. France*) and ECtHR 2 August 1984, appl. no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, §66 (*Malone v. The United Kingdom*).

[39] ECHR, "Guide on Article 8 of the European Convention on Human Rights Right to Respect for Private and Family Life, Home and Correspondence," https://www.echr.coe.int/documents/d/echr/guide_art_8_eng. It should be noted that in some cases, the ECtHR only tests the foreseeability of the law, which is then considered as part of the required quality of the law. See, for example, ECtHR 2 September 2010, appl. no. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, § 60 (*Uzun v. Germany*).

[40] See, for example, ECtHR 23 September 1998, appl. no. 27273/95, ECLI:CE:ECHR:1998:0923JUD002727395, § 37–38 (*Petra v. Romania*).

[41] See, for example, ECtHR 2 August 1984, appl. no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, §66–68 (*Malone v. The United Kingdom*) and ECtHR 4 May 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, § 55 (*Rotaru v. Romania*).

[42] See, for example, ECtHR 1 July 2008, appl. no. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300, § 62 (*Liberty and Others v. The United Kingdom*).
[43] Oerlemans, "Investigating Cybercrime," pp. 79–80.
[44] See, for example, ECtHR 5 December 2015, appl. no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, § 232 (*Roman Zakharov v. Russia*).
[45] Ainara Bordes Perez, "Open Source Intelligence: An Overview of Today's Operational Challenges and Human Rights Affected as a Consequence," *Romanian Intelligence Studies Review*, Vol. 2, No. 30 (2023), pp. 5–33.
[46] See, similarly, *Commissie modernisering opsporingsonderzoek in het digitale tijdperk, "Regulering van opsporingsbevoegdheden in een digitale omgeving"* [Committee on Modernizing Criminal Investigations in the Digital Age, "Regulation of Investigative Powers in a Digital Environment"], s.l. (2018), https://hdl.handle.net/1887/68377, pp. 163–164.
[47] Dutch Review Committee on Intelligence and Security Services, "Automated OSINT," p. 20.
[48] See, for example, ECtHR 8 February 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD00314412 (*Ben Faiza/France*). See also CJEU 6 October 2020, C-511/18 and C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net e.a./Premier ministre and others*) and CJEU 21 December 2016, C-203/15 and C-698/15, ECLI:EU:C:2016:572 and ECLI:EU:C:2016:970, § 99 (*Tele2 Sverige AB and Watson*).
[49] Dominika Czerniak, "Collection of Location Data in Criminal Proceedings—European (the EU and Strasbourg) Standards," *Revista Brasileira de Direito Processual Penal*, Vol. 7 (2021), p. 123.
[50] Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps."
[51] See also Wetzling and Dietrich, "Disproportionate Use of Commercially and Publicly Available Data."
[52] ECtHR 25 May 2021, appl. nos. 58170/13, 62322/14, and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, § 330 (*Big Brother Watch and Others v. The United Kingdom*).
[53] See also Wetzling and Dietrich, "Disproportionate Use of Commercially and Publicly Available Data."
[54] See, for example, ECtHR 25 May 2021, appl. nos. 58170/13, 62322/14, and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, § 335 and 339 (*Big Brother Watch and Others v. The United Kingdom*). See also Dominika Czerniak, "Collection of Location Data in Criminal Proceedings," p. 123.
[55] The original report in Dutch was published in February 2022.
[56] Dutch Review Committee on Intelligence and Security Services, "Automated OSINT," pp. 17–18.
[57] Section 38 of the Dutch Act on Intelligence and Security Services 2017.
[58] Dutch Review Committee on Intelligence and Security Services, "Automated OSINT," pp. 19–21.
[59] U.S. Office of the Director of National Intelligence, "ODNI Senior Advisory Group Panel Declassified Report on Commercially Available Information"

(January 2022, declassified June 2023), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

60 Ibid., p. 13.

61 Ibid., p. 2.

62 Ibid., p. 2.

63 Ibid., p. 28.

64 U.S. Office of the Director of National Intelligence, "Intelligence Community Policy Framework for Commercially Available Information" (May 2024), https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf

ORCID

Jan-Jaap Oerlemans http://orcid.org/0000-0002-7854-8047