

June 5, 2025

City Councilor Ruthzee Louijeune
President
Boston City Council
One City Hall Plaza
Boston, MA 02201

RE: Boston Police Department
"Social Media Analysis Tools"

Dear Council President Louijeune:

Pursuant to Section 16-63.3(b)(3) of the City of Boston Municipal Code (Ordinance on Surveillance Oversight and Information Sharing), I am writing to report the Boston Police Department's use of three "Social Media Analysis Tools." Additionally, attached please find the "Surveillance Use Policy" questionnaire and the relevant Department policies that govern the use of these tools.

Like all Department resources, including all Software and Databases, these analysis tools are used only for valid law enforcement purposes. Specifically, "Social Media Analysis Tools" are used to gather timely information in furtherance of preventing criminal activity, to support criminal investigations and intelligence development (including suspected terrorist related activity), and to identify and evaluate current emerging threats.

Use of these tools is subject to legal oversight and guidance and in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, BPD policies and procedures and the Boston Regional Intelligence Center (BRIC) Privacy, Civil Rights, and Civil Liberties Protection Policy.

From January 2023 to date, the Department has utilized the following "Social Media Analysis Tools" as described above:

1. "SourceFeed" and "Search Feed" Databases

In May 2023, the Department accessed "SourceFeed" and "SearchFeed" Databases maintained by SITE Intelligence Group (SITE) for a short trial period, under exigent circumstances. Beginning in February 2025, the Department has access to SITE Intel Group SourceFeed - Global Jihadist Threat and SITE Intel Group SearchFeed. These databases are used by a small number of personnel assigned to the Counterterrorism and Threat Assessment Section in the BRIC, with supervisor oversight and legal guidance, to detect and review online threats.

SITE provides access to searchable databases that contain content from online forums utilized by domestic violent extremists (DVEs), foreign terrorist organizations (FTOs), and those inspired by FTOs. Within the current threat environment, key focus areas include the DVE sub-categories of racially or ethnically motivated violent extremism (RMVE) and anti-government or anti-authority violent extremism (AGAAVE), as well as the FTO sub-category of global jihad-inspired violent extremism. SITE's methodology of targeted collection through the use of human experts ensures that content within online forums is not indiscriminately collected and confirms that the content contains violent rhetoric or is associated with these extremist or terrorist groups.

To date, use of this tool has aided the BRIC's analysis and investigative activity in several ways. On a daily basis, it has provided additional context and leads in counterterrorism investigations into foreign terrorist organizations, including translation capabilities, access to specific content in non-searchable platforms and often changing group discussion boards, and the ability to filter international content to those with a more direct nexus to the New England area and Boston specifically. Awareness of this content allows adjustment of the Department's security posture to protect the City more effectively.

Specifically, the tool assisted with the investigation of threats to local elected leadership that resulted in the recovery of dozens of firearms and a significant amount of ammunition, and provided context to analysis of locally active RMVE groups, including the identification of a newly formed group. Additionally, the tool aided in identifying an attempt to dox an individual affiliated with a local religious group, which was then followed up on to ensure the safety of the individual and religious group.

2. Chorus Intelligence Suite

Beginning in October 2024, the Department utilized Chorus Intelligence Suite (CIS) under exigent circumstances for approximately 30 days. In the weeks leading up to the November 2024 National Elections, the threat environment nationally and in Boston necessitated the exigent use of this tool. The Department in good faith reasonably believed that the volume of online content related to election events would be high during this period, requiring efficient review of threat information that could impact the Boston Metro Area beyond existing personnel resources.

Beginning in February 2025, the Department has access to the Chorus Intelligence Suite. Use is limited to a small group of personnel in the BRIC, with supervisor oversight and legal guidance.

Chorus Intelligence Suite consists of tools and capabilities for gathering data from open source (i.e., publicly available) data sources coupled with capabilities to analyze the data. CIS provided analysts the ability to locate an individual's open source social media profiles by searching based on name, phone number or a social media handle. This tool is limited to open source, publicly available information.

Use of this tool thus far has aided investigations into violent groups, sexual assault and human trafficking related criminal activity, including the identification of leads related to suspects engaged in this activity.

3. Tangles

Beginning in October 2024, the Department also utilized Tangles, maintained by PenLink, under exigent circumstances as described above for approximately 30 days.

This tool was utilized by a small group of personnel from the BRIC, with supervisor oversight and legal guidance, for workups of individuals involved in criminal investigations. Tangles provided analysts the ability to locate an individual's open source social media profiles by searching based on name, phone number or a social media handle.

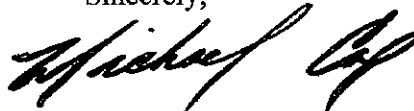
The Department does not currently have access to this tool.

Conclusion

"Social Media Analysis Tools," like those described above, are necessary tools for law enforcement to detect, prevent, and investigate criminal activity. These tools improve personnel efficiency and increase analytic accuracy when reviewing these large datasets, while also protecting individuals' privacy, civil rights and civil liberties.

Please do not hesitate to contact me with any questions you may have. Thank you.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Cox", with a stylized flourish at the end.

Michael A. Cox
Police Commissioner

Department: Boston Police Department
Submitted by: Boston Police Department
Date: June 4, 2025

Technology: Social Media Analysis Tools

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 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).

The Department has access to the following social media analysis tools:

- **SITE Intel Group SourceFeed - Global Jihadist Threat and SITE Intel Group SearchFeed**
- **Chorus Intelligence Suite**

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.

All authorized users 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 authorized users 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?

SITE: SITE provides access to searchable databases that contain content from online forums utilized by domestic violent extremists (DVEs), foreign terrorist organizations (FTOs), and those inspired by FTOs. Within the current threat environment, key focus areas include the DVE sub-categories of racially or ethnically motivated violent extremism (RMVE) and anti-government or anti-authority violent extremism (AGAAVE), as well as the FTO sub-category of global jihad-inspired violent extremism. SITE's methodology of targeted collection means that collected content has been confirmed by human experts to contain violent rhetoric or is associated with these extremist or terrorist groups, and online forums are not indiscriminately collected.

Chorus: Chorus Intelligence Suite (CIS) consists of tools and capabilities for gathering data from open source data sources coupled with capabilities to analyze the data. CIS provided analysts the ability to locate an individual's open source social media profiles by searching based on name, phone number, or a social media handle. This tool is limited to open source, publicly available information.

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 SITE and Chorus 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 monthly 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.

Information will be accessed and analyzed only to:

- Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the Department.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

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).

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 quarterly reviews and ongoing maintenance to validate or purge information.

Each database is 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) and the Public Record Law (PRL)).

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.

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. 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 monthly 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)

DATA USE AGREEMENT

New Hire ☒ Intern ☐ Contractor ☐ Special Officer ☐ Other (Describe below) ☐ Renewal ☐

This Agreement is entered into effective as of _____ between the Boston Police Department ("Department") and _____ ("Recipient").

As a condition to and in consideration of the Department's allowing access to confidential information within the Boston Police Department Network, as well as BPD Record Management System ("RMS") to Recipient, Recipient agrees to the restrictions and undertakings contained in this Agreement.

Recipient hereby acknowledges that he/she is employed by _____, an organization to which he/she is in good standing. Recipient agrees (1) not to disclose any information that can be accessed when logged into any Boston Police Department system/RMS, with the exception of information contained in incident reports authored by the Recipient, unless for legitimate law enforcement purposes; (2) to identify himself/herself within the narrative of authored incident reports; (3) not to view or access information which he/she has not been granted access and to immediately notify the Department in the event of any unauthorized or improper use or disclosure of the information contained within any BPD system/RMS; and (4) to renew this Agreement with the Department annually.

Recipient hereby acknowledges that unauthorized disclosure or use of confidential information could cause irreparable harm and significant injury, which may be difficult to ascertain. Accordingly, Recipient agrees that the Department shall have the right to seek and obtain immediate injunctive relief from breaches of this Agreement, in addition to any other rights and remedies it may have.

This Agreement shall bind and inure to the benefit of the parties hereto, except that confidential information available within any BPD system/RMS and the rights and obligations under this Agreement may not be assigned by Recipient without prior written consent of the Department. This document contains the entire agreement between the parties with respect to the subject matter hereof, and may not be amended, nor any obligation waived, except by a writing signed by both parties hereto. Any failure to enforce any provision of this Agreement shall not constitute a waiver. This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of Massachusetts and the parties hereto agree to submit to the exclusive jurisdiction of the courts of Massachusetts any disputes arising out of the subject matter.

UNDERSTOOD AND AGREED:

Recipient Signature:

Date:

Name:

Telephone Number

Company:

Email Address

BPD Sponsor Name

BPD Sponsor Signature

BPD Sponsor Phone #

Approved ☒

Denied ☐

Reason _____

BPD Technology Services Signature

Date.

DATA USE AGREEMENT

INTERNS ONLY

Below indicate the dates of internship. Your access will be terminated upon internship end date. Any change of date must be approved by a supervisor and the appropriate parties must be notified in order to maintain access.

Start Date _____

End Date _____

Check the application(s) you request access to and the reason for the access. Some applications will require additional training and/or certification before access can be granted.

Application Name	Reason for Access	Additional Requirements
<input type="checkbox"/> CAD/NetViewer		CJIS Certification
<input type="checkbox"/> Mark43		Mark43 Report Writing Training
<input type="checkbox"/> Booking Applications		CJIS Certification
<input type="checkbox"/> CJISweb		CJIS Certification / NexTEST
<input type="checkbox"/> Gateway Applications (Please Describe)		
<input type="checkbox"/> Other (Please Describe)		

All persons who may have physical or logical access to Criminal Justice Information (CJI) must complete Criminal Justice Information System (CJIS) security awareness training and pass the Level 4 CJISonline exam. Any person needing direct access to a CJIS terminal must complete CJIS training at the Boston Police Academy and pass the CJIS nexTEST exam for CJIS credentials. CJIS training will be coordinated by ISG when required.