

APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT

Department or Division:	Somerville Police Department (SPD)
Compliance Officer (name and position):	Lt. Jeff DiGregorio
Submitted by:	Lt. Jeff DiGregorio
Date:	
Surveillance Technology:	BriefCam

X	Please identify the purpose(s) of the proposed surveillance technology. Select ALL that apply by entering "X" in the left column.
x	Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property
x	Identifying, apprehending, and prosecuting criminal offenders
x	Gathering evidence of violations of any law in criminal, civil, and administrative proceedings
x	Providing information to emergency personnel
	Documenting and improving performance of City employees
	Executing financial transactions between the City and any individual engaged in a financial transaction with the City
	Preventing waste, fraud, and abuse of City resources
	Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property
	Enforcing obligations to the City
	Operating vehicles for City business
	Analyzing and managing service delivery
	Communicating among City employees, with citizens, or with third parties
	Surveying and gathering feedback from constituents
	Other (Describe): If the surveillance technology is used for a purpose not listed above, does the purpose comply with the surveillance use policy? ___ Yes ___ No

Complete ALL of the following items related to the proposed surveillance technology. Be as specific as possible. If an item is not applicable, enter "N/A." Do NOT leave fields blank.

1. Information describing the surveillance technology and how it works:

This is potential new technology. The department does not use this technology at this time.

BriefCam is a program that filters through video such as surveillance, private, and security and pulls out only things requested by investigators. For example, if investigators are looking for a red pick up truck, the program will filter all other vehicles and show only red trucks. The tool saves investigators hours of time viewing footage and helps resolve cases much faster.

a. Authorized use – the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited (10.64.b.2):

This technology would be used under the direction of a detective supervisor during active criminal investigations only.

b. Training – the training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials (10.64.b.9):

The vendor of this technology offers training programs and will come onsite to train users.

2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1):

This technology only streamlines video already accessible to investigators. It could potentially cut the work hours of an investigation down by several hours or even days.

3. Information describing the kind of surveillance the surveillance technology is going to conduct and what surveillance data is going to be gathered (10.64.b.3):

This technology only filters video that investigators would view for an investigation. It does not surveille per se, only makes use of already surveillance more efficient.

a. Data access – the individuals who can access or use the collected surveillance data, and the rules and processes required before access or use of the information (10.64.b.4):

Only members of the detective bureau, under the direction of a supervisor, could use this technology on specified cases

<p>b. Data protection – the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms; (10.64.b.5)</p>
<p>Only members of the detective bureau under the direction of a supervisor could use this technology. All information would be secured on a department computer only accessible by the investigator.</p>
<p>c. Data retention – the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period (10.64.b.6):</p>
<p>This technology only filters existing methods of reviewing and retaining video footage. It does not surveil per se, only amplifies existing technologies.</p>
<p>d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):</p>
<p>Information discovered via this technology would be subject to discovery rules. All other public information requests would be reviewed by the law office.</p>
<p>e. Third-party data-sharing – if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data (10.64.b.8):</p>
<p>Information would be shared with other city or law enforcement agencies based on the individual event. If there was an exigent circumstance or if there was an investigation that crossed jurisdictional lines information could be shared.</p>
<p>4. The location(s) it may be deployed and when:</p>
<p>This technology would only be used internally to filter existing video footage obtained via private citizens, authorized city cameras, or private security footage.</p>
<p>5. A description of the privacy and anonymity rights affected and a mitigation plan describing how the department’s use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse:</p>
<p>This technology would be case specific and used under the direction of a supervisor. There would be limited</p>

accounts for this technology and would not be open for general use. As this technology is not currently used there is no plan in place to mitigate privacy.

6. The potential impact(s) on privacy in the city; the potential impact on the civil rights and liberties of any individuals, communities or groups, including, but not limited to, communities of color or other marginalized communities in the city, and a description of whether there is a plan to address the impact(s):

This technology only compliments existing video and does not create new surveillance. Any facial recognition features of the program are able to be disabled.

7. An estimate of the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding:

Software is free through UASI however hardware costs are approximately \$10,000 to upgrade the system to support the program.

8. An explanation of how the surveillance use policy will apply to this surveillance technology and, if it is not applicable, a technology-specific surveillance use policy:

Since this technology is used in conjunction with other surveillance technology the surveillance use policy would apply .

- a. Oversight – the mechanisms to ensure that the surveillance 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 surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy (10.64.b.10):

The detective supervisor that authorizes the use of BriefCam will oversee that it is used in compliance of the Surveillance Ordinance. This technology would only be accessed by very few people and under authority of the supervisor so tracking of when it was used will be simple. Due to the very limited number of people who have access to the technology due to licensing restrictions (1-3) it will not be likely to be misused. Due to this technology being used in active criminal investigations it is not viable to have an outside entity oversee use of BriefCam. Sanctions for the misuse of this technology would be department discipline up to and including termination.