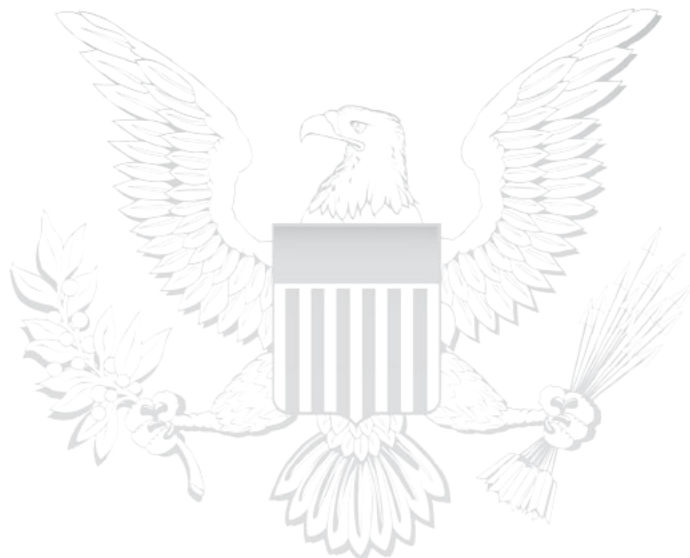




Office of the Director of National Intelligence

(U) 2026 Commercially Available Information Biannual Report

September 2026



Classified By:
Derived From:
Declassify On:



(U) Commercially Available Information

(U) Commercially Available Information (CAI) provides foundational and enduring insight to every Intelligence Community (IC) collection discipline, enabling IC personnel to better position collection capabilities to acquire important information, analyze foreign threats to the United States, plan and carry out operations, and provide decision advantage for policymakers, warfighters, and partners. From commercial satellite imagery and analytics to cybersecurity, counterterrorism, and many other missions, CAI informs almost every facet of the IC's work.

(U) **Background:** In May 2024, the IC publicly released, on DNI.gov, the IC's Policy Framework for CAI (hereinafter the CAI Framework). The CAI Framework provided the following background information:

(U) [C]ommercial entities are collecting and aggregating unprecedented amounts of personal data through networked computing applications. This data comes from a variety of sources including cell phones, cars, household appliances, and other personal devices. Some of these commercial entities make such information available to a diverse set of purchasers, including for-profit and non-profit entities, foreign adversaries, and domestic and transnational organizations.

(U) Like these other purchasers, elements of the IC lawfully access, collect, and process such CAI in pursuit of mission imperatives, and the information often provides critical intelligence value.

(U) At the same time, these datasets can reveal sensitive and intimate personal details and activities. The IC's access to and collection and processing of this information is subject to numerous laws and policies governing intelligence activities, which include those found in the Constitution; statutes such as the Federal Information Security Modernization Act and the Privacy Act of 1974; Executive Order 12333; IC element procedures approved by the Attorney General for the protection of U.S. persons' information pursuant to Section 2.3 of Executive Order 12333 ("Attorney General Guidelines"); and other relevant policies and procedures, such as those promulgated by the Office of Management and Budget. Dedicated IC officials, including privacy and civil liberties, oversight, compliance, and legal officers, provide counsel and monitor compliance with these laws and policies.

(U) The CAI Framework established principles governing the IC's access, collection, and processing of CAI, including certain Sensitive Commercially Available Information (SCAI) (discussed in the section below).

(U) **Scope:** Subsequently, in December 2024, the Director of National Intelligence (DNI) issued the IC Policy Memorandum (ICPM) 504 (01), *Intelligence Community Policy Framework for CAI* (hereafter "CAI ICPM"), which was publicly released on 17 December 2024 on dni.gov. The CAI ICPM established a policy that governs the IC's access, collection, and processing of CAI and defined CAI as:

[REDACTED]

(U) [A]ny data or other information that is of a type customarily made available or obtainable and sold, leased, or licensed to members of the general public or to non-governmental entities for purposes other than governmental purposes. CAI also includes data and information for exclusive government use knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity or on their own initiative.

(U) [But] CAI does not include data and information: obtained by the government pursuant to legal process; voluntarily provided to law enforcement by a corporate entity where such disclosures are made pursuant to a specific statutory scheme [...]; or obtained from activities undertaken through human sources or through human-enabled means.

(U) **Transparency:** Among other things, the CAI ICPM directed certain transparency actions. Specifically, the CAI ICPM directed the ODNI, with the support of the IC elements, to:

- (U) [r]eport annually to Congress on the IC's access to and collection, processing, and safeguarding of [SCAI]; and
- (U) [p]rovide a report to the public every two years [beginning in 2026] on the IC's access to and collection, processing, and safeguarding of [SCAI].

(U) Reflecting the President's commitment to transparency, in September 2025, the DNI submitted the inaugural annual classified report to Congress. The report, *Use of Sensitive Commercially Available Information in the Intelligence Community*, summarized the IC's handling of SCAI from May 2024–May 2025, incorporating input on SCAI safeguards from all 18 IC elements and aligning with new policy and reporting requirements.

(U) To meet the second transparency requirement, the DNI is reporting information and certain statistics related to CAI for the first time in this report.

(U) Sensitive Commercially Available Information

(U) **SCAI Scope:** SCAI is a subset of CAI and it is used by the IC for identifying and analyzing foreign threats and for security- and personnel-related functions including consent-based Continuous Evaluation (CE) of the IC workforce. Per the CAI ICPM, SCAI is defined as [the part of the CAI that is] known or reasonably expected to contain a substantial volume of Personally Identifiable Information (PII) about U.S. persons (USP) or a greater than de minimis volume of data that captures sensitive activities or attributes. Specifically, the CAI ICPM directs that CAI should be considered SCAI if it meets the following criteria:

- (a) (U) The CAI is purchased from a commercial entity through a commercial transaction for a fee or made available by the commercial entity at no cost through a commercial transaction that normally would involve a fee (e.g., a free trial offering of CAI); and

[REDACTED]

(b) (U) The CAI is known or reasonably expected to contain:

- i. (U) A substantial volume of PII regarding USPs; or
- ii. (U) A greater than de minimis volume of:
 1. (U) Sensitive data, which is defined as data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific USPs, either through the dataset itself or by correlating the dataset with other available information; and that concerns the USP's or USPs' race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the USP or USPs described by the data; or
 2. (U) Data that captures the sensitive activities of USPs or persons in the United States, with sensitive activities defined as activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts; enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the USP or person in the United States who engaged in the activity.

(U) The CAI ICPM explains that SCAI does not include:

- (U) Newspapers or other periodicals; weather reports; books, journal articles, or other published works; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost; or
- (U) Limited data samples made available so an IC element can evaluate whether to purchase the full dataset and not accessed, retained, or used for any other purpose.

(U/[REDACTED]) **SCAI Use:** The IC principally uses SCAI to identify and analyze foreign threats to U.S. interests. It is also used for compliance purposes and for security- and personnel-related functions, including the CE program in which the IC workforce consents to access of their SCAI for clearance vetting purposes.



(U) **Types of Datasets:** The IC obtains CAI, including SCAI, from global datasets, foreign datasets, and U.S. datasets. Specifically, datasets are categorized as:

- (U) “Global” because they cover or focus on more than one country per the nature of the data or per the details of the contract;
- (U) “Foreign” or “individual foreign countries” because they cover or focus on a single foreign country per the nature of the data or per the details of the contract; or
- (U) “U.S.” because they cover or focus only on the United States per the nature of the data or per the details of the contract.

(U//) **SCAI Statistics:** Based on documentation contained in the inaugural report, *September 2025 CAI Report to Congress*, 7 IC elements accessed or purchased a total of 23 SCAI datasets. These 23 SCAI datasets account for only 3.8 percent of the total dollar amount that the IC collectively spent last year on all CAI acquisitions. Of the 23 SCAI datasets, only 6 were “U.S.” focused and all 6 were utilized for the IC’s consent-based CE program. When SCAI specific information is identified in these data-sets, it is handled via the safeguards established in ICPM 504(01), including filtering processes.

(U//) Except for using SCAI about the IC workforce for CE, USP PII is not the focus of the information, or the reason for its acquisition, or, in several cases, even a substantial amount of the information. However, IC elements have made an independent assessment that information about USP in these datasets warrants their designation as “sensitive.” Even though the vast majority of the data is predominately foreign-sourced, IC elements have opted for caution and transparency in documenting their access, collection, or processing of CAI.

Cost of SCAI and Dataset Sources for SCAI		CY 2025
Out of the total dollar amount spent on all of CAI, the percentage that was SCAI obtained from all locations.		3.8%
- Percentage of the total dollar amount that was SCAI data obtained from global and foreign datasets.		2.28%
- Percentage of the total dollar amount that was SCAI data obtained from U.S. specific datasets.		1.52%





(U) Civil Liberties and Privacy Protections for CAI and SCAI

(U) The CAI ICPM establishes general principles for CAI to govern the IC's access to and collection and processing of all CAI, and informs the more specific requirements applicable to SCAI. These include:

- (U) protecting privacy and civil liberties of USPs;
- (U) ensuring that any intelligence products created with that data are consistent with applicable IC standards for accuracy and objectivity;
- (U) applying appropriate safeguards tailored to the sensitivity of information; and
- (U) providing transparency on the policies and procedures governing the IC's access to and collection and processing of CAI to the public and relevant oversight entities while continuing to protect intelligence sources and methods, law enforcement sensitive information, and privileged and other operationally sensitive information.

(U) In addition to the CAI ICPM, the IC's access, collection, and processing of CAI, including SCAI, is subject to additional laws and policies governing intelligence activities, which include those found in the Constitution, statutes, Executive Order 12333, IC element's Attorney General Guidelines, IC and agency policies, and other relevant policies and procedures.

(U) Each element of the IC, supported by their respective legal counsel and Civil Liberties and Privacy Officer (CLPO), is responsible for ensuring their element's activities related to access, collection, and processing of SCAI are within their authorized mission, align with existing legal requirements, and implement internal controls to mitigate privacy and civil liberties risks in accordance with the CAI ICPM. One example of such controls is the requirement to complete a risk analysis prior to accessing or collection of the information to determine whether the value of accessing or collecting the SCAI likely outweighs the privacy and civil liberties, data integrity, quality, and security risk, that cannot reasonably be mitigated. Another control entails requiring IC elements that maintain SCAI to use a system with authority to operate that implements the relevant privacy control baseline and a moderate or high-level privacy overlay control set.

(U) While the IC primarily focuses on foreign intelligence, USP data may be included in commercial datasets either through deliberate acquisition for authorized purposes such as consent-based CE, or incidentally when gathering information on foreign geographies or entities. To minimize and safeguard USP data, the IC has implemented internal controls at various levels. These controls may include policies that mandate analysts to mask or label identifiable USP data, as well as report incidental USP data collection to their supervisors, CLPOs, and legal counsel offices.

(U) These safeguards are implemented on a daily basis as part of the IC's required routine practice, and are not exclusive to just CAI.