# DIGITAL FOURTH

The Massachusetts campaign to protect digital data from warrantless government surveillance

November 17, 2020.

**COMMENTS ON:**

**AGENDA ITEM #209592, APPROVAL OF SURVEILLANCE USE POLICY DRAFT #1**

**AGENDA ITEMS #210788-210791 & 210906, APPROVAL OF SURVEILLANCE TECHNOLOGY IMPACT REPORTS**

***In the interests of a timely submission of our existing comments, our comments on items 210907-210912 will follow tomorrow when we have prepared them.***

Dear members of the Legislative Matters Committee,

Digital Fourth (now the Greater Boston affiliate of nationwide civil liberties group Restore The Fourth), is a volunteer-run civil liberties advocacy group founded in 2012, with particular expertise on surveillance and the Fourth Amendment. We have been involved in the adoption of surveillance ordinances in several Massachusetts communities, including Somerville, and several of our activists are Somerville residents. So, we are particularly concerned to ensure that Somerville's ordinance is implemented in a way that honors your intent in passing it, and that serves as a model to other communities, at a time when Boston has begun hearings on adopting an ordinance partly based on yours.

Unless otherwise noted, Digital Fourth endorses the comments and questions already submitted by the ACLU of Massachusetts and Councillor Ben Ewen-Campen. For questions or concerns on our own detailed comments that follow, please email digitalfourth@protonmail.com, or call us on 617 208-9002.

Sincerely,

ALEX MARTHEWS, Chair.

**AGENDA ITEM #209592, APPROVAL OF SURVEILLANCE USE POLICY DRAFT #1**

First, it appears that what is being submitted for approval by the City Council is a first draft ("1.1") that is almost two years old. It would be surprising if, thanks to this long intervening period, there were no changes that needed to be made.

**Section II.6**

The aim of the Surveillance Use Policy is to set defaults for the use of Surveillance Technologies and for access and use restrictions on the data they generate. In the absence of an approved technology-specific policy, these are the binding constraints. As such, they need to be drafted at a high enough level of generality that they make sense for a broad array of technologies, without being so vague as to not in fact set any constraints on the technology's use.

We believe that the wording on data retention in this section goes too far towards vagueness. It simply says that *"Surveillance Data will not be maintained any longer than is necessary to achieve its approved purpose(s)."* We have several objections to this language.

First, it is not clear from the text that data that is *"not maintained any longer"* will in fact be destroyed. The default should be that "Surveillance Data *will be destroyed*", not that it will "*not be maintained.*" Otherwise, the intent of the Ordinance will be frustrated by having an endlessly growing archive of data that, while no longer maintained, may be accessible to and searchable by city officials, employees and others.

Second, the Surveillance Use Policy should set a default length of time for Surveillance Data retention. The length of time that *"is necessary to achieve its approved purpose"* should not rest only on the subjective determination of the city officials with access to the data. We recommend that in general, such data should be deleted after 90 days. Variations from this for individual technologies may be considered and implemented with City Council approval on a technology-specific basis.

**Section III. Use of Surveillance Technology in Exigent Circumstances**

The provisions relating to exigent circumstances seem loose. In particular:

- There is no limitation placed on the duration of exigent circumstances, and none of the provisions requiring reporting are triggered until ninety days after the exigent circumstances are deemed by the Chief of Police to have ended. That time period may itself be extended an unspecified number of times.

- Redactions to the reports are limited so weakly that effectively, they lie entirely within the *"reasonable discretion"* of the Chief of Police. It is appropriate to allow redactions to comply with court orders, but it is not appropriate to also allow redactions to *"exclude information that, in the reasonable discretion of the Chief of Police, if disclosed, would materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security"*. There is no process identified to review the judgment of the Chief of Police that releasing information would indeed *"materially jeopardize an ongoing investigation"* or that it would *"represent a significant risk to public safety and security."* Given that police departments often, inaccurately, believe that merely disclosing the existence or use of a Surveillance Technology is a *"significant risk to public safety and security"*, the Police Chief may never, for a given technology, reach the point that they believe that *"the reason for the redaction no longer exists."*

**APPENDIX A: Surveillance Technology Impact Report**

Given the initial set of Surveillance Technology Impact Reports, it seems that some clarification may be required on point #6. Instead of "*What are the estimated fiscal costs of the Surveillance Technology, including initial costs, ongoing maintenance and personnel costs, and source of funds?"*, we believe it should read, *"What are all estimated fiscal costs of the Surveillance Technology, including all costs to the City and all costs borne by outside parties such as private donors, 501(c)(3) nonprofits, proceeds of forfeitures, state and federal funds? Please include initial costs, ongoing maintenance and personnel costs, and amounts by source of funds."* This change will make it even clearer to City employees that the City Council wishes to know all sources of funds, not simply the fiscal impact to the City Budget assuming that other sources of funds remain constant. The same point applies to point #7 in Appendix B.

## AGENDA ITEMS #210788-210791 & 210906, APPROVAL OF SURVEILLANCE TECHNOLOGY IMPACT REPORTS

### Agenda Item #210788, Requesting approval of the Surveillance Technology Impact Report for Homeland Security Cameras

For its response to question #7, the report simply reads, *"UASI funds paid for installation and maintenance of the cameras so there is no cost to the city."* The police department should not fail to specify costs simply because those costs are currently covered by another party. The police department should disclose the amount of the UASI grant for (a) installation and (b) maintenance. If this was a past grant, it also cannot be expected to pay for current maintenance, so the City Council cannot tell from this report who maintains those cameras, how much time that takes, and how much of those costs are being covered by received or expected UASI funds. Elements of UASI, such as Urban Shield, are controversial, so it would also be helpful to specify which UASI program in particular is the source of these funds.

The ACLU of Massachusetts and Councillor Ben Ewen-Campen have also identified an array of defects with this STIR. Consequently, we recommend that Councilors not approve this STIR until the defects identified by both us and them are cured.

### Agenda Item #210789, Requesting approval of the Surveillance Technology Impact Report for Green Line Extension Cameras

We echo the ACLU's observation for the responses to questions #5 and #6 that the report makes absolutely no effort to describe or quantify either the privacy impacts from these cameras, or a mitigation plan. Instead, there is a mere statement that they are used to "monitor traffic", which implies that traffic-monitoring cameras have no privacy impacts worth discussing. The same statement appears in the response to question #3.

However, knowing this bare fact does not enable Councilors to understand how invasive the cameras in question are. For example, is the camera resolution high enough to identify license plates? Is it high enough to capture images of drivers? Do the cameras have the ability to be upgraded to use facial recognition, contravening Somerville's

municipal ban? Do they have the ability to pan, tilt or zoom? Or are they simply there to provide a count of how many vehicles pass, so as to mitigate congestion?

In the response to question #7, costs for the equipment and installation are mentioned, but, similarly to the STIR for Homeland Security Cameras, nothing is specified relating to personnel costs for monitoring the camera footage or maintaining the cameras.

Given these defects, we recommend that Councilors not approve this STIR until the defects identified by us, the ACLU of Massachusetts and Councilor Ben Ewen-Campen are cured.

**Agenda Item #210790, Requesting approval of the Surveillance Technology Impact Report for 911.**

Our only concern relating to this STIR is that, in common with other STIRs, the police department believe that only the direct fiscal costs to the City need to be listed. Important as this technology is, even if the equipment is *"owned by the State of Massachusetts"*, the City Council should be aware of how much the provision of these services costs; if only a statewide figure is available, it can be pro-rated based on the number of Somerville residents or based on the percentage of statewide 911 calls that occur in Somerville, as the City deems appropriate.

Since this Report has fewer defects than the others, and the technology has unquestionable benefits for public safety, we recommend the approval of this STIR.

**Agenda Item 210791, Requesting approval of the Surveillance Technology Impact Report for ShotSpotter.**

ShotSpotter is a controversial technology, and in the City of Cambridge, the ShotSpotter STIR went through several iterations before being acceptable to the Cambridge City Council. Unfortunately, this STIR suffers from similar defects to the first iteration of Cambridge's ShotSpotter STIR.

The most critical problem is that the Report consistently misleads the City Council as to the nature of this technology. Officer DiGregorio provides a secondhand report that ShotSpotter believes the inclusion of voices in audio snippets to be *"highly unusual."*

Even if unusual, this technology would conflict with Massachusetts' wiretapping law, meaning that it records people's voices - even if in *"unusual"* cases - without their consent. However, we also doubt that the inclusion of voices in the continuously recorded audio snippets is in fact as *"unusual"* as ShotSpotter reportedly claims.

In a way, ShotSpotter resembles a less sophisticated home Alexa system, where the trigger, instead of "Alexa", is a *"gunshot-like sound"*. The system is continually listening for the trigger, and continually recording in case the trigger happens. The system does not know what it's recording before the trigger, and is perfectly capable of capturing audio that is not gunshots. The ACLU correctly observes that such recordings (of voices) have already been used in prosecutions; we further observe that they have also been used in prosecutions here in Massachusetts.[1] Furthermore, *"gunshot-like sounds"* are not the same as gunshots. It's not only true that, as Officer DiGregorio observes, actual gunshots can be misclassified as firecrackers; it's much more likely, but he does not mention, that firecrackers, a car backfiring or even popping balloons can be misclassified as gunshots, especially in a city that happily, in most years, has no murders.[2] He provides no figures on the scale of these false positives. It's also misleading for him to state that "*human voices and street noise will never trigger the sensor*", because the issue is not that voices will trigger the sensor, but that the continuously recording sensors will incidentally pick up human voices from the time around the gunshot-like sound that triggers the sensor.

Data from such situations can then be made available to investigators, posing a separate privacy risk.

The description of the locations of the ShotSpotter sensors is helpful, as is the statement that the sensors were installed based on crime data from roughly 2010. We should observe that This suggests to us that even if future responses to the ACLU's and

[1] Fraga, B., "ShotSpotter recording of street argument raises potential privacy issues", January 11, 2012, available at https://www.southcoasttoday.com/article/20120111/News/201110339

[2] in 2010 there were 238 violent crimes in Somerville; since then, they have steadily fallen, and in 2018, the most recent year for which figures were available, there were 177. There were no murders in either year. https://patch.com/massachusetts/somerville/fbi-crime-stats-where-somerville-stands

Councilor Ewen-Campen's questions show that ShotSpotter has been used to solve actual crimes, the need for ShotSpotter technology may well be on the wane.

Cities like Charlotte, NC and San Antonio, TX, with much higher crime rates than Somerville, have decided that Shotspotter is a poor investment, partly because the number of false positives led to police wasting time mobilizing for gunfire situations that never existed.[3]

This STIR should be thoroughly redrafted to acknowledge and address the privacy implications, which are much more significant than the STIR currently suggests, and to provide data on false positive rates. Without such information, the City Council is ill equipped to assess whether ShotSpotter is a wise investment for Somerville, and this STIR is very far from being at a point where it ought to be approved.

**Agenda Item #210906, Requesting approval of the Surveillance Technology Impact Report for BriefCam.**

Our first observation is that this Report seeks to deny that BriefCam constitutes surveillance at all, saying that it *"does not surveille per se, only makes use of already surveillance more efficient."* But of course, surveillance technology is precisely that which makes more efficient things that could previously only be done using expensive and laborious methods, such as human observation and paper records. Justice Scalia famously observed that police putting a GPS tracker on a car might be analogized to a more efficient version of what in the 1790s would have required hiding a tiny constable, with "incredible fortitude and patience," in a suspect's carriage; but this resemblance does not make GPS tracker surveillance not surveillance.[4]

---

[3] *See* "ShotSpotter boss defends system", November 13, 2020, Charlotte Observer, *available at* https://www.charlotteobserver.com/news/local/crime/public-safety-blog/article60938427.html; "San Antonio police cut pricey gunshot detection system", August 16, 2017, San Antonio Express-News, *available at* https://www.expressnews.com/news/local/article/San-Antonio-police-cut-pricey-gunshot-detection-11824797.php.

[4] "Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner … The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience." Scalia, A., writing for a

In fact, the City's existing surveillance cameras were installed subject to a set of unstated assumptions that BriefCam's software violates. It was not assumed when they were installed that the footage would always be monitored by an untiring digital eye, or that the footage would be infinitely exploitable for police purposes. BriefCam offers the police a level of power over that footage that has never been seen before in this City.[5]

In the response to question 3c. (data retention periods), the STIR does not address data retention periods at all, but simply presumes that the retention period of camera footage newly exploitable by BriefCam software should be the same as the unexploitable footage previously held by the camera. Since BriefCam makes the existing footage a quantum leap more intrusive, this assumption is unsafe. If the City Council takes the unwise decision

In the response to question 3e. (data sharing with other agencies), the STIR says, *"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."* This sharing of information will likely fall foul of Somerville's facial recognition ban. Footage could be shared with jurisdictions or agencies without a ban, facial recognition could be applied to the footage, and then the footage reshared back to Somerville PD, rendering the ban a dead letter. This response must be revised and clarified to exclude this possibility.

In the response to question 5. (description of privacy impact and mitigation plan), the STIR says, *"There would be limited 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."* The fact that this is not a tool proposed for general public use scarcely addresses the privacy impacts from the actual use of the technology, which are not addressed. And the essence of passing an Ordinance is that *before* a technology is deployed, police must develop an actual plan to mitigate privacy impacts in the context of that deployment. What Officer DiGregorio appears to be asserting here is that there are no privacy impacts to the general public, and so no plan is necessary to mitigate them. We believe that this software should not be deployed, and believe that there is

unanimous Supreme Court in US v. Jones, 2012, available at https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

[5] See BriefCam's highly disturbing promotional video here: https://youtu.be/EkB6_0Y9WgM.

no way to adequately mitigate its privacy impacts if it were deployed, though reducing data retention limits on all surveillance cameras in the City to 24 hours or less might conceivably maintain some residuum of the prior balance between police powers and residents' freedom.

The response to question #7 shares the limitations of other STIRs' responses, in that it covers only the direct cost to the City of hardware upgrades, not the cost of personnel to monitor or maintain the system.

The response to question #8 reads, in substance, *"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."* This response fails to grasp that privacy impacts do not only occur if external third parties such as hackers obtain access to police surveillance technology. We are centrally concerned with misuse of this technology by the police themselves. The fact that the agents of government provided with this extraordinary power are few in number, does not remove the risk that those agents will abuse it, and increases their ability to conspire in secret to do so. The extraordinary nature of the power requires that even though it is used in active investigations, there must be some outside entity overseeing its use.

We recommend that if this technology is adopted – which we strongly oppose – there also be a permanent, staffed Privacy Commission in Somerville, on the model of that created in Oakland, California; that the Commission be tasked with receiving monthly, detailed reports on the use of BriefCam; and that any violation of the City's Ordinance with respect to BriefCam be classified as a misdemeanor.