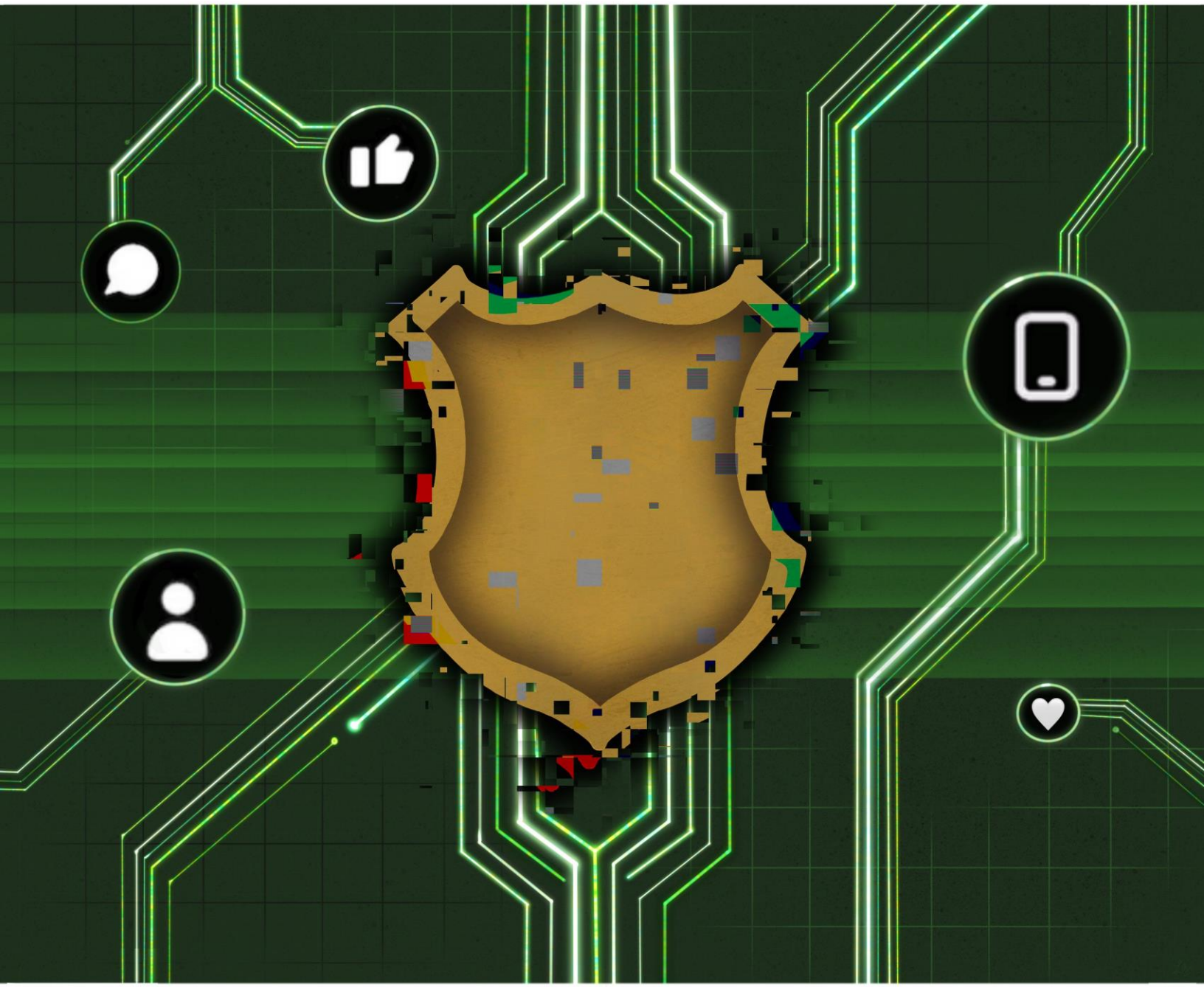
The Privacy and Civil Liberties Oversight Board



Use of Open Source Information by the Federal Bureau of Investigation

Staff Report

November 20, 2025

[THIS PAGE INTENTIONALLY LEFT BLANK]

THE
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

USE OF OPEN SOURCE INFORMATION BY THE FEDERAL BUREAU OF INVESTIGATION

STAFF REPORT

NOVEMBER 20, 2025

Privacy and Civil Liberties Oversight Board

Beth A. Williams, Board Member

TABLE OF CONTENTS

PREFATORY NOTE

This is an unclassified version of a comprehensive report by the staff of the Privacy and Civil Liberties Oversight Board ("PCLOB") on the use of open source information by the Federal Bureau of Investigation ("FBI"). All PCLOB oversight reports undergo a robust accuracy and classification review process with the appropriate Executive Branch agencies to determine whether information contained in a PCLOB report is operationally accurate and whether the information can be made available to the public. At PCLOB's request, the FBI agreed to decontrol significant portions of internal policies governing its use of open source information, as well as information related to the tools the FBI uses to collect and analyze open source information. PCLOB understands this to be the first time such information has been publicly and officially disclosed. Nevertheless, the FBI determined it could not decontrol certain information, including about its use of several tools—Clearview AI, ZeroFox, and Babel Street—such that the information about those tools could be releasable to the public. PCLOB thoroughly investigated the FBI's use of these tools and included that information in its non-public version, which was provided to the White House, to Executive Branch agencies including the FBI, and to Congress.

In accordance with its statutory directive to "make its reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law," PCLOB provides here a public, unclassified version of its report.[1]

[1] 42 U.S.C. § 2000(ee).

I. INTRODUCTION[2]

This is the first comprehensive government report addressing the Federal Bureau of Investigation's ("FBI's") use of open source information.[3] Open source information includes both Commercially Available Information ("CAI")—information available for sale from a commercial entity—and Publicly Available Information ("PAI")—information freely accessible by the public.[4] Early stages of counterterrorism investigations often rely on such information, which is found in public records, news reporting, public social media, commercial databases, and other similarly accessible places.

Open source information includes both information freely accessible to the public and information available for sale from a commercial entity.

While many elements of the Intelligence Community ("IC") access, collect, and process open source information, this report by the Privacy and Civil Liberties Oversight Board ("PCLOB") focuses on uses by the FBI for counterterrorism purposes.[5] Because of the FBI's dual role in investigating domestic crimes while also collecting and analyzing intelligence to prevent them, U.S. persons' privacy and civil liberty interests are especially implicated in the use of such information. The collection and use of open source information poses some risk to privacy and civil liberties, especially when aggregated with other information that may reveal sensitive personal information. At the same time, because open source information is publicly available, it is among the least intrusive means of investigation for counterterrorism and other potential crimes or threats.

The collection and use of open source information poses some risk to privacy and civil liberties, especially when aggregated with other information that may reveal sensitive personal information.

[2] The initiation of this oversight project was approved by a quorate Board in January 2017. The report contains the analysis of PCLOB's staff but has not been voted on or approved by a quorate Board. Per the Board's Sub-Quorum Policy, adopted October 23, 2024, all conditions for publication of this report have been met. *See* PRIV. AND C.L. OVERSIGHT BD., *Sub-Quorum Authorities and Operations when Position of Chair is Vacant*, Policy 102-01, at § 6.1.C (2024), https://documents.pclob.gov/prod/DynamicImages/Generic/59b039ee-73ef-44fc-a80d-862d10a2ca84/102-01~1.PDF.

[3] Board Member Williams thanks all current and former staff members who contributed to this project over the past eight years. Member Williams and PCLOB staff also thank the FBI, and especially its privacy and civil liberties leadership, for their cooperation and assistance with PCLOB's questions and requests.

[4] CAI is generally considered to be a subset of PAI.

[5] PCLOB's enabling statute limits its oversight review to policies, practices, and actions of the Executive Branch "relating to efforts to protect the nation from terrorism." 42 USC § 2000ee(d)(2).

Because open source information is publicly available, it is among the least intrusive means of investigation for counterterrorism and other potential crimes or threats.

The FBI includes privacy and civil liberties protections in all phases of its collection and use of open source information. These protections are evidenced by the FBI's processes governing acquisition of commercial tools, its internal policies, and additional safeguards that it applies to more comprehensive tools. The FBI has heightened access requirements for certain search tools considered to present greater privacy and civil liberties risks. Notably, the FBI does not purchase continuous or "real time" location data from any phone, internet, or electronic service provider.[6] Nevertheless, some of the tools the FBI uses to collect and exploit open source information can potentially reveal sensitive personal details about an individual or permit more invasive queries, including automated searches of social media or databases of biometric information.[7] This report aims to bring transparency to those tools, as well as the policies governing their use.

The FBI does not purchase continuous or "real time" location data from any phone, internet, or electronic service provider.

[6] Responses to PCLOB from Fed. Bureau of Investigation (Oct. 9, 2025). There may be circumstances in which the FBI utilizes real time location data it did not purchase, for example if a cell phone is volunteered to help locate a missing child. *Id.*

[7] The FBI uses the terms "queries" and "searches" interchangeably to mean using a commercial service or tool to access open source information in a focused manner. *See generally* FED. BUREAU OF INVESTIGATION, PRIVACY THRESHOLD ANALYSIS: BABEL STREET (BABEL X AND BABEL SYNTHESIS) 9 (2022) [hereinafter BABEL STREET PTA]; FED. BUREAU OF INVESTIGATION, PRIVACY THRESHOLD ANALYSIS: ZEROFOX 9 (2021) [hereinafter ZEROFOX PTA].

II. REPORT OVERVIEW

A. PCLOB Project Background

PCLOB was established in its current form by the Implementing Recommendations of the 9/11 Commission Act of 2007. The Board's mission is to ensure that efforts by the Executive Branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties.

In January 2017, the Board initiated an oversight project to review the FBI's collection and analysis of open source information for counterterrorism purposes. This oversight project investigated the FBI's collection of information from social media platforms, data brokers, and other sources. It also evaluated the use of such datasets and whether the FBI was purchasing continuous location data.[8] The Board's project did not examine the use of open source information by other IC elements, although PCLOB is aware that other IC elements also utilize open source information.

In preparing this report, PCLOB gathered information from the FBI through requests for documentation, multiple rounds of questions and responses, as well as demonstrations and briefings on the commercial and proprietary tools the FBI uses to collect and use open source information. PCLOB reviewed the FBI's policies, privacy impact assessments and privacy threshold analysis of certain tools, and related documentation from other federal oversight agencies to inform this report.

B. Scope of Report

This report is intended to provide transparency about the FBI's use of open source information, including the commercial and proprietary tools used to acquire such information. It describes the current open source tools used by the FBI at the time of publication. This report also describes the policy limitations on the collection, use, and storage of open source information, and the technological and policy safeguards in place to protect privacy and civil liberties. Given the relatively recent adoption of several of the governing policies, the current report cannot evaluate their operational effectiveness. Further, because the Board in 2017 limited the scope of this project to the FBI, this report does not address the broader IC's use of Open Source Intelligence ("OSINT") through data

[8] Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024). The FBI uses the term "continuous location information" to reflect location information with continuous or intermittent location tracking capabilities. The FBI distinguishes continuous location information from "tagged location information" which refers to location information included in the content of or tags of publicly available posts and does not include any continuous or persistent location information collected directly from an individual's device. *See Id.*; BABEL STREET PTA, *supra,* at 9; ZEROFOX PTA, *supra,* at 9.

brokers and fusion centers. Such topics may warrant further investigation by PCLOB or other entities, and related analysis and potential recommendations would be appropriate under a broader review.

III. BACKGROUND

The types of information that the FBI can obtain online or purchase are generally the same types of information that members of the public can access on their own (such as social media profiles and activity) and information that commercial entities are collecting or aggregating for sale to the public, companies, or foreign adversaries.[9] Open source information often serves as the first tool employed by the FBI in the earlier stage of investigations. In using open source information and any associated analytic tools, FBI employees[10] must comply with the law and applicable IC, Department of Justice ("DOJ"), and internal FBI policies regarding use, retention, and dissemination of open source information. These policies include the Attorney General's Guidelines for Domestic FBI Operations ("AGG-DOM") (governing authorized activities in domestic investigations), Appendix L of the FBI Domestic Investigations and Operations Guide ("DIOG") (governing FBI access to and use of open source information), and FBI Policy Notice 1295N ("PN 1295N") (governing FBI access to and use of CAI).[11] The following section explains the relevant definitions the FBI uses for open source information and what the FBI excludes from those definitions.

A. Definitions

1. Publicly Available Information

PAI, as defined by the FBI, is:

> Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made

[9] Exec. Order No. 14117 (and its associated final rule issued by the Department of Justice) prohibits the sale of bulk sensitive U.S. person data to several adversarial countries. Exec. Order No. 14117, 89 Fed. Reg. 15421 (Mar. 1, 2024); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (final rule Jan. 8, 2025). Note, some of the commercial tools used by the FBI to access open source information are not accessible by the public, such as Clearview AI (discussed below).

[10] The FBI uses the terms "employee" and "personnel" interchangeably across the policies discussed within the report. *See generally* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2020) [hereinafter DIOG].

[11] U.S. DEP'T OF JUST., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS (2008) [hereinafter AGG-DOM]; FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, APPENDIX L (2020) [hereinafter APPENDIX L]; FED. BUREAU OF INVESTIGATION, ACCESS TO AND USE OF COMMERCIALLY AVAILABLE INFORMATION POLICY NOTICE (1295N) (2023) [hereinafter PN 1295N].

> available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.[12]

FBI policies specify that, for use in an investigation, PAI must be available to an employee in the same manner that it is to the general public.[13] Where access to an online resource requires employee registration, that resource is considered publicly available if the registration process accepts all applications from the public and does not further restrict who may access the information.[14] Information on member-only social media sites is also considered PAI unless a user restricts access to the information posted on them.[15]

2. Commercially Available Information

CAI is generally considered to be a subset of PAI, but can only be accessed through paying, leasing, or licensing.[16] The Office of the Director of National Intelligence ("ODNI") defines CAI as:

> Any 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.[17]

---

[12] AGG-DOM, *supra*, at § VII.L. FBI stated that the AGG-DOM definition of PAI encompasses both the definitions of CAI and PAI in DOJ Order 0602, as the AGG-DOM definition from 2008 did not break out PAI and CAI as two separate definitions. Fed. Bureau of Investigation's Correspondence to PCLOB (Oct. 16, 2025). DOJ Order 0602 defines CAI as "any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities" and defines PAI as "information available to the general public that is not sold, leased, or licensed." DEP'T OF JUST., ORDER 0602: COMMERCIALLY AVAILABLE INFORMATION 5 (Jan. 2025).

[13] APPENDIX L, *supra*, at § 3.1.1.

[14] *Id.*

[15] *Id.*

[16] PN 1295N, *supra*, at § 8.1.3. Aside from PN 1295 (discussed further below), FBI policy documents use the terms "open source information" and "PAI" interchangeably. Additionally, the FBI did not distinguish open source information or PAI from CAI until PN 1295, released in December 2023. As such, PCLOB has relied on the CAI definitions proffered in the FBI's PN 1295 and ODNI's CAI Framework. OFF. OF THE DIR. NAT'L INTEL., INTELLIGENCE COMMUNITY POLICY FRAMEWORK FOR COMMERCIALLY AVAILABLE INFORMATION 1 (2024), https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf [hereinafter FRAMEWORK].

[17] FRAMEWORK, *supra*, at § IV.C.

3. Sensitive Information

Sensitive information, including both PAI and CAI, is generally considered to be "known or reasonably expected to contain a substantial volume of personally identifiable information regarding U.S. persons, or a greater than de minimis volume" of sensitive data of U.S. persons, or data on sensitive activities of anyone in the United States.[18]

B. Exclusions

The FBI prohibits employees from accessing online open source information for which a person would have a reasonable expectation of privacy, including where an individual has restricted public access to one's information, unless FBI employees first obtain legal process or consent.[19] For instance, information is not considered PAI, and therefore is not available for access by FBI personnel, "if the information owner restricts access to the information," such as on websites, chatrooms, and instant messaging applications where privacy features have been enabled or access is invitation-only.[20]

[18] FRAMEWORK, *supra*, at § II.A. At the time of this report, the FBI stated it did not have a standard definition for "sensitive data" but would adhere to any approved policy definition from ODNI or DOJ. Responses to PCLOB from Fed. Bureau of Investigation (May 2024).

[19] Briefing to PCLOB from Fed. Bureau of Investigation (Oct. 20, 2022); PN 1295N, *supra*, at § 4.1.

[20] APPENDIX L, *supra*, at § 3.1.1. Note, additional information is available in the non-public version of the report.

IV. GUIDELINES FOR USE OF OPEN SOURCE INFORMATION

The FBI's use of open source information is governed by multiple laws and policies, most pertinently, federal constitutional protections, FBI, DOJ, and IC policies, the Federal Records Act of 1950, Executive Order 12333, and the National Security Act of 1947.[21] The FBI reported that it only purchases access to commercial tools consistent with its authorities and applicable law and policy, including the Fourth Amendment, the Electronic Communications Privacy Act, and internal policies.[22] The following sections discuss the applicable administrative documents that govern and establish parameters for the FBI's collection and use of open source information.

A. IC Commercially Available Information Policies

The proliferation of open source information, its potential sensitivity, and advances in artificial intelligence ("AI") required standardization and clarity across the IC for how open source information can be used while ensuring the appropriate protection of privacy and civil liberties. Accordingly, throughout 2024, ODNI promulgated several policies and strategic frameworks to better integrate open source information into IC products, govern the IC's handling of CAI, and establish consistent requirements for citing and referencing the sources of open source information in intelligence products. Given the relatively recent release of these policy documents, how the underlying policies will be operationalized throughout the IC, including the FBI, has yet to be determined.

In March 2024, ODNI and the Central Intelligence Agency ("CIA") released the IC OSINT Strategy for 2024–2026. The OSINT Strategy provides the framework for integrating open source information more fully into IC workflows by focusing on four strategic areas: (1) "coordinat[ing] open source data acquisition and expand[ing] sharing," (2) "establish[ing] integrated open source collection management," (3) "driv[ing] OSINT innovation to deliver new capabilities," and (4) "develop[ing] the next generation OSINT workforce and tradecraft."[23] The OSINT Strategy asserts that these efforts will support the IC in harnessing the value of open source information while safeguarding privacy and civil

[21] Note, this is a list of general privacy-related legal authorities, not specific to use of open source information. *See* FED. BUREAU OF INVESTIGATION, OFF. OF THE GEN. COUNS., PRIVACY POLICY GUIDE (1113PG) § 5.1 (2021); *see generally* U.S. CONST. amend. I; Federal Records Act of 1950, 44 U.S.C. § 3101; National Security Act of 1947, 50 U.S.C. § 3001; Exec. Order No. 12333, as amended, 46 Fed. Reg. 59941 (1981).

[22] Responses to PCLOB from Fed. Bureau of Investigation (Mar. 20, 2024); *see generally* U.S. CONST. amend. IV; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); AGG-DOM, *supra*; DIOG, *supra*.

[23] U.S. INTEL. CMTY., THE IC OSINT STRATEGY 2024–2026 1 (March 2024), https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

liberties.[24] For example, the OSINT Strategy calls on the IC to develop harmonized tradecraft and training standards, "to ensure all OSINT activities are conducted in a manner that protects [IC] collection requirements and sources, and safeguards U.S. persons' information and privacy."[25] This high-level strategy notes the dynamic open source environment, and calls on the OSINT community annually to review the strategy and develop an action plan to guide implementation efforts.[26]

In May 2024, ODNI released its Policy Framework for Commercially Available Information ("Framework") establishing general principles governing the IC's access, collection, and processing of CAI.[27] The Framework also provides guidance for identifying categories of CAI that pose a heightened risk to privacy and civil liberties, referred to as "sensitive CAI."[28] In addition to defining sensitive CAI, the Framework requires all IC elements to establish policies and procedures that safeguard sensitive CAI, and periodically review and reassess these safeguards as well as whether sensitive CAI should be retained.[29] Finally, the Framework requires more robust analysis prior to access or collection of sensitive CAI and a determination based on the totality of circumstances that the access or collection of sensitive CAI "likely outweighs the privacy and civil liberties risks, data integrity and quality risks, security risk, and any other risks not [specified], that cannot reasonably be mitigated."[30]

The FBI's PN 1295N also governs access to and use of CAI.[31] It establishes guidance for the FBI's "access to and collection, processing, use, and sharing of [CAI], whether purchased or not, to ensure compliance with applicable laws and [executive orders], and with DOJ and Intelligence Community policies."[32] FBI employees are prohibited from accessing, collecting, processing, using, or sharing CAI, including CAI obtained from a data broker or any other type of external partner, without formal approval through the CAI

[24] *Id.*

[25] *Id.* at 4.

[26] *Id*. at 1.

[27] *See generally* FRAMEWORK, *supra*.

[28] *Id*. at 3–10.

[29] *Id.* at 7–9.

[30] *Id.* at 6.

[31] PN 1295N, *supra*, at § 2.1. The FBI has advised that a more robust policy directive for guidance on CAI to meet mission needs will be forthcoming. Responses to PCLOB from Fed. Bureau of Investigation (Sept. 25, 2025).

[32] PN 1295N, *supra*, at § 2.1.

governance process, which includes review by several FBI components, including the Privacy and Civil Liberties Unit within the Office of the General Counsel.[33]

B. Other FBI Internal Policies

The FBI's internal policies impose different requirements for accessing open source information depending on the stage of the inquiry: prior to an assessment, assessment, or investigation. As described above, each of these stages is established by the AGG-DOM and the DIOG.[34]

1. Prior to an Assessment

The FBI's internal policies impose different requirements for accessing open source information depending on the stage of the inquiry: prior to an assessment, assessment, or investigation.

FBI employees can initially process a complaint, observation, or information without opening an assessment.[35] When engaged in these activities, FBI employees must have a reason that is tied to an authorized FBI criminal or national security purpose.[36] With regard to open source research specifically, Appendix L of the DIOG stipulates that, even at this early stage, employees must identify "a rational reason—tied to criminal activity or a national security threat—to search for and view the online information or data being sought."[37] FBI employees "must always ensure that all online investigative activities are 'focused in scope, time, and manner to achieve the underlying purpose' [and] FBI employees must document this relationship, as necessary, in the case file."[38]

Prior to opening an assessment, FBI employees are authorized to engage in certain online investigative methods including, among others: viewing public information, viewing records or other information already in the possession of the FBI, and utilizing online services and resources.[39] Appendix L authorizes FBI employees to search for and view

[33] *Id.* at § 5.2.

[34] APPENDIX L, *supra*, at § 1.

[35] FBI DIOG, *supra*, at § 5.1.1.

[36] *Id.* An example of an authorized activity prior to an assessment includes checking records in internal FBI databases or searching internet databases related to preliminary unverified information through an incoming phone or internet "tip."

[37] APPENDIX L, *supra*, at § 3.1.

[38] *Id.* at § 2.1 (citing FBI DIOG, *supra*, at § 4.1.2).

[39] FBI DIOG, *supra*, at § 5.1.1.

"government systems and paid-for-service databases, as well as information available to the public via the Internet" without an open assessment or investigation.[40] It also permits FBI employees to conduct proactive online searches (i.e., searches that are not conducted as a result of incoming complaints, tips, leads, or referrals) of open source information in order to process observations or other information for authorized purposes prior to an assessment.[41]

Appendix L of the DIOG recognizes that the protection of civil liberties and privacy is "particularly important when applied to online investigative methods because much of the content and many of the activities available or conducted on the Internet fall within some category of [First Amendment] protected information."[42] Even at this early stage, FBI employees are directed to protect the public's privacy and civil liberties and carefully review and document their investigative activities.[43]

2. Assessment

The FBI may open an assessment regarding a potential threat to national security or a federal crime so long as it has an authorized purpose and clearly defined objective. The AGG-DOM does not require any particular factual predication to open an assessment, but the authorized purpose must be an authorized national security, criminal, or foreign intelligence collection purpose.[44] In addition, the purpose "must be well-founded and well-documented."[45] The objective of the assessment must be clearly defined, such as to detect, prevent, or obtain information about federal crimes or national security threats, or to collect foreign intelligence.[46]

Once an assessment has been opened, the DIOG and Appendix L authorize additional online investigative methods.[47] For example, FBI employees are permitted to use automated searches (e.g., Google alerts) to conduct regular searches of open source information or create, under certain circumstances, an online account using fictitious information to access

[40] APPENDIX L, *supra*, at § 3.1.

[41] *Id.* at § 3.4.2.

[42] *Id.* at § 2.1.

[43] *Id.* Executive Order 12333 and the AGG-DOM also specify that collection of information must be handled via the "least intrusive method feasible." AGG-DOM, *supra*, at § I.C.2.a; *see* Exec. Order No. 12333, *supra*, at § 2.4.

[44] AGG-DOM, *supra*, at § II.

[45] FBI DIOG, *supra*, at § 4.1.2.

[46] *Id.* at § 5.1.; AGG-DOM, *supra*, at § II.

[47] FBI DIOG, *supra*, at 18.5.4.

open source information.[48] Consistent with its limits on the use of open source information, however, the FBI prohibits access to open source information where an individual restricts public access to his or her information online, or where information is not otherwise publicly accessible.[49]

3. Predicated Investigation

The FBI may open a predicated investigation when the FBI identifies evidence of a crime, a national security threat, or foreign intelligence activity.[50] In essence, assessments are used to determine whether an identified threat activity exists, while predicated investigations are used to evaluate evidence of threat activity. Predicated investigations concerning federal crimes or threats to national security require supervisor approval; assessments do not.[51] Certain other investigative methods, including physical and electronic surveillance requiring a search warrant, require a predicated investigation, but all open source investigative methods are permissible at the assessment stage.

[48] APPENDIX L, *supra*, at § 4.2.

[49] *Id.* at § 3.1.1.

[50] FBI DIOG, *supra*, at §§ 6.1, 7.1.

[51] *Id.* at § 5.6.3.1.3; AGG-DOM, *supra*, at §§ II.A.2, II.B.2.

V. THE FBI'S USE OF COMMERCIAL AND PROPRIETARY TOOLS

Commercial tools[52] consolidate substantial amounts of open source information, enabling users to more efficiently conduct searches by bypassing the need to visit individual websites and conduct manual searches. These tools also filter vast amounts of open source information, thereby limiting the amount of information that must be reviewed. The FBI reported that its employees may directly access and enter search terms into commercial tools (e.g., Babel Street, discussed in the non-public version).[53] However, with ZeroFox (also discussed in the non-public version), the FBI provides its search terms to the commercial tool provider who conducts searches on behalf of the FBI.[54]

In addition, the FBI can purchase newsletters or similar products from commercial providers, which can contain search results and other information developed by providers.[55] Below is a survey of the enterprise (i.e., agency-wide) commercial and proprietary tools used by the FBI to access, collect, and analyze open source information for counterterrorism purposes.

A. Commercial Services and Tools for Use with an Authorized Purpose

The following is a list of enterprise commercial tools the FBI currently uses for counterterrorism purposes when there is an authorized investigative purpose—the minimal threshold required for using open source tools.[56] Commercial tools requiring an open assessment or investigation (in addition to requiring an authorized investigative purpose) due to a heightened risk to privacy and civil liberties (e.g., Clearview AI, ZeroFox, and Babel Street) will not be addressed in this public report but are discussed in the version that includes controlled but unclassified information provided to the White House, relevant Executive Branch agencies, and Congress. Prior to the Directorate of Intelligence granting access to the commercial tools described in this section (except Experian,[57] discussed below), FBI employees must have completed required privacy training, have a need to know

[52] The term "commercial tool" includes commercial databases and services that allow FBI employees to access, collect, and analyze open source information. This report omits commercial tools used exclusively for analysis of open source information already collected by the FBI. Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024).

[53] *Id*.

[54] *Id.*

[55] *Id.*

[56] AGG-DOM, *supra*, at § II. Note, the FBI used CLEAR, CLEAR-License Plate Reader, and Thomas Reuters World Check until October 1, 2025. Responses to PCLOB from Fed. Bureau of Investigation (Sept. 25, 2025).

[57] Experian does not require prior supervisory approval because it is a direct feed.

the information they are querying, and obtain supervisor approval.[58] The Directorate of Intelligence will also conduct annual audits of user accounts for these tools.[59]

1. LexisNexis & Thomas Reuters Tools

LexisNexis and Thomas Reuters allow authorized users to conduct searches of a person's or business's information and is one of the primary commercial providers of open source information. LexisNexis provides users with reports, based on search criteria, compiled in an organized manner to aid in investigations.[60] For LexisNexis and Thomas Reuters, when query results are deemed relevant to an open assessment or investigation, FBI employees may download and save reports, but they are otherwise not retained by the FBI.[61]

Accurint for Law Enforcement: Accurint is a web-based tool that is available to courts, law enforcement, or other government agencies.[62] Accurint permits person and business queries, which can provide information about: bankruptcies, business affiliations, driver's licenses and motor vehicles, Federal Aviation Administration filings (such as pilot's licensing information), internet domain names, merchant vessels, listings of individuals required under the Patriot Act (such as the Terrorist Exclusion List—a Department of State authority to designate terrorist organizations for immigration purposes), property deeds and assessments, criminal and civil court searches, and filings related to commercial transactions involving creditors.[63] Exact databases searched are unknown to the FBI and considered proprietary by LexisNexis.[64]

[58] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[59] Responses to PCLOB from Fed. Bureau of Investigation (Sept. 25, 2025).

[60] Responses to PCLOB from Fed. Bureau of Investigation (June 17, 2020).

[61] Briefing to PCLOB from Fed. Bureau of Investigation (Aug. 19, 2024); Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024); Responses to PCLOB from Fed. Bureau of Investigation (June 17, 2020).

[62] *See* LexisNexis Risk Solutions*, LexisNexis Accurint*, https://www.accurint.com/ (last visited Nov. 10, 2025) for a list of customer-types that Accurint serves.

[63] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020); Fed. Aviation Admin., *Pilot Certificates & Records*, https://www.faa.gov/pilots/lic_cert (last visited Nov. 10, 2025); U.S. Dep't of State, *Terrorist Exclusion List*, https://www.state.gov/terrorist-exclusion-list (last visited Nov. 10, 2025).

[64] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020); Briefing to PCLOB from Fed. Bureau of Investigation (Aug. 19, 2024).

Accurint Virtual Crime Center: The Virtual Crime Center brings together disconnected crime and civil violation data from over 10,000 different sources, including state, local, tribal and territorial police agencies and public records.[65]

LexisNexis CourtLink: CourtLink offers access to a collection of court dockets and documents as well as alert and search features.[66]

Westlaw Edge: Westlaw Edge is a legal research platform that utilizes AI to expedite research.[67] Westlaw Edge also includes analytic services to assist users in developing legal documents and litigation strategy.[68]

2. Other Tools

Experian: The FBI receives quarterly updates to Experian's telephone subscriber data collections.[69] Experian provides the FBI self-reported phone data provided by consumers.[70] These numbers frequently contain unpublished phone numbers, phone numbers where the consumer previously resided, and cell phone numbers not available in other sources.[71] Experian assists FBI users in locating consumers by providing the last known addresses associated with a consumer's phone number on record.[72]

B. Commercial Services and Tools Requiring an Open Assessment or Investigation

This section concerns the FBI's use of commercial services and tools requiring an open assessment or investigation, such as Babel Street,[73] ZeroFox, and Clearview AI. The FBI

---

[65] *LexisNexis Accurint Virtual Crime Center*, LEXISNEXIS, https://risk.lexisnexis.com/products/accurint-virtual-crime-center (last visited Nov. 10, 2025).

[66] *See CourtLink*, LEXISNEXIS, https://www.lexisnexis.com/en-us/products/courtlink.page (last visited Nov. 10, 2025).

[67] *Westlaw Edge with AI-Assisted Research*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/products/westlaw-edge/features (last visited Nov. 10, 2025); Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024); Responses to PCLOB from Fed. Bureau of Investigation (June 17, 2020).

[68] *Westlaw Edge with AI-Assisted Research*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/products/westlaw-edge/features (last visited Nov. 10, 2025).

[69] Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024); Responses to PCLOB from Fed. Bureau of Investigation (June 17, 2020).

[70] *Id*.

[71] *Id*.

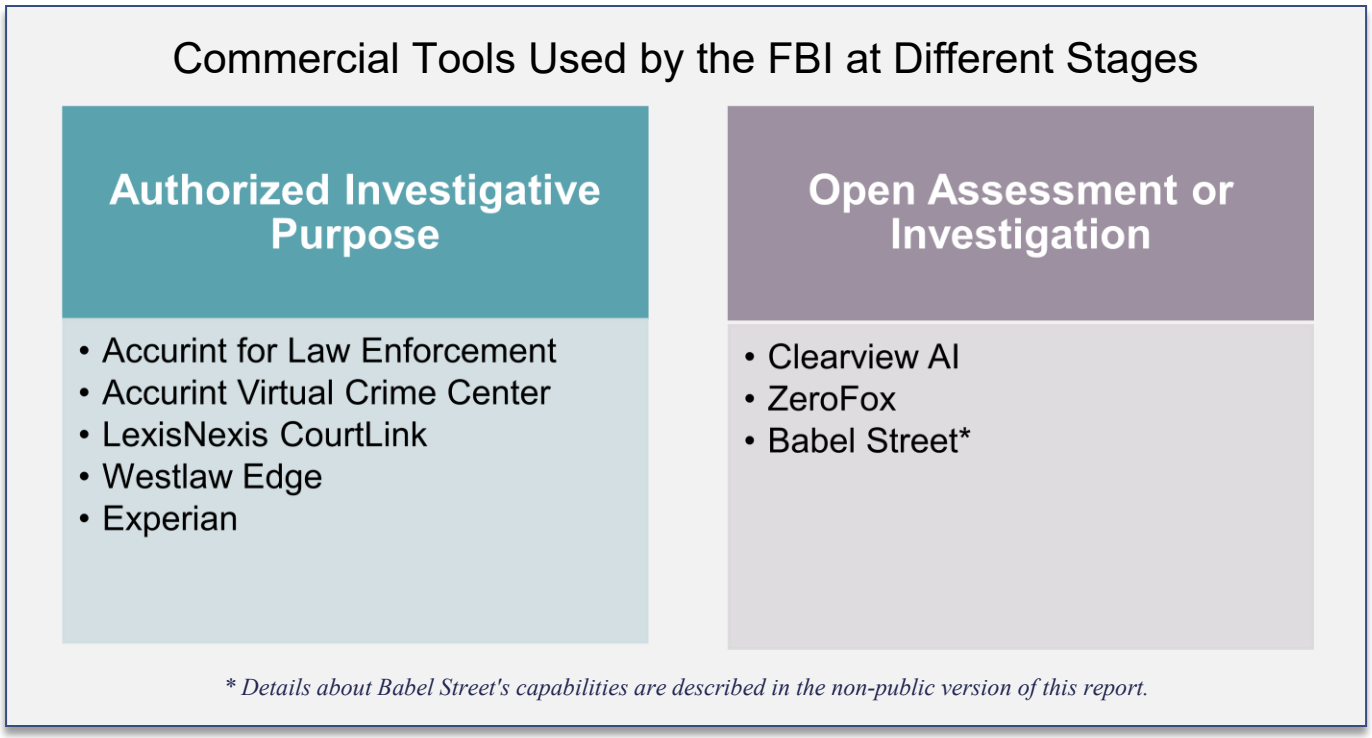
[72] *Id*.

[73] In some instances, Babel Street may be used prior to an open assessment or investigation.

provided PCLOB staff with multiple in-person demonstrations of these tools, policy compliance documentation governing their use and any privacy protective safeguards, as well as responses to tool-specific questions from PCLOB staff. The non-public version describes these tools, how the FBI uses them in assessments or investigations, any safeguards in place, and how the FBI retains information collected from these tools. The FBI considers information about these tools to be controlled but unclassified information and not able to be publicly released. PCLOB's non-public version, which includes this section, was provided to the White House, to Executive Branch agencies including the FBI, and to Congress.

C. Proprietary Tools

This section concerns the FBI's use of proprietary tools. More information is available in the non-public version of this report.



VI. USE AND LOGGING OF OPEN SOURCE INFORMATION

The manner in which FBI employees document their use of commercial tools varies, but the use and documentation must comply with the DIOG, including Appendix L.[74]

In December 2024, ODNI released Intelligence Community Standard ("ICS") 206-01 to standardize requirements for citing and referencing sources of open source information across intelligence products.[75] According to ICS 206-01, whenever open source information is cited in intelligence products, it must be cited in accordance with the new prescribed guidelines, including: (1) required elements of source reference citations, (2) formatting instructions for source reference citations, and (3) guidelines for referencing standalone open source information products (e.g., contents from a commercial database, open source media, social media, or websites).[76] In addition to the citation conventions, ICS 206-01 states that descriptive source reference citations should be the default, and generic citations should only be used where "legitimate and data-driven security concerns" preclude descriptive details.[77] ICS 206-01 states that for the purposes of PAI and CAI, products should include a source description and must name the commercial database or, if the data is aggregated by a third-party provider, the entity that owns or created the original data.[78] The FBI stated that its current definition and process of CAI governance generally encompasses the IC CAI definition and process requirements.[79]

Appendix L also requires FBI employees to "review, analyze, and document their [online] investigative activities carefully" due to the privacy and civil liberties concerns associated with such activities.[80] FBI employees must also comply with tool-specific

[74] The non-public version of this report includes more information regarding variability in the use of commercial tools.

[75] OFF. OF THE DIR. OF NAT'L INTEL., INTELLIGENCE COMMUNITY STANDARD 206-01: CITATION AND REFERENCE FOR PUBLICLY AVAILABLE INFORMATION, COMMERCIALLY AVAILABLE INFORMATION, AND OPEN SOURCE INTELLIGENCE (2024), https://www.dni.gov/files/documents/ICD/ICS-206-01.pdf [hereinafter ICS 206-01].

[76] *Id*. at 2, 8–17. A source reference citation is a specified set of factual information elements about a source, present in uniform format in an endnote. Information in source reference citations enable readers to locate and retrieve the source and may help readers assess the quality or credibility of the source in accordance with Intelligence Community Directive 206. *Id.* at 6.

[77] *Id*. at 8.

[78] *Id*. at 10–11. The FBI informed PCLOB staff that the FBI's Style Guide for FBI Analytic Intelligence Products is being updated to include a link to the ICD 206-01. Additionally, the citation requirements will be referenced in the next update to the CAI Policy, mentioned above. Responses to PCLOB from Fed. Bureau of Investigation (Sept. 25, 2025).

[79] Responses to PCLOB from Fed. Bureau of Investigation (Oct. 9, 2025).

[80] APPENDIX L, *supra*, at § 3.1.; Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

documentation requirements. Such requirements are articulated in the applicable tool's privacy documentation.[81] If the parameters of an FBI employee's queries or the purposes for using the tool change beyond what is reasonably expected during the course of an assessment or investigation, FBI employees must file follow-up electronic communications that explain the changes.[82]

Appendix L also directs FBI employees to retain the contents of stored electronic messages (e.g., email), "if they would have retained those messages if they would have been written on paper."[83] If an employee "observes information that cannot be printed due to the short duration it is available, (i.e., Snapchat [posts]), the employee should memorialize any information of investigative value in an FD-302 ('Form for Reporting Information that May Become the Subject of Testimony')."[84]

[81] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[82] *Id.*

[83] APPENDIX L, *supra*, at § 2.4.

[84] *Id.*

VII. AUDITING THE USE OF OPEN SOURCE INFORMATION

The use of open source information is primarily audited through file review and justification review processes that apply to both assessment and investigation files.[85] File and justification reviews are intended to ensure that the investigative methods used in a given matter comply with applicable legal and policy requirements (e.g., the DIOG and Appendix L) and that privacy and civil liberties are protected during the investigative process.[86] The FBI advised that it does not monitor and audit all queries made by employees because doing so would increase the risk to an individual's privacy by requiring vendors to permanently store FBI searches and information.[87]

Whether the FBI conducts a file review or a justification review depends on whether the review is being conducted for certain types of assessments or a predicated investigation. File reviews, when a supervisor examines all files to ensure that they meet investigative criteria, are conducted for all predicated investigations and Types 3–6 Assessments every 90 days; or every 60 days for probationary employees.[88] Type 3 Assessments identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities; Type 4 Assessments obtain and retain information to inform or facilitate intelligence analysis and planning; Type 5 Assessments seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources; and Type 6 Assessments seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.[89]

Justification reviews, which consider whether progress has been made towards an authorized investigative purpose in compliance with the DIOG or whether the assessment should be terminated, are conducted for Types 1–2 Assessments every 30 days.[90] Type 1 and 2 Assessments seek information (proactively or in response to investigative leads) relating to activities—or the involvement or role of individuals, groups or organizations relating to

[85] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[86] *Id.*; Email to PCLOB Staff from Fed. Bureau of Investigation (Jan. 10, 2022); Email to PCLOB Staff from Fed. Bureau of Investigation (Oct. 29, 2021).

[87] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[88] DIOG, *supra*, at §§ 3.5.4, 6.7.5.

[89] *Id.* at §§ 3.5.4, 5.4.1.

[90] *Id.*

those activities—constituting violations of federal criminal law or threats to the national security.[91]

FBI supervisors are responsible for ensuring that all online investigative activities are conducted in accordance with the DIOG, including Appendix L.[92] Supervisors can address mishandled open source information in various ways depending on the specific circumstances.[93] Within the FBI, non-compliance with the DIOG can be reported to the Legal Compliance and Enterprise Risk Unit, Inspection Division (formerly the Office of Integrity and Compliance), investigative misconduct can be reported to the Initial Processing Unit, Inspection Division, and privacy or civil liberties violations can be reported to the Privacy and Civil Liberties Officer, Office of the General Counsel.[94] Likewise, misuse of open source information can also be reported to DOJ's Office of the Inspector General and Chief Privacy and Civil Liberties Officer.[95]

Moreover, an FBI policy directive establishes a procedure for handling information determined to have been gathered in violation of the Privacy Act's restrictions on maintaining records of individuals' First Amendment activities.[96] Finally, supervisors can address potential mishandling of open source information by coordinating with management, Office of the General Counsel, or respective Chief Division Counsel if the mishandling occurs at a field office.[97] Disciplinary outcomes are outlined in the applicable policies and factors to be considered include the severity of the violation, whether the employee has been previously disciplined, and length of service.[98]

---

[91] *Id.*

[92] *Id.* at § 3.5.4.5.

[93] Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024).

[94] *Id.*

[95] *Id.*

[96] *See* FED. BUREAU OF INVESTIGATION, HANDLING OF PRIVACY ACT RECORDS MAINTAINED IN VIOLATION OF THE PRIVACY ACT'S PROVISION CONCERNING FIRST AMENDMENT ACTIVITY POLICY DIRECTIVE (1270D) (2023).

[97] APPENDIX L, *supra*, at § 1.

[98] *See generally* U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S DISCIPLINARY SYSTEM 144-45 (2009), https://www.govinfo.gov/content/pkg/GOVPUB-J37-PURL-gpo134090/pdf/GOVPUB-J37-PURL-gpo134090.pdf.

VIII. RETENTION OF OPEN SOURCE INFORMATION

The FBI advised that there are no minimization procedures that specifically apply to open source information, but the retention of open source information follows the retention policies applicable to investigative or intelligence records, in accordance with internal policy and the Federal Records Act.[99] While processing a complaint or responding to a tip or lead, FBI employees are permitted to collect and retain records checks and other information accessed prior to the opening of an assessment, as long as there is a law enforcement, national security, intelligence, or public safety purpose.[100] For proactive online searches of open source information, they may only collect and retain information resulting from proactive online searches if a law enforcement, national security, intelligence, or public safety purpose exists for doing so and the information is within the scope of an open assessment or a predicated investigation, or if it serves as the basis for opening an assessment or predicated investigation.[101]

The FBI stated that it may only collect and retain U.S. person information relating to the exercise of a First Amendment right if: (1) the collection is "logically related" to an authorized investigative purpose; (2) the collection does not "materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights;" and (3) the method of collection is the "least intrusive alternative that is reasonable, based upon the circumstances of the investigation."[102] The DIOG imposes these restraints for all FBI investigative activities.[103]

[99] Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024); Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020). Retention of investigative and intelligence records is directly managed by the FBI's Information Management Division ("IMD") Records Disposition Unit. The retention period for open source information acquired by the FBI is the retention period for the applicable case file and/or system where the information is maintained. All records must be retained according to the National Archives and Records Administration ("NARA") approved disposition schedules. Therefore, any open source information records assume the NARA-approved retention periods approved for the file classification. FBI records that describe the exercise of First Amendment rights that are determined to have been collected or retained in violation of the Privacy Act must be destroyed in accordance with IMD policy. Responses to PCLOB from Fed. Bureau of Investigation (Mar. 2024); Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[100] APPENDIX L, *supra*, at § 3.4.1.; DIOG, *supra*, at § 5.1.1.

[101] APPENDIX L, *supra*, at § 3.4.2.; DIOG, *supra*, at § 5.1.1.

[102] APPENDIX L, *supra,* at § 2.1.

[103] DIOG, *supra*, at § 4.2.1.

IX. DISSEMINATION OF OPEN SOURCE INFORMATION

The FBI reported that it may disseminate open source information collected through commercial tools outside of the agency.[104] While the source of the information does not change the analysis, the type of information may impact how information is disseminated and under what authorities (e.g., terrorism, foreign intelligence, counterintelligence, and criminal).[105] General dissemination guidance applies to open source information, including permitting dissemination if necessary to prevent a crime or threat to national security.[106] Disseminations to an outside agency involving a U.S. person must be documented and logged pursuant to the Privacy Act, DIOG Sections 12.6 and 12.7, and FBI Policy Directive 0012D, FBI Information Sharing Activities with Other Government Agencies.[107] Disseminations outside the FBI are reviewed through supervisory reviews of case files.[108]

[104] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020). For instance, DIOG Section 14.3.1 contains general dissemination guidance, which applies to open source products. DIOG, *supra*, at § 14.3.1. The FBI stated that all disseminations are made in accordance with law, regulation, and policy.

[105] Responses to PCLOB from Fed. Bureau of Investigation (Jan. 9, 2020).

[106] *Id.*

[107] *Id.*

[108] *Id.*

X. CONCLUSION

As access to aggregated open source information continues to evolve, the FBI will need to continually evaluate the privacy and civil liberties impacts of new tools and datasets.

The FBI has been able to rely on the proliferation of open source information to support its counterterrorism mission. Despite being publicly available, the collection and use of open source information poses some risk to privacy and civil liberties, especially when aggregated with other information that may reveal sensitive personal information. To mitigate this risk, the FBI includes privacy and civil liberties safeguards in all phases of its collection and use of open source information. These safeguards include internal policies that impose different requirements depending on the investigative phase, and a compliance process to ensure those policies are followed. FBI internal governance processes also establish requirements that must be followed prior to the acquisition of commercial tools. PCLOB's review confirmed the FBI does not purchase real time continuous location information, one of the most sensitive types of data. PCLOB's review also found that the FBI includes additional safeguards specific to Clearview AI, Babel Street, and ZeroFox, the three tools capable of collecting more sensitive data. Finally, as access to aggregated open source information continues to evolve, the FBI will need to continually evaluate the privacy and civil liberties impacts of new tools and datasets.

APPENDIX: HYPOTHETICAL USES OF OPEN SOURCE INFORMATION

The following hypotheticals demonstrate how an FBI employee might use open source information and the tools available to them in counterterrorism operations. The examples are not based on real-life cases.

1. ***Open source queries were initially conducted prior to the opening of an assessment or an investigation but OSINT revealed sufficient information to support the initiation of an assessment or an investigation.***

The FBI receives an anonymous online tip to its Internet Crime Complaint Center which states, "I saw three men in a blacked out car taking pictures in front of a church located at 123 1st Street, Random, OH. The license plate of the vehicle was XXX XXXX."

By researching the license plate number provided in open source databases, the FBI is able to identify the owner of the vehicle, along with his date of birth, address, and contact information. Searches of internal FBI and other federal and local databases do not reveal a criminal history or other derogatory information. Further searches of PAI resources identify several social media accounts associated with the vehicle's owner. Upon reviewing these social media accounts, the FBI learns the individual has posted ISIS propaganda, videos of jihadi leaders, and a photo of himself holding an assault rifle.

Based on its evaluation of this information, the FBI decides to open a Type 1 & 2 Assessment to further examine whether this individual may have been conducting pre-attack surveillance or otherwise poses a threat of terrorism.

2. ***Open source queries supported the closure of an investigative matter (i.e., results were not revelatory or did not substantiate an allegation).***

Starting from the same initial information as in Example 1 above; however, when the FBI searched PAI resources the social media accounts instead revealed the owner was active in several local civic organizations including a nearby religious organization. Social media showed no indications of association with violent extremism or other propensity for violence.

Based on its evaluation of this information the FBI decides to document its findings but takes no further action on the matter.

3. ***How the FBI has successfully used Clearview AI, Babel, or ZeroFox***

The FBI receives an anonymous online tip to its Internet Crime Complaint Center which states, "Other students in my school are saying someone has been talking online about wanting to attack a school in City, OR."

The FBI might use Clearview AI, Babel Street, ZeroFox or other online tools to analyze social media posts regarding City, OR in association with authorized threat terms, such as "kill," "pipe bomb," "shoot," etc. Threat terms are selected by FBI analysts based on the nature of the threat, and the terms are reviewed by FBI attorneys to ensure they are not legally objectionable. FBI analysts then review the results obtained from the search tool to confirm the social media posts returned indicate a possible threat, based on the context of the post, and to eliminate any false positive hits. After review, the FBI analysts would send those posts that indicate a potential threat as a lead to the appropriate field office for further investigative action.

Investigators in the receiving field office will evaluate the lead information to determine what further action may be warranted. For example, the field office may choose to open a Type 1 & 2 Assessment directly, or the field office may want to conduct additional complaint processing or may determine the lead does not present a threat and close the matter.