FACT SHEET

This document provides information regarding the Intelligence Community's (IC) standards and processes for accessing, collecting, and processing Commercially Available Information (CAI) and the IC's guidance for cataloguing CAI. The IC uses CAI in a range of scenarios and given the increasingly important role it is playing in our work while also carrying the risk of revealing sensitive information about individuals, we are proactively disclosing this framework, which we will continue to refine, clarify, and strengthen. This framework augments the numerous laws and policies that already govern our work, including the Constitution; specific statutes, such as the Privacy Act of 1974; Executive Order 12333; IC element procedures approved by the Attorney General for the protection of U.S. persons information; and other relevant policies and procedures, including those focused on privacy and civil liberties, oversight, and compliance.

Definition

We define CAI as any data or other information that is of a type customarily made available or obtainable and sold, leased, or licensed to 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. As such, CAI does not include information obtained through compulsory process, such as a court order or directive under the Foreign Intelligence Surveillance Act.

Cataloguing

We have issued IC-wide guidance for cataloguing CAI acquired by IC elements, to ensure that information about CAI holdings is accessible within the U.S. Government, as appropriate, in a manner that is consistent with relevant legal, security, classification, access control, and privacy considerations.

Principles

The following general principles govern the IC's access to, collection, and processing of all CAI:

- IC elements' access to and collection and processing of CAI shall be authorized by and consistent with all applicable law and in furtherance of a validated mission or administrative need or function.
- The protection of privacy and civil liberties, and compliance with procedures governing the conduct of intelligence activities, shall be integral considerations, timely considered, in an IC element's access to and collection and processing of CAI.
- IC elements shall undertake reasonable efforts to determine the original source(s) of CAI they access or collect and the method(s) through which the CAI was generated and aggregated.

- IC elements shall assess the integrity and quality of CAI they access or collect—including, as appropriate, by assessing whether the CAI reflects any underlying biases or inferences—in order to ensure that any intelligence products created with that data are consistent with applicable IC standards for accuracy and objectivity (with a focus on standards relating to the quality and reliability of the information).
- IC elements shall not access, collect, or process CAI for the purpose of disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; nor shall they access, collect, or process CAI for the purpose of taking adverse action against an individual based solely on that individual's exercise of Constitutionally-protected rights.
- IC elements shall apply to CAI appropriate safeguards that are tailored to the sensitivity of the information—generally determined by the volume, proportion, and nature of information concerning U.S. persons—and its anticipated use. These safeguards shall reflect consideration of any newly available privacy enhancing methods or technologies and must ensure CAI is properly secured, handled appropriately, and subject to appropriate auditing, retention, destruction, and oversight requirements.
- IC elements shall have in place appropriate processes for managing and periodically reviewing CAI, and any new uses of CAI, in order to ensure the fulfillment of mission or administrative needs and the proper implementation of safeguards and privacy-enhancing techniques.
- To the extent appropriate and practicable, IC elements shall maintain and make available to other IC elements documentation regarding access to and the collection, processing, and safeguarding of CAI, in order to support oversight and promote visibility and learning across the Community on best practices.
- The IC shall provide appropriate transparency to the public and relevant oversight entities on the policies and procedures governing its access to and collection and processing of CAI to further public understanding of intelligence activities while continuing to protect intelligence sources and methods and law enforcement sensitive information, as well as other privileged and operationally sensitive information.

Sensitive CAI

While the above principles are applicable to all CAI, it is possible to identify conditions that elevate the sensitivity of CAI, such that it should be subject to additional protection given the increased potential such information holds for raising privacy and civil liberties concerns. The IC considers CAI that meets the following conditions to be "Sensitive CAI":

- CAI that is known or reasonably expected to contain (1) a substantial volume of personally identifiable information regarding U.S. persons; or (2) a greater than de minimis volume of:
    i. sensitive data, which is defined as data that captures personal attributes,

conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person's or U.S. persons' 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 U.S. person or U.S. persons described by the data; or

ii. data that captures the sensitive activities of U.S. persons 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 U.S. person or person inside the United States who engaged in the activity.

- The above criteria notwithstanding, Sensitive CAI does not include: 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 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 unless assessed in accordance with the framework's policies and procedures for Sensitive CAI.

Protections for Sensitive CAI

The IC is committed to applying the following additional protections to Sensitive CAI:

- *Safeguards.* IC elements must have in place policies and procedures to ensure they appropriately safeguard any Sensitive CAI. Such policies and procedures must take into account not only factors such as the volume, proportion, nature, and intended use of information concerning U.S. persons, but also include enhanced safeguards such as restricted access, additional internal controls, and approval requirements. In addition, IC elements must periodically review such policies and procedures in light of any newly available privacy enhancing methods or technologies.
- *More robust analysis at the point of access or collection.* In order to ensure the proper development and implementation of enhanced safeguards, the timely analysis of sensitivity issues by appropriate officials will be prioritized whenever practicable. Thus, to the extent appropriate given operational security considerations, determinations to access or collect Sensitive CAI shall involve privacy and civil liberties officials, intelligence oversight officials, legal counsel, information officers, and other offices or components that possess relevant equities or experience.

Before such access or collection determinations are made, IC element shall assess the privacy and civil liberties risks associated with accessing or collecting the Sensitive CAI, as well as how the IC element may be able to mitigate such risks. In particular, IC elements are expected to assess whether the relevant mission or administrative requirements can be achieved if any reasonably available privacy-enhancing techniques, such as filtering or anonymizing, the application of traditional safeguards (to include access limitations and retention limits), differential privacy techniques, or other information masking techniques (such as restrictions or correlation), are implemented for information concerning U.S. persons.

- *Periodic review and reassessment.* IC elements will review and evaluate periodically whether Sensitive CAI should be retained in light of its current uses, and if so, whether the existing safeguards are adequate.
- *System requirements.* Sensitive CAI must be retained and processed in systems that: (1) ensure and verify that Sensitive CAI is appropriately secured; and (2) enable IC elements to effectively implement, manage, and audit, as practicable, the privacy and civil liberties protections for Sensitive CAI in accordance with the framework.
- *Documentation and reporting to the Office of the Director of National Intelligence (ODNI).* IC elements will provide documentation to ODNI on the Sensitive CAI that IC elements acquire.
- *Transparency.* Consistent with the *Principles of Intelligence Transparency for the Intelligence Community*, the protection of intelligence sources and methods, and the protection of law enforcement sensitive information, ODNI, in coordination with relevant IC elements, shall provide a report to the public every two years regarding the IC's access to and collection, processing, and safeguarding of Sensitive CAI.

* * * * *

This is not a comprehensive list of the framework's requirements but it is intended to provide the public with a sense of the constraints, principles, and processes that IC elements are applying to CAI.