

Department: Boston Police Department
Submitted by: Boston Police Department
Date: September 9, 2026

Technology: Social Media Analysis Tools (Version 2)

1. Purpose: What is the purpose of this Technology?

The Boston Police Department utilizes “Social Media Analysis Tools” to identify potential criminal threats to public safety, including threats of mass violence, and to gain situational awareness of developments within online forums utilized by various types of criminal actors, domestic violent extremists (DVEs), foreign terrorist organizations (FTOs), and those inspired by FTOs. Social media analysis tools are also used in furtherance of criminal investigations by providing an efficient and comprehensive means to locate an individual’s public online presences.

These tools improve personnel efficiency and increase analytic accuracy when reviewing these large datasets, while also protecting individuals’ privacy, civil rights and civil liberties. The tools allow targeted review of voluminous online content to locate and allow analysts to review threat information that could impact the Boston Metro Area.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing. BPD Rule 113A (Bias-Free Policing Policy).

2. Authorized Use: What are the uses of this Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?

Use of these tools, like all Department software and databases, shall be limited to users authorized by the Department to access these tools in the course and scope of their employment to support the administrative and investigatory functions of the Department.

Department personnel shall only utilize Social Media Analysis Tools to seek or retain information based on one or more of the following factors:

- (1) Information based upon a Criminal Nexus¹ or threat to public safety;
- (2) Information based on a reasonable suspicion that an identifiable individual or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity

¹ Criminal Nexus is defined as an individual or group’s involvement or planned involvement in a criminal activity is substantiated by indicators such as behavior or circumstances.

that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal conduct or activity;

- (3) Information relevant to the investigation or prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, or the prevention of crime; or
- (4) Information useful in crime analysis, situational assessments, and event planning for maintaining public safety.

Department personnel shall not utilize Social Media Analysis Tools to seek or retain information about:

- (1) An individual or group based solely on their religious, political, or social views or activities;
- (2) An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation, unless such information is relevant to the individual's criminal conduct or activity, or if required to identify the individual; or
- (3) An individual's age other than to determine if the person is a minor, or to assist in correctly identifying an individual.

All Department personnel must have a valid law enforcement, public safety, or administrative purpose for using software and interacting with data in a database accessible to the Department. Valid law enforcement purposes, include, but are not limited to leadership situational awareness, enhanced officer awareness, suspect identification, witness and victim identification, investigative support, and resource deployment.

All Department personnel are required to complete and agree to the BPD Data Use Agreement prior to accessing any database maintained by the Department. Use is further governed by and subject to the BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy.

3. Data Collection: What Data can be collected by the Technology?

These technologies provide the ability to collect content from publicly available social media and other internet sites. This may include the username, social media handle, text, video, and picture content, emojis, and other types of media that may be linked. The tools may also provide a URL to access the original content on the original site.

Additional information regarding specific applications in use during the year will be included in the Surveillance Ordinance Annual Report for Social Media Analysis Tools.

4. Data Access: What individuals can access or use the collected Data, and what are the rules and processes required before access or use of the information?

Use of the application(s) shall be limited to users authorized by the Department to use the tools in the course and scope of their employment to support the administrative and investigatory functions of the Department. *See also* BPD Rule 322 (Department Property).

Use of Social Media Analysis Tools is limited to a small group of personnel in the BRIC in the Criminal Intelligence and Counterterrorism and Threat Assessment Sections. Each tool is used under close legal guidance and oversight by supervisory personnel. Use of the tool is also reviewed by the BRIC Privacy Committee.

All authorized users must have a valid law enforcement or public safety purpose for using the tools and interacting with data in a database maintained by or accessible to the Department. All authorized users are required to complete and agree to the BPD Data Use Agreement prior to accessing any BPD database. Use is further governed by and subject to the BRIC Privacy Policy.

The Department will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

5. Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, only as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

BPD personnel using these tools will be subject to regular audits to ensure compliance with all policies and procedures.

6. Data Retention:

- a. What time period, if any, will information collected by the Technology be routinely retained?**

- b. Why is that retention period appropriate to further the purpose(s)?**
- c. What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

Authorized users will review the data and information within the tools and determine whether and what action is required, if any, including whether and what documentation and data should be retained and stored within an appropriate BPD database(s).

Social Media Analysis Tools are not generally used as repositories for Department data. Any information gathered from these tools will be stored in the Department's approved applications / databases for investigative follow up. Social Media Analysis Tools are primarily intended to improve efficiency of Department personnel.

Data within BPD-maintained databases is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) (the "Schedule") and BPD Rule 322A (Retention and Destruction of Records and Materials).

Data within BRIC-managed databases is further subject to the retention policy in the BRIC Privacy Policy, Section M (Information Retention and Destruction). In particular, the BRIC will review all applicable information for record retention (validation or purge) at least every five (5) years, as provided by 28 C.F.R. Part 23 (Criminal Intelligence Systems Operating Policies). The BRIC conducts regular reviews and ongoing maintenance to validate or purge information within BRIC-managed databases.

All BPD databases are subject to relevant data retention policies. Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all public agencies in the Schedule.

7. Public Access: How can collected Data be accessed by members of the public, including criminal defendants?

All public records requests will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations. *See also* BPD Rule 307 (Security of Criminal Offender Record Information (CORI)); BRIC Privacy Policy, Section K.1 (Redress - Disclosure).

All media requests will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R.

Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

8. Information and Data-Sharing:

- a. How can other City or non-City entities access or use the Data?**
- b. How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
- c. What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Data?**

When necessary, the Department may issue notification(s) to law enforcement and public safety partner agencies based on threat or other information developed from these tools. Any notification would be consistent with standard practice for similar types of information received and will in all cases be consistent with Federal, State, and Local laws and ordinances. See [BRIC Standard Operating Procedure for Dissemination](#); and [BRIC Standard Operating Procedure for Request for Information Processing](#).

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

9. Training:

- a. What training, if any, is required for any individual authorized to use the Data or technology or to access information collected by the Technology?**
- b. What are the training materials?**

Authorized users receive training and instruction provided by the developers of the applications on the operation of the applications before access is permitted. Authorized users receive ongoing guidance and are subject to oversight by supervisor(s) and legal counsel.

Generally, regarding Department software and databases, authorized users receive training before gaining access to software and databases. The type and manner of training varies based on the complexity and nature of the software, the type and sensitivity of the data and records, and the users' role and responsibility within or relationship to the Department. Training includes, but is not limited to, Boston Police Academy training on report writing and record management system use, training on CORI and CJIS laws and rules, training on Bias-Free Policing and Implicit Bias training. Analysts also receive training on combating implicit bias and use of analytic tradecraft to reduce the impact of bias. Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse

communities they represent. *See* Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

Additionally, all BRIC personnel are trained at least annually on the BRIC Privacy Policy and 28 C.F.R. Part 23, as well as all other relevant BRIC policies and standard operating procedures.

10. Oversight: What mechanisms ensure that the Technology Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?

The Department will ensure use of Social Media Analysis Tools is in compliance with all applicable laws and regulations. When software or databases have embedded audit features, the Department shall conduct audits as it deems necessary to ensure appropriate use. Each tool is used under close legal guidance and oversight by supervisory personnel. Use of the tool is also reviewed by the BRIC Privacy Committee.

If an Authorized User is found to be in noncompliance with the provisions of the Privacy Policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC may:

- Suspend or discontinue access to information by the center personnel, the participating agency, or the Authorized User.
- Apply administrative and/or legal actions or sanctions as consistent with Department rules and regulations or applicable law.
- If the Authorized User is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

Additional details regarding accountability and enforcement are available in the BRIC Privacy Policy, Section N (Accountability and Enforcement).

Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

11. Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Data and technology?

All Boston Police Department use of software and access to databases and data contained therein shall be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. Child Rights: What are the special considerations specific to the Technology and Data pertaining to minor children?

All Boston Police Department use of software and access to databases and data contained therein shall be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

Attachments:

- [Surveillance Technology: Software and Databases, dated August 7, 2022](#) (without attachments)
- [Boston Police Department Data Use Agreement](#)
- [BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy](#) (2024)