



September 20, 2022

The Honorable Mayor Michelle Wu

Via email

Re: Request for Additional Information Pursuant to the Ordinance on Surveillance Oversight and Information Sharing

Dear Mayor Wu,

As you know, the Surveillance Oversight and Information Sharing ordinance that was unanimously approved by the City Council last year went into effect in August 2022. As required by the ordinance, your administration submitted various Surveillance Use Policies ("SUPs") and other supplemental information pertaining to the surveillance technologies currently in use by the Police Department, Office of Emergency Management, Parks Department, Housing Authority, Municipal Services, and Public Schools. The ordinance requires that the City Council vote to approve or deny authorization for continued use of these technologies. The Council may also request additional information or policy changes before deciding whether to approve or deny technologies and policies.

On September 14, we met with members of your staff, City Councilor Michael Flaherty, and other advocates to discuss your administration's initial submissions and ordinance implementation generally. At that meeting, we thanked the administration for the hard work you have done to comply with the ordinance—thanks we are happy to echo in writing. We also said that our review of the materials left us with additional questions about surveillance technologies in use in Boston today, and we discussed some concerns with existing policy as presented to the council. We agreed that we would follow up, in writing, with specific requests for additional information and some policy suggestions.

The purpose of this letter is to request additional information from the administration for City Council and public review. A subsequent letter will lay out some recommendations for policy improvements.

Seeking further information about surveillance technologies

Across the board, we identified that most of the submissions lack the following information:

- For those surveillance technologies that involve the use of multiple devices (e.g., surveillance cameras, ShotSpotter sensors, etc.), the policies should provide:
 - The locations of each device; and
 - The total number of devices owned or accessed by the city and whether they are in use or ready to be used;
- The number of employees from each department that can access surveillance data produced by each surveillance technology, including information about whether that access is granted via a web-based log-in system or by individual request;
- The number of people from non-Boston agencies (including BRIC consultants and federal agents assigned to BRIC, or federal task forces) that can access surveillance data produced by each surveillance technology, including the name of each agency and information about whether that access is granted via a web-based log-in system or by individual request;
- Contract dates and costs, including the price per unit when the surveillance technology includes different units of the same general type of device (e.g., surveillance cameras), and the cost of software, installation, and updates, if applicable;
- A brief description of the process by which the city acquired the surveillance technology, including the source of the money used to pay for the technology (e.g., regular budget process, civil asset forfeiture, nonprofit donation like the Boston Police Foundation);
- All training materials for each technology, including those authored by third-party vendors;
- Information pertaining to how many individuals have faced disciplinary consequences, and what disciplinary consequences were imposed, for violating departmental or municipal policies relating to records access and retention pertaining to each technology or data system;
- The time period that the surveillance technology has been in use by the department reporting it; and
- All completed audits pertaining to surveillance technologies, databases, or data, and any schedules or policy pertaining to future audits.

Additionally, we respectfully request the following additional information about specific technologies:

Surveillance Cameras

The materials provided by the City did not provide a clear overview of the surveillance camera networks controlled or accessed by the Boston Police Department. It would be extremely helpful to have a document that lays out clear details about every camera remotely accessible to *or* owned by the BPD, including but not limited to those in the Critical Infrastructure Monitoring System (CIMS). This information should include:

- The number of cameras in each system, broken down by agency (e.g. MassDOT, MBTA, State Police, Boston Housing Authority, Parks Department, federal agencies, etc.);
- The location of each camera;
- Rules relating to the retention and sharing of video data for each system;
- All available details about the technology (camera type and features, video analytics tools, etc.);
- A full accounting of all external entities that have access to the cameras or camera systems (for example, the Massachusetts State Police, other local police, the FBI, etc.); and

- Information about who within and outside BPD can access the cameras, how, for what reasons, and from what kind of devices (e.g. cell phones, department issued laptops, personal computers, etc.).

Software and Databases (BPD)

BPD provided a list of databases but did not provide any information about what kinds of information are available in those databases, what information BPD provides to which databases, or when or by whom databases can be queried. We therefore respectfully request the following information:

- Exhaustive descriptions of the categories of data that can be accessed via each database (e.g. property records, criminal records, associational information, intelligence data, cell phone location information, license plate reader records, insurance data, credit information, etc.);
- Descriptions of the types of data BPD contributes to each database;
- The number of people that have access to these systems and information about their positions;
- The costs associated with each database system;
- Information about how access is granted to database systems;
- Information pertaining to the logging and auditing of database searches (for each database), including whether it is internally or externally audited, how often it is audited, and whether records have previously been purged; and
- All CJIS audits.

BriefCam (BPD)

- A SUP for this technology that includes the specific version of the software the city possesses;
- Any details about rules or processes in place to prevent facial recognition from being added to the software, as required by city law;
- A full accounting of all persons authorized to access the software;
- Specific limitations on how and when BriefCam can be used, and by whom;
- Information about logging and auditing capabilities associated with BriefCam searches; and
- A description of the software's capabilities and how BPD uses it.

Audio and Video Devices - Recording and Non-Recording (BPD)

- The BPD supplied a non-exhaustive list of these devices. Please provide an exhaustive list.

Mayor Wu, thank you for your leadership in pushing for the adoption of this important ordinance, and for your administration's hard work to implement it. We look forward to continued collaboration with the City of Boston and the City Council to bring effective oversight, transparency, and accountability to all surveillance operations in Boston. Thank you for your public service and commitment to ensuring meaningful democratic control and oversight of government surveillance in our city.

Fatema Ahmad
Muslim Justice League
fahmad@muslimjusticeleague.org

Kade Crockford
ACLU of Massachusetts
kcrockford@aclum.org

Alex Marthews
Digital Fourth
digitalfourth@protonmail.com

Cc: Boston City Council, Tali Robbins