

## **Surveillance Ordinance Hearing - Jul 31, 2024**

Below please find responses to the information request submitted by the ACLU, dated July 23, 2024, regarding the technology used by the Boston Police Department and detailed in the Surveillance Ordinance annual report.

1. Information about whether BPD surveillance cameras capture sound.

As previously reported, the cameras on the BAT Camera System and the DoIT/BTD Camera System do not capture or record audio.

2. License plate reader surveillance system.

The Department reported: "As of December 31, 2023, the Department operates fewer than ten License Plate Readers." Further public disclosure and specificity as to the precise location of the LPRs - particularly where they are not widely deployed - would compromise their utility.

3. Surveillance camera network.

### *Locations*

As of July 29, 2024, there were 1153 cameras deployed on public streets in Boston in the following districts:

A1 (Downtown Boston):	430 Cameras
A7 (East Boston):	5 Cameras
A15 (Charlestown):	44 Cameras
B2 (Roxbury):	182 Cameras
B3 (Mattapan):	85 Cameras
C6 (South Boston):	86 Cameras
C11 (Dorchester):	139 Cameras
D4 (South End):	131 Cameras
D14 (Brighton):	9 Cameras
E5 (West Roxbury):	9 Cameras
E13 (Jamaica Plain):	23 Cameras
E18 (Hyde Park):	2 Cameras
Harbor:	8 Cameras

In addition to the above referenced cameras, there are approximately 150 cameras located in and around department facilities to secure the infrastructure and surrounding property.

*Comprehensive data showing how often surveillance camera footage was instrumental in leading to arrests, prosecutions, or convictions, and for which types of criminal cases.*

## **Surveillance Ordinance Hearing - Jul 31, 2024**

In criminal investigations, camera footage is used in a vast number of cases and is an invaluable tool used by investigators in the aftermath of a crime to identify and apprehend a suspect and by prosecutors in the course of a criminal prosecution. While we don't collect the information specifically requested, every investigation starts by determining whether or not camera footage of the incident exists, either through BPD cameras, private cameras or both. Camera footage is a key element to establishing the movements of both victim and suspect before, during, and after incidents and is often compelling evidence when determining what occurred. In the follow up investigation, investigators will routinely expand that search for cameras when trying to piece together the movements of suspects either before or after an incident. This again will involve BPD cameras, private resident cameras, transit cameras and commercial locations. This evidence is then provided in nearly all, if not all, criminal prosecutions and relied upon when seeking a conviction.

The investigative value of cameras can be seen in the shooting incident earlier this week in Jamaica Plain where officers were able to view footage of the incident, identify the direction of flight of the suspect and make an arrest shortly thereafter.

On the contrary, the lack of cameras in an area can result in investigative delays and potential unsolved crimes.

### **4. Cell-Site Simulator.**

Each use of the cell site simulator must be approved by the Commander of SIU (Special Investigations Unit) and/or BIS (Bureau of Investigative Services) Commander. Only SIU personnel can operate the cell-site simulator and can only do so with internal approval and either a search warrant or exigent circumstances.

In 2023, the cell-site simulator was deployed two times, both under exigent circumstances, as described in the Annual Report. On one occasion, the equipment was used during an investigation and resulted in the apprehension of an individual wanted on an outstanding arrest warrant for armed robbery. During an unrelated investigation, the equipment was used to confirm the location of a suspect in an aggravated assault incident.

While the cell-site simulator is in use, the simulator searches for a specific electronic device. The search is limited to the target phone's known phone service carrier (*i.e.*, AT&T, Verizon, etc.), within an identified band, and within a defined tower in a precise geographic area. The cell-site simulator collects a list of unique electronic identifying numbers; for example, International Mobile Equipment Identity (IMEI) number or International Mobile Subscriber Identity (IMSI). The cell-site simulator does not collect phone numbers, subscriber info, or any contents from a cell phone. The target phone's unique electronic identifying number(s) are compared to those collected to ascertain location.

After each use of the cell-site simulator, all data - that is, the list of unique electronic identifying numbers - is deleted.