Madalyn Letellier

From: Alex Marthews <[redacted]>
Sent: Thursday, March 12, 2026 12:19 PM
To: Public Comments
Subject: Comments of Digital Fourth on 2026 Annual Surveillance Report
Attachments: Comments of Digital Fourth on 2026 Somerville Annual Surveillance Report 2026-03-11.pdf; Comments of Digital Fourth on 2026 Somerville Annual Surveillance Report 2026-03-11.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Dear members of the City Council,

Please find attached our comments on the 2026 Annual Surveillance Report, which is on the agenda for this evening's City Council meeting, for expected referral to Legislative Matters.

As a result of significant privacy issues with the technologies, and significant and recurring failures of Somerville PD to provide key information to Councilors, we are recommending that the City Council should revoke approval of **GrayKey**, **Pole Cameras** and **ShotSpotter**; and that you send back for correction the Surveillance Technology Impact Reports for **Covert Device Cameras**, **GLX Cameras**, **Homeland Security Cameras**, **Fire Station Exterior Cameras** and the **Parking Department Safety Sticks**. We have no objection to the remaining six technologies in the Report, but we do have concerns that some technologies Somerville PD uses that ought to be in the Annual Surveillance Report, like the BRIC Omega Dashboard, are missing from it.

Best wishes
Alex.

Alex Marthews
Co-Chair, Digital Fourth
[redacted]
Digital Fourth is a local chapter of national civil liberties advocacy group Restore The Fourth.

------- Forwarded Message -------
From: Alex Marthews [redacted]>
Date: On Thursday, March 12th, 2026 at 12:02 PM
Subject: Comments of Digital Fourth on 2026 Annual Surveillance Report
To: [redacted]

> Dear members of the City Council,
>
> Please find attached our comments on the 2026 Annual Surveillance Report, which is on the agenda for this evening's City Council meeting, for expected referral to Legislative Matters.
>
> As a result of significant privacy issues with the technologies, and significant and recurring failures of Somerville PD to provide key information to Councilors, we are recommending that the City Council should revoke approval of **GrayKey**, **Pole Cameras** and **ShotSpotter**; and that you send back for

correction the Surveillance Technology Impact Reports for **Covert Device Cameras**, **GLX Cameras**, **Homeland Security Cameras**, **Fire Station Exterior Cameras** and the **Parking Department Safety Sticks**. We have no objection to the remaining six technologies in the Report, but we do have concerns that some technologies Somerville PD uses that ought to be in the Annual Surveillance Report, like the BRIC Omega Dashboard, are missing from it.

Best wishes
Alex.

Alex Marthews
Co-Chair, Digital Fourth
[redacted]
Digital Fourth is a local chapter of national civil liberties advocacy group Restore The Fourth.

DIGITAL FOURTH

The Massachusetts campaign to protect digital data from warrantless government surveillance

Somerville City Council

93 Highland Ave.

Somerville, MA 02143

March 11, 2026

RE: COMMENTS OF DIGITAL FOURTH ON 2026 SOMERVILLE ANNUAL SURVEILLANCE REPORTS

Dear members of the Somerville City Council,

Digital Fourth is a local, volunteer-run civil liberties group, founded in 2012, and active on the issue of government surveillance. We have participated extensively in the development, passage, and implementation of the City's Surveillance Ordinance. Since that passed in 2021, we have provided regular comments to the City Council and the Legislative Matters Committee on the surveillance technologies operated by City agencies. We have also advised members of the City Council and Mayor Wilson on ways to Constitutionally limit ICE raids in the City.

We are grateful for the City's steady commitment to preserving the privacy of Somerville residents by refusing to deploy automated license plate readers. Somerville has therefore wisely avoided the confused and inept rollout of Flock Safety in other nearby municipalities, culminating in Boston having to pause, and Cambridge having to revoke its Flock Safety contract in December 2025.

In 2024, we advised the City Council to not approve Surveillance Technology Impact Reports ("STIRs") not containing information on the costs of the technologies in question, or an honest assessment of disparate impacts as required under the Ordinance. It is still not the general practice of the City's departments to actually identify and state the costs of the surveillance technology, both at acquisition, and in terms of ongoing costs for maintenance, training, license renewals and staff time. Some STIRs fail even to identify the equipment vendor (like the "Safety Stick", which is manufactured by MPS). We have also steadily advised in particular that the City's deployment of ShotSpotter is ineffectual, invasive, and unfair to the residents of East Somerville.

Here's our analysis of the individual technologies in the Report. We believe that this Report as a whole will be referred to the Legislative Matters Committee, and we look forward to providing detailed feedback to that Committee as they evaluate the appropriate recommendations for the Council as a whole.

Surveillance Technology Impact Reports to be rejected [3]:

[Police Department:] GrayKey

Captain Sheehan's reports regarding this intrusive technology continue to be gravely deficient. As a result, we are recommending rejection of this STIR. In 2021, we recommended against GrayKey deployment. In 2023, we supplied a nine-page analysis again recommending rejection of the use of GrayKey, including a detailed analysis of what was missing from the STIR and how it could be improved. In 2024, we reiterated this analysis. Somerville PD, in response, has adopted none of our suggestions for improving this STIR, despite the fact that the Ordinance envisions a process where Somerville PD does iteratively improve their reporting to Council. Instead, with the City Council annually approving this STIR no matter how deficient it is, the information provided in it has steadily thinned relative to 2021-2023.

Poor explanation of the technology:

Captain Sheehan explains:

> *"GrayKey is a digital forensic tool that enables the Somerville Police Department Digital Forensic Unit to bypass encryption on locked Android and IOS devices. The devices accessed would only be accessed in accordance with a duly issued search warrant or consent from the owner of the device. The type of data extracted from the digital devices includes, but is not limited to, digital pictures, videos, text messages, call logs and any other data which would normally be stored on a digital device which could be used in a criminal investigation."*

This question is intended for the applying agency to provide to Councillors an accessible explanation of how the technology works. Instead, Lt. Sheehan focuses on the legalities of using the technology, which is interesting but only supplemental to explaining the technology and how it works. We believe that the City Council would benefit from such an explanation, which would also show that the Police Department themselves understand how the technology they're proposing for approval works. We believe that a response to this question that would be complete, and that would also show that Somerville PD's use of the technology would satisfy standards of Constitutional policing, would read something like as follows:

> "*GrayKey is a digital forensic tool that enables the Somerville Police Department Digital Forensic Unit to bypass encryption on locked Android and IOS devices.* GrayKeys are sold by GrayShift Technologies, now part of Magnet Forensics (link). GrayKeys are focused on obtaining photographic evidence from Computers, Mobile Phones, Digital Cameras, Tablets and any device used to communicate, store data and facilitate the commission of crimes, for which the password, pattern or fingerprint access is unknown, though they can also provide law enforcement access to *digital pictures, videos, text messages, call logs and any other data which would normally be stored on a digital device which could be used in a criminal investigation*. We have used them in the past, and intend to use them in the future, in the context of criminal investigations, to unlock devices of criminal suspects when consent is unavailable or has been refused, or in some cases, with the suspect's consent, to conveniently conduct a deeper and more forensic examination of a phone's contents. A valid search warrant, based on probable cause and issued by the appropriate jurisdictional Massachusetts Court, or a valid consent to search, is required in order to legally extract the evidence from the device. Through the Urban Area Security Initiative (UASI) Boston Office

> the SPD has acquired a License for the GrayKey Digital Forensics Analysis Tool and a Laptop computer which is used to analyze the data extracted from these devices. Our use of the GrayKey is also bound by the Attorney-General's Guidelines (link) and the relevant laws of the Commonwealth (link). We use a further premium add-on service, "Magnet AXIOM", which allows users to search for photos in the whole filesystem of the phone, and to confirm their provenance via hash matches."

At Council in 2024, Legislative Matters Committee Chair Davis and Councilor J. T. Scott "both requested that detail about storage, security (both physical and digital) and access protocols for the tech be added to the report", and we endorsed those calls. Unfortunately, the Police Department continues to fail to address these deficiencies.

No explanation of costs

As was the case previously, the 2026 GrayKey Surveillance Impact Report has provided you with no details on costs, this time simply saying "None." In discussion in Council, though not in the report itself, Lt. Mitsakis disclosed in 2024 that the license type sought for GrayKey "is the one that costs $38,000." This premium offering from GrayKey requires no Internet connection and has no limit to the number of unlocks. It is also the express intent of the Ordinance to consider costs in addition to the direct cost of acquisition to the City or Somerville PD. GrayKey has costs associated with annual training courses for the detective and the supervisor; staff time involved in attending those courses; and proportional costs of participation in the UASI grant process. If the City Council were not to approve the use of a GrayKey, those training costs would no longer be incurred, and the staff time would presumably be spent on other non-GrayKey-related investigative activities.

Repeated refusal to address the key issue of over-seizure of data

None of Somerville PD's responses in the Surveillance Technology Impact Report have ever addressed a key question, namely, what happens to device data that the GrayKey gives access to that is not relevant to a particular investigation? In the original Surveillance Use Policy for this technology, then-Lt. Sheehan specified, "*The technology cannot be used to collect personal information unrelated to the investigation. The information gathered must be relevant to the investigation as indicated in the search warrant."* But that's simply not true. GrayKey images the entire device. There is then a process on the part of the police department, which is not explained or described in any way, to identify and segregate information "relevant to the investigation as indicated in the search warrant." What happens to the *other* information collected? If it is destroyed before being used or shared, then there's no problem. If it is retained, then how long for? Is that data exploited by Somerville PD, and if so, in what circumstances? Have there been instances where evidence of a different crime has been uncovered by a GrayKey search; if so, was a separate warrant obtained for that data, and was that crime prosecuted? Have there been instances where embarrassing data that is not immediately evidence of a different crime, has been used to pressure an individual, for example, to take a plea, to become an informant, or to do other favors for law enforcement? Does Somerville PD also analyze the whole pattern of location data contained in the phone and cross-reference it with other crimes, or probe through the photo gallery to find evidence of other criminal activities not specified in the warrant, or delve into the list of contacts to find potential contacts of the suspect who are also suspected or convicted of crimes or who are listed as "gang associates" or "gang members"? Are there any limitations as to the type of criminal investigations for which a GrayKey would be used? For example, does any stated policy or practice preclude Somerville PD from arresting a protester for disorderly conduct or resisting arrest, and then using a GrayKey to hack into their phone and map out their contacts for further

investigation, or find compromising information unrelated to the investigation that would pressure that protester to become an informant or plead guilty?

Our phones contain evidence relating to our whole lives; police should not be able to use a GrayKey to bypass someone's password and gain full access to every part of their life for close digital review, simply because that person is suspected in a particular crime. The question of the admissibility and constitutionality of such "over-seized" data is a ferociously contested one in Fourth Amendment jurisprudence. We have now raised these issues in the context of the City of Somerville's use of GrayKey for five years. It is time for Somerville PD to address them.

No provision of training materials

Contrary to the specific language of the Ordinance, Somerville PD has consistently refused to provide the actual training materials for GrayKey. Despite our comments and requests, councilors don't even have a description of what is in the training materials, the number of hours spent in training, or the entities providing the training. Whether or not the trainings contain anything disturbing, this repeated failure, over the course of years, to answer this question disrespects the Ordinance and the Council. If there are training materials, Somerville PD must supply them; if not, Somerville PD should state that they do not exist. The question of the content of officer training is often key to the question of whether they have exceeded their authority.

[Police Department] Pole cameras

This STIR significantly misstates the state of the jurisprudence governing the use of pole cameras by law enforcement. Captain Sheehan wrongly states, "Pole cameras are installed in *public areas where there is no expectation of privacy."* As of, perhaps, twenty years ago, this was an accurate depiction of the law. However, during the 2010s, the Supreme Court, in three decisions (*Jones*, *Riley* and *Carpenter*), explored situations where law enforcement used digital surveillance to monitor people in public, and where nevertheless the Supreme Court found that there was sometimes a reasonable expectation of privacy in public areas. In particular (condensing a great deal of legalese here), surveillance that occurred for a long enough period for law enforcement to be able to discern the "patterns of life" of residents, was a search under the Fourth Amendment. On pole cameras in particular, the ruling in *U.S. v. Moore-Bush,* in our First Circuit Court of Appeals, is binding. That ruling decided whether the pole camera evidence should stay in on other grounds, but then split evenly across two concurrences on the Fourth Amendment issue of whether people had a reasonable expectation of privacy in police monitoring of the curtilage of their home over an eight-month period, and therefore whether that monitoring constituted a search requiring a warrant. Captain Sheehan does the Council a disservice, then, by presenting the law as unambiguously on the police's side when it comes to pole cameras. We have repeatedly, in this surveillance ordinance process, alerted the City Council and Somerville PD to these precedents.

Beyond this serious misstatement, the STIR is also thin to the point of contempt for the Ordinance in several other respects. Captain Sheehan writes, in response to the question of whether pole cameras have been effective, "Pole Cameras have been effective in assisting the SPD during the course of investigations." He doesn't bother with details or examples; he gives no figures that would enable City Council independently to assess his bare claim. He might as well have just written "Yes." Perhaps that will come next year, after the City Council approves this STIR and thereby shows that they don't expect examples or details as the price of approval. Regarding costs, instead of following the clear language of the Ordinance and specifying "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", he simply says, "All costs associated with

this technology are covered by UASI." That's not what the question asks. The intent of the Ordinance on costs is to enable the City Council to determine annually how much is being spent on surveillance in the City, whether that money is covered by the municipal budget, by an external government grant, via a gift from a police foundation, or via a gift from a billionaire. By that means, they can gain insight into how City Departments avoid municipal scrutiny while creating their own ecosystem of surveillance technologies. When Captain Sheehan is asked, "Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the city are disproportionately impacted by the deployment of the surveillance technology", he simply says, "None", which manages to be contemptuous, ungrammatical, and unresponsive all at once. In order to assess this question, the City Council would need to know the quantity, location to the census block level, and duration of pole camera deployments. None of that information is in this STIR.

[Police Department] ShotSpotter:

The ShotSpotter STIR suffers from the same systemic defects as the other STIRs we're recommending for rejection: vague descriptions of the technology, conclusory and unsupported claims of effectiveness, unresponsive statements on costs, and casual dismissal of differential impacts.

Worse than that, it uses more or less exactly the same wording as the 2023 ShotSpotter STIR. We provided thorough feedback on that STIR to the City, in a letter dated March 11, 2024. We are now forced to reproduce much of the substance of that letter here, in the hope that the City Council will now direct Somerville PD to remedy the deficiencies identified then.

The brief description provided by Captain Sheehan to the Legislative Matters Committee of what ShotSpotter does is as follows:

> *“ShotSpotter is a gunshot detection service that utilizes 35 sensors installed in the city’s coverage area to identify and locate gunfire. Sensors detect noises suggestive of gunshot and trigger only when 3 different sensors detect a gunshot-like sound at the same time to determine location. ShotSpotter records gunshot-like sounds and does not record video.”*

This description leaves out everything that would make one concerned about the privacy implications of this technology. First, the “sensors” are in fact always listening, much like an Alexa unit is always listening for the trigger word “Alexa.” They are listening not only for actual “gunfire”, but for anything that ShotSpotter’s artificial intelligence software has previously chosen to class as a “gunfire-like sound.” It can and does trigger in response to sounds of firecrackers or of cars backfiring. When it triggers, ShotSpotter HQ sends Somerville PD an audio clip of the time surrounding the “gunfire-like sound.” That audio clip, of course, can include any sound the sensors recorded, including human conversations. Massachusetts police have in fact attempted to introduce conversations recorded in this way into evidence. So, it’s a much broader audio monitoring technology than this description makes out.

Captain Sheehan reports,

> *During Calendar year 2025 we received 9 ShotSpotter activation notices [...] a total of 24 shell casings were recovered. ShotSpotter has been effective in achieving its identified purpose.*
>
> *This information [i.e., the activation notices] was shared with the Middlesex District Attorney’s Office for 2 Criminal Investigations. The ShotSpotter detection information was shared with Middlesex District Attorney’s Office to assist in the prosecution of criminal*

*cases. The data was shared pursuant to the Massachusetts Rules of Evidence. **(When a ShotSpotter Activation occurs and is confirmed, that info is included in our weekly crime bulletin, which is supplied to surrounding Police Departments)*

Of course, this tells us nothing about whether ShotSpotter is effective. All that it tells us is that it was actually switched on rather than off. For all we know from this information, all 24 shell casings could have been deposited in connection to one incident of gunfire, and the other 8 ShotSpotter alerts could have been false alarms. In fact, given that the ShotSpotter coverage area is notable for its trash complaints, there's not even any guarantee that casings found near an alert relate to the same incident at all.

To really answer this question, we have to be clear about what we mean. ShotSpotter is sold to municipalities above all on the basis that it reduces gun violence. But neither this report, nor any other evidence so far presented by Somerville PD, shows that ShotSpotter in Somerville reduces gun violence. Somerville PD admits they don't "audit" the program. There's no information on how the ShotSpotter alerts affected anything. Unlike the ShotSpotter report provided last week to the Cambridge City Council by Cambridge PD, there's no reporting from Somerville PD on false positives or false negatives. In Cambridge, the false-positive rate was 62.5% and the false-negative rate was 57.5%; in other words, ShotSpotter's overall accuracy rate was a miserable 40%. Likewise, Somerville PD, unlike Cambridge PD, doesn't identify whether these ShotSpotter activations were accompanied by, or preceded by, 911 calls from the public. In Cambridge, for the second year running, ShotSpotter didn't alert Cambridge PD to any incident that did not also have at least one 911 call from the public.

Somerville PD provides no data on whether anybody was arrested, prosecuted, or convicted for any gun-related crimes in response to a ShotSpotter alert, and no data on whether there were even any incidental arrests, and if so, what charge if any was brought.

An independent study, conducted in St. Louis, MO, found "no evidence that the implementation of ShotSpotter resulted in more arrests related to gunfire incidents", and that "overall crime reporting appears not to have been impacted by the implementation of ShotSpotter." A longitudinal study published in the Journal of Urban Health, covering 17 years' worth of homicide data from 68 counties across the US that had adopted ShotSpotter, also found "no evidence that the technology reduces firearm homicides." In other words, even with the wealth of data provided in the context of a bigger city, **ShotSpotter cannot be shown to have any effect at all on gun violence.**

So, why does Somerville PD have ShotSpotter at all, if it can't be shown to work? We believe the reason to be structural. DHS provides grant funding to key urban areas through the "Urban Areas Security Initiative." The Commonwealth's Executive Office of Public Safety and Security, or EOPSS, applies for the funding. EOPSS itself is dominated by law enforcement interests, and police chiefs get intensely lobbied by private vendors. The grants structure, in other words, socializes the financial costs away from the police department, and the residents whose privacy is affected generally don't know they're being monitored. The technology seems to police chiefs like something they can get more or less for free, and that might work, and it's easy for police departments to misinterpret skepticism on the part of activist groups as anti-police bias.

Captain Sheehan breezes past the notion that ShotSpotter might have disparate impacts on particular neighborhoods. In response to the question, "*Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the city are disproportionately impacted by the deployment of the surveillance technology"*, he simply writes, as he did in previous years, *"None."*

Map showing census tracts containing at least one ShotSpotter sensor, from https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/, Feb. 22, 2024

Thanks to reporting from WIRED in February 2024, we can prove he's wrong. We now know, and reported to the City back in March 2024, every census tract in Somerville where at least one ShotSpotter sensor is located. They're in Ten Hills, Assembly Square, heavily Hispanic East Somerville, Winter Hill, Prospect Hill and Boynton Yards (Wards 1-4) (see map on next page). In fact, for none of the technologies in the whole Annual Surveillance Report do Somerville PD even state that there are any disproportionate impacts at all, let alone suggest that there's anything that they should do to mitigate them. It should not be hard for Captain Sheehan to understand that there is an equity issue here. The poorer and more diverse folks of East Somerville, living in neighborhoods with constant high levels of traffic noise, including cars backfiring, get constant audio monitoring from "35 sensors" in case there is a "gunshot-like sound." The richer folks of West Somerville don't.

To sum up: ShotSpotter doesn't work to reduce gun violence. It may not directly come out of the municipal budget, but it does bind our Police Department financially to President Trump's abusive DHS. And it puts poorer and more diverse folks in particular - the very people being hunted down by DHS - under continuous audio microphone surveillance, with no demonstrable benefit to public safety. The City Council is being deprived of meaningful information in this STIR that other PDs provide to their elected officials as part of surveillance ordinance reporting. The City Council should not tolerate this continuing, and worsening, state of affairs.

Surveillance Technology Impact Reports to be further reviewed or amended before acceptance [4]:

[Parking Department] Safety Stick:

We do not believe that this technology infringes on the privacy rights of Somerville residents. However, it's not clear to us how this technology is compatible with M. G. L. ch. 90, section 20A, which is generally held to have the effect of prohibiting the deployment of automated cameras to enforce traffic or parking violations; which is why Massachusetts House and Senate leaders are contemplating legalizing automated speed cameras this session. It would therefore be worthwhile

for City Councilors to understand the analysis of the City Solicitor as to how these fixed Safety Sticks at bus stops comply with existing law.

[Fire Department] Fire Station Exterior Cameras:

We are generally skeptical about CCTV cameras. It's always hard to reverse an unwise decision. It's not unprecedented - as referred to above, Cambridge City Council just reversed course on Flock Safety cameras - but we understand that it's always a heavier lift once a decision to install a technology has been made.

In this STIR, the Fire Department doesn't present any evidence that the cameras are actually deterring any criminal activity or traffic violations, but it's clear that they envision these cameras being used for law enforcement purposes. Every time you put up new cameras, of course, you create a new data stream that can be captured and exploited by the federal government as well. Because of our voluntary participation as a City in BRIC, as far as we're aware, DHS doesn't even have to ask for access to footage from these cameras.

These cameras aren't accompanied, as far as we know, by a policy for their use or for the sharing of data, and unlike for other Fire Department technologies, it seems clear that in the event of an incident, the footage would be shared. The cameras will be operated by the Police Department, and they are funded by President Trump's DHS, through the Urban Areas Security Initiative; the same DHS that is under orders to use every available means to hunt down immigrants and dissidents. In the context of these newly intensified federal threats, it seems worthwhile to ask what the policy is and whether there is one, and for the cameras to cease operation at least until a clear policy, with substantial community buy-in, is in place.

[Police Department] Covert Device Cameras:

Covert police cameras are a serious invasion of residents' privacy. It appears that this year, as last year, the Police Department didn't use this technology, and that the Police Department expects to get a warrant if they were to use them. But it worries us to have this approval on the books nonetheless.

No information is given in this STIR about the policy governing the use of such cameras, or how they would be approved. Some transparency on that matter would be appropriate, and the process for deploying them should resemble the "super-warrant" process in the Massachusetts wiretapping law, because of the very significant Fourth Amendment issues at stake in the Police Department deciding to secretly bug people's homes.

[Police Department] GLX Cameras / Homeland Security Cameras:

We repeat our comments from 2024, because the same defects in the STIR for GLX cameras and the STIR for Homeland Security Cameras that year are reproduced here. Whether there are disparate civil liberties impacts on any particular group of people cannot be assessed without knowing exactly where the GLX/Homeland Security cameras are. Logically, the people disproportionately impacted by the deployment of fixed surveillance cameras, are the people who live and work in the areas the cameras surveil, but the Green Line Extension goes through a large part of Somerville. Somerville PD should disclose the location of these cameras to the nearest census block, as required by the Surveillance Ordinance.

In both reports, Lt. Sheehan argues that the only relevant costs are if a camera is moved, and that, as none of these cameras were moved during this year, there are no costs. This is obviously false.

Costs associated with cameras include the costs of replacement and maintenance, as well as the cost of staff time spent monitoring and reviewing camera footage that, but for the cameras, would not exist. Only if the Committee understands these cost elements, will they be able to fairly judge those costs against the benefits fairly attributable to the cameras.

Last, the same objections to the DHS-funded Fire Station Exterior Cameras are also applicable here. They are funded through the same program, and with the same threat posed by federal exploitation of every available datastream to hunt down immigrants and dissidents. In order for the City Council to approve these cameras, there needs to be a clearly stated policy governing their use, and these cameras, too, should cease operation till there is one.

Surveillance Technology Impact Reports to be accepted [6]:

[IAM] Unmanned Aircraft System:

This isolated use, to examine the state of the terracotta tiles on the Somerville High School facade, poses no ongoing threat to students' or residents' privacy.

[OPSCD] Video/Photography Drone:

This drone is reported to not have been used in the past year, and therefore poses minimal ongoing threat to residents' privacy.

[Fire Department] FLIR MC300C Marine Camera:

This camera is reported to have been used only once in the past year, and is designed for night-time marine operations only. It therefore poses no ongoing threat to residents' privacy.

[Fire Department] Thermal Imaging Cameras:

This technology seems critical for core Fire Department functions. While it is frequently used, we have no reason to doubt the Fire Department's representation in the STIR that the *"technology is not intended for law enforcement purposes or intelligence gathering, does not store data, and is only deployed in emergency response situations where it is deemed necessary to protect life or property."*

[Police Department] E-911 Services:

We have no problem with a technology that, in the event of a 911 call, more accurately triangulates the location from which the call is made. That's an improvement to the process of locating people who are seeking assistance from the City, not a general surveillance technology that harms the privacy interests of people in general.

[Police Department] GPS Monitors:

These are placed in "bait bikes" in case those bikes are stolen. As such, the only people whose privacy is implicated, are people who steal the bait bikes. The technology was apparently not used this year. As such, it poses no ongoing threat to the privacy of residents not involved in a crime.

DIGITAL FOURTH

The Massachusetts campaign to protect digital data from warrantless government surveillance

Somerville City Council

93 Highland Ave.

Somerville, MA 02143

March 11, 2026

RE: COMMENTS OF DIGITAL FOURTH ON 2026 SOMERVILLE ANNUAL SURVEILLANCE REPORTS

Dear members of the Somerville City Council,

Digital Fourth is a local, volunteer-run civil liberties group, founded in 2012, and active on the issue of government surveillance. We have participated extensively in the development, passage, and implementation of the City's Surveillance Ordinance. Since that passed in 2021, we have provided regular comments to the City Council and the Legislative Matters Committee on the surveillance technologies operated by City agencies. We have also advised members of the City Council and Mayor Wilson on ways to Constitutionally limit ICE raids in the City.

We are grateful for the City's steady commitment to preserving the privacy of Somerville residents by refusing to deploy automated license plate readers. Somerville has therefore wisely avoided the confused and inept rollout of Flock Safety in other nearby municipalities, culminating in Boston having to pause, and Cambridge having to revoke its Flock Safety contract in December 2025.

In 2024, we advised the City Council to not approve Surveillance Technology Impact Reports ("STIRs") not containing information on the costs of the technologies in question, or an honest assessment of disparate impacts as required under the Ordinance. It is still not the general practice of the City's departments to actually identify and state the costs of the surveillance technology, both at acquisition, and in terms of ongoing costs for maintenance, training, license renewals and staff time. Some STIRs fail even to identify the equipment vendor (like the "Safety Stick", which is manufactured by MPS). We have also steadily advised in particular that the City's deployment of ShotSpotter is ineffectual, invasive, and unfair to the residents of East Somerville.

Here's our analysis of the individual technologies in the Report. We believe that this Report as a whole will be referred to the Legislative Matters Committee, and we look forward to providing detailed feedback to that Committee as they evaluate the appropriate recommendations for the Council as a whole.

Surveillance Technology Impact Reports to be rejected [3]:

[Police Department:] GrayKey

Captain Sheehan's reports regarding this intrusive technology continue to be gravely deficient. As a result, we are recommending rejection of this STIR. In 2021, we recommended against GrayKey deployment. In 2023, we supplied a nine-page analysis again recommending rejection of the use of GrayKey, including a detailed analysis of what was missing from the STIR and how it could be improved. In 2024, we reiterated this analysis. Somerville PD, in response, has adopted none of our suggestions for improving this STIR, despite the fact that the Ordinance envisions a process where Somerville PD does iteratively improve their reporting to Council. Instead, with the City Council annually approving this STIR no matter how deficient it is, the information provided in it has steadily thinned relative to 2021-2023.

Poor explanation of the technology:

Captain Sheehan explains:

> *"GrayKey is a digital forensic tool that enables the Somerville Police Department Digital Forensic Unit to bypass encryption on locked Android and IOS devices. The devices accessed would only be accessed in accordance with a duly issued search warrant or consent from the owner of the device. The type of data extracted from the digital devices includes, but is not limited to, digital pictures, videos, text messages, call logs and any other data which would normally be stored on a digital device which could be used in a criminal investigation."*

This question is intended for the applying agency to provide to Councillors an accessible explanation of how the technology works. Instead, Lt. Sheehan focuses on the legalities of using the technology, which is interesting but only supplemental to explaining the technology and how it works. We believe that the City Council would benefit from such an explanation, which would also show that the Police Department themselves understand how the technology they're proposing for approval works. We believe that a response to this question that would be complete, and that would also show that Somerville PD's use of the technology would satisfy standards of Constitutional policing, would read something like as follows:

> "*GrayKey is a digital forensic tool that enables the Somerville Police Department Digital Forensic Unit to bypass encryption on locked Android and IOS devices.* GrayKeys are sold by GrayShift Technologies, now part of Magnet Forensics (link). GrayKeys are focused on obtaining photographic evidence from Computers, Mobile Phones, Digital Cameras, Tablets and any device used to communicate, store data and facilitate the commission of crimes, for which the password, pattern or fingerprint access is unknown, though they can also provide law enforcement access to *digital pictures, videos, text messages, call logs and any other data which would normally be stored on a digital device which could be used in a criminal investigation*. We have used them in the past, and intend to use them in the future, in the context of criminal investigations, to unlock devices of criminal suspects when consent is unavailable or has been refused, or in some cases, with the suspect's consent, to conveniently conduct a deeper and more forensic examination of a phone's contents. A valid search warrant, based on probable cause and issued by the appropriate jurisdictional Massachusetts Court, or a valid consent to search, is required in order to legally extract the evidence from the device. Through the Urban Area Security Initiative (UASI) Boston Office

> the SPD has acquired a License for the GrayKey Digital Forensics Analysis Tool and a Laptop computer which is used to analyze the data extracted from these devices. Our use of the GrayKey is also bound by the Attorney-General's Guidelines (link) and the relevant laws of the Commonwealth (link). We use a further premium add-on service, "Magnet AXIOM", which allows users to search for photos in the whole filesystem of the phone, and to confirm their provenance via hash matches."

At Council in 2024, Legislative Matters Committee Chair Davis and Councilor J. T. Scott "both requested that detail about storage, security (both physical and digital) and access protocols for the tech be added to the report", and we endorsed those calls. Unfortunately, the Police Department continues to fail to address these deficiencies.

No explanation of costs

As was the case previously, the 2026 GrayKey Surveillance Impact Report has provided you with no details on costs, this time simply saying "None." In discussion in Council, though not in the report itself, Lt. Mitsakis disclosed in 2024 that the license type sought for GrayKey "is the one that costs $38,000." This premium offering from GrayKey requires no Internet connection and has no limit to the number of unlocks. It is also the express intent of the Ordinance to consider costs in addition to the direct cost of acquisition to the City or Somerville PD. GrayKey has costs associated with annual training courses for the detective and the supervisor; staff time involved in attending those courses; and proportional costs of participation in the UASI grant process. If the City Council were not to approve the use of a GrayKey, those training costs would no longer be incurred, and the staff time would presumably be spent on other non-GrayKey-related investigative activities.

Repeated refusal to address the key issue of over-seizure of data

None of Somerville PD's responses in the Surveillance Technology Impact Report have ever addressed a key question, namely, what happens to device data that the GrayKey gives access to that is not relevant to a particular investigation? In the original Surveillance Use Policy for this technology, then-Lt. Sheehan specified, "*The technology cannot be used to collect personal information unrelated to the investigation. The information gathered must be relevant to the investigation as indicated in the search warrant."* But that's simply not true. GrayKey images the entire device. There is then a process on the part of the police department, which is not explained or described in any way, to identify and segregate information "relevant to the investigation as indicated in the search warrant." What happens to the *other* information collected? If it is destroyed before being used or shared, then there's no problem. If it is retained, then how long for? Is that data exploited by Somerville PD, and if so, in what circumstances? Have there been instances where evidence of a different crime has been uncovered by a GrayKey search; if so, was a separate warrant obtained for that data, and was that crime prosecuted? Have there been instances where embarrassing data that is not immediately evidence of a different crime, has been used to pressure an individual, for example, to take a plea, to become an informant, or to do other favors for law enforcement? Does Somerville PD also analyze the whole pattern of location data contained in the phone and cross-reference it with other crimes, or probe through the photo gallery to find evidence of other criminal activities not specified in the warrant, or delve into the list of contacts to find potential contacts of the suspect who are also suspected or convicted of crimes or who are listed as "gang associates" or "gang members"? Are there any limitations as to the type of criminal investigations for which a GrayKey would be used? For example, does any stated policy or practice preclude Somerville PD from arresting a protester for disorderly conduct or resisting arrest, and then using a GrayKey to hack into their phone and map out their contacts for further

investigation, or find compromising information unrelated to the investigation that would pressure that protester to become an informant or plead guilty?

Our phones contain evidence relating to our whole lives; police should not be able to use a GrayKey to bypass someone's password and gain full access to every part of their life for close digital review, simply because that person is suspected in a particular crime. The question of the admissibility and constitutionality of such "over-seized" data is a ferociously contested one in Fourth Amendment jurisprudence. We have now raised these issues in the context of the City of Somerville's use of GrayKey for five years. It is time for Somerville PD to address them.

No provision of training materials

Contrary to the specific language of the Ordinance, Somerville PD has consistently refused to provide the actual training materials for GrayKey. Despite our comments and requests, councilors don't even have a description of what is in the training materials, the number of hours spent in training, or the entities providing the training. Whether or not the trainings contain anything disturbing, this repeated failure, over the course of years, to answer this question disrespects the Ordinance and the Council. If there are training materials, Somerville PD must supply them; if not, Somerville PD should state that they do not exist. The question of the content of officer training is often key to the question of whether they have exceeded their authority.

[Police Department] Pole cameras

This STIR significantly misstates the state of the jurisprudence governing the use of pole cameras by law enforcement. Captain Sheehan wrongly states, "Pole cameras are installed in *public areas where there is no expectation of privacy."* As of, perhaps, twenty years ago, this was an accurate depiction of the law. However, during the 2010s, the Supreme Court, in three decisions (*Jones*, *Riley* and *Carpenter*), explored situations where law enforcement used digital surveillance to monitor people in public, and where nevertheless the Supreme Court found that there was sometimes a reasonable expectation of privacy in public areas. In particular (condensing a great deal of legalese here), surveillance that occurred for a long enough period for law enforcement to be able to discern the "patterns of life" of residents, was a search under the Fourth Amendment. On pole cameras in particular, the ruling in *U.S. v. Moore-Bush,* in our First Circuit Court of Appeals, is binding. That ruling decided whether the pole camera evidence should stay in on other grounds, but then split evenly across two concurrences on the Fourth Amendment issue of whether people had a reasonable expectation of privacy in police monitoring of the curtilage of their home over an eight-month period, and therefore whether that monitoring constituted a search requiring a warrant. Captain Sheehan does the Council a disservice, then, by presenting the law as unambiguously on the police's side when it comes to pole cameras. We have repeatedly, in this surveillance ordinance process, alerted the City Council and Somerville PD to these precedents.

Beyond this serious misstatement, the STIR is also thin to the point of contempt for the Ordinance in several other respects. Captain Sheehan writes, in response to the question of whether pole cameras have been effective, "Pole Cameras have been effective in assisting the SPD during the course of investigations." He doesn't bother with details or examples; he gives no figures that would enable City Council independently to assess his bare claim. He might as well have just written "Yes." Perhaps that will come next year, after the City Council approves this STIR and thereby shows that they don't expect examples or details as the price of approval. Regarding costs, instead of following the clear language of the Ordinance and specifying "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", he simply says, "All costs associated with

this technology are covered by UASI." That's not what the question asks. The intent of the Ordinance on costs is to enable the City Council to determine annually how much is being spent on surveillance in the City, whether that money is covered by the municipal budget, by an external government grant, via a gift from a police foundation, or via a gift from a billionaire. By that means, they can gain insight into how City Departments avoid municipal scrutiny while creating their own ecosystem of surveillance technologies. When Captain Sheehan is asked, "Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the city are disproportionately impacted by the deployment of the surveillance technology", he simply says, "None", which manages to be contemptuous, ungrammatical, and unresponsive all at once. In order to assess this question, the City Council would need to know the quantity, location to the census block level, and duration of pole camera deployments. None of that information is in this STIR.

[Police Department] ShotSpotter:

The ShotSpotter STIR suffers from the same systemic defects as the other STIRs we're recommending for rejection: vague descriptions of the technology, conclusory and unsupported claims of effectiveness, unresponsive statements on costs, and casual dismissal of differential impacts.

Worse than that, it uses more or less exactly the same wording as the 2023 ShotSpotter STIR. We provided thorough feedback on that STIR to the City, in a letter dated March 11, 2024. We are now forced to reproduce much of the substance of that letter here, in the hope that the City Council will now direct Somerville PD to remedy the deficiencies identified then.

The brief description provided by Captain Sheehan to the Legislative Matters Committee of what ShotSpotter does is as follows:

> *“ShotSpotter is a gunshot detection service that utilizes 35 sensors installed in the city’s coverage area to identify and locate gunfire. Sensors detect noises suggestive of gunshot and trigger only when 3 different sensors detect a gunshot-like sound at the same time to determine location. ShotSpotter records gunshot-like sounds and does not record video.”*

This description leaves out everything that would make one concerned about the privacy implications of this technology. First, the “sensors” are in fact always listening, much like an Alexa unit is always listening for the trigger word “Alexa.” They are listening not only for actual “gunfire”, but for anything that ShotSpotter’s artificial intelligence software has previously chosen to class as a “gunfire-like sound.” It can and does trigger in response to sounds of firecrackers or of cars backfiring. When it triggers, ShotSpotter HQ sends Somerville PD an audio clip of the time surrounding the “gunfire-like sound.” That audio clip, of course, can include any sound the sensors recorded, including human conversations. Massachusetts police have in fact attempted to introduce conversations recorded in this way into evidence. So, it’s a much broader audio monitoring technology than this description makes out.

Captain Sheehan reports,

> *During Calendar year 2025 we received 9 ShotSpotter activation notices [...] a total of 24 shell casings were recovered. ShotSpotter has been effective in achieving its identified purpose.*
>
> *This information [i.e., the activation notices] was shared with the Middlesex District Attorney’s Office for 2 Criminal Investigations. The ShotSpotter detection information was shared with Middlesex District Attorney’s Office to assist in the prosecution of criminal*

*cases. The data was shared pursuant to the Massachusetts Rules of Evidence. **(When a ShotSpotter Activation occurs and is confirmed, that info is included in our weekly crime bulletin, which is supplied to surrounding Police Departments)*

Of course, this tells us nothing about whether ShotSpotter is effective. All that it tells us is that it was actually switched on rather than off. For all we know from this information, all 24 shell casings could have been deposited in connection to one incident of gunfire, and the other 8 ShotSpotter alerts could have been false alarms. In fact, given that the ShotSpotter coverage area is notable for its trash complaints, there's not even any guarantee that casings found near an alert relate to the same incident at all.

To really answer this question, we have to be clear about what we mean. ShotSpotter is sold to municipalities above all on the basis that it reduces gun violence. But neither this report, nor any other evidence so far presented by Somerville PD, shows that ShotSpotter in Somerville reduces gun violence. Somerville PD admits they don't "audit" the program. There's no information on how the ShotSpotter alerts affected anything. Unlike the ShotSpotter report provided last week to the Cambridge City Council by Cambridge PD, there's no reporting from Somerville PD on false positives or false negatives. In Cambridge, the false-positive rate was 62.5% and the false-negative rate was 57.5%; in other words, ShotSpotter's overall accuracy rate was a miserable 40%. Likewise, Somerville PD, unlike Cambridge PD, doesn't identify whether these ShotSpotter activations were accompanied by, or preceded by, 911 calls from the public. In Cambridge, for the second year running, ShotSpotter didn't alert Cambridge PD to any incident that did not also have at least one 911 call from the public.

Somerville PD provides no data on whether anybody was arrested, prosecuted, or convicted for any gun-related crimes in response to a ShotSpotter alert, and no data on whether there were even any incidental arrests, and if so, what charge if any was brought.

An independent study, conducted in St. Louis, MO, found "no evidence that the implementation of ShotSpotter resulted in more arrests related to gunfire incidents", and that "overall crime reporting appears not to have been impacted by the implementation of ShotSpotter." A longitudinal study published in the Journal of Urban Health, covering 17 years' worth of homicide data from 68 counties across the US that had adopted ShotSpotter, also found "no evidence that the technology reduces firearm homicides." In other words, even with the wealth of data provided in the context of a bigger city, **ShotSpotter cannot be shown to have any effect at all on gun violence.**

So, why does Somerville PD have ShotSpotter at all, if it can't be shown to work? We believe the reason to be structural. DHS provides grant funding to key urban areas through the "Urban Areas Security Initiative." The Commonwealth's Executive Office of Public Safety and Security, or EOPSS, applies for the funding. EOPSS itself is dominated by law enforcement interests, and police chiefs get intensely lobbied by private vendors. The grants structure, in other words, socializes the financial costs away from the police department, and the residents whose privacy is affected generally don't know they're being monitored. The technology seems to police chiefs like something they can get more or less for free, and that might work, and it's easy for police departments to misinterpret skepticism on the part of activist groups as anti-police bias.

Captain Sheehan breezes past the notion that ShotSpotter might have disparate impacts on particular neighborhoods. In response to the question, "*Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the city are disproportionately impacted by the deployment of the surveillance technology"*, he simply writes, as he did in previous years, *"None."*

Map showing census tracts containing at least one ShotSpotter sensor, from https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/, Feb. 22, 2024

Thanks to reporting from WIRED in February 2024, we can prove he's wrong. We now know, and reported to the City back in March 2024, every census tract in Somerville where at least one ShotSpotter sensor is located. They're in Ten Hills, Assembly Square, heavily Hispanic East Somerville, Winter Hill, Prospect Hill and Boynton Yards (Wards 1-4) (see map on next page). In fact, for none of the technologies in the whole Annual Surveillance Report do Somerville PD even state that there are any disproportionate impacts at all, let alone suggest that there's anything that they should do to mitigate them. It should not be hard for Captain Sheehan to understand that there is an equity issue here. The poorer and more diverse folks of East Somerville, living in neighborhoods with constant high levels of traffic noise, including cars backfiring, get constant audio monitoring from "35 sensors" in case there is a "gunshot-like sound." The richer folks of West Somerville don't.

To sum up: ShotSpotter doesn't work to reduce gun violence. It may not directly come out of the municipal budget, but it does bind our Police Department financially to President Trump's abusive DHS. And it puts poorer and more diverse folks in particular - the very people being hunted down by DHS - under continuous audio microphone surveillance, with no demonstrable benefit to public safety. The City Council is being deprived of meaningful information in this STIR that other PDs provide to their elected officials as part of surveillance ordinance reporting. The City Council should not tolerate this continuing, and worsening, state of affairs.

Surveillance Technology Impact Reports to be further reviewed or amended before acceptance [4]:

[Parking Department] Safety Stick:

We do not believe that this technology infringes on the privacy rights of Somerville residents. However, it's not clear to us how this technology is compatible with M. G. L. ch. 90, section 20A, which is generally held to have the effect of prohibiting the deployment of automated cameras to enforce traffic or parking violations; which is why Massachusetts House and Senate leaders are contemplating legalizing automated speed cameras this session. It would therefore be worthwhile

for City Councilors to understand the analysis of the City Solicitor as to how these fixed Safety Sticks at bus stops comply with existing law.

[Fire Department] Fire Station Exterior Cameras:

We are generally skeptical about CCTV cameras. It's always hard to reverse an unwise decision. It's not unprecedented - as referred to above, Cambridge City Council just reversed course on Flock Safety cameras - but we understand that it's always a heavier lift once a decision to install a technology has been made.

In this STIR, the Fire Department doesn't present any evidence that the cameras are actually deterring any criminal activity or traffic violations, but it's clear that they envision these cameras being used for law enforcement purposes. Every time you put up new cameras, of course, you create a new data stream that can be captured and exploited by the federal government as well. Because of our voluntary participation as a City in BRIC, as far as we're aware, DHS doesn't even have to ask for access to footage from these cameras.

These cameras aren't accompanied, as far as we know, by a policy for their use or for the sharing of data, and unlike for other Fire Department technologies, it seems clear that in the event of an incident, the footage would be shared. The cameras will be operated by the Police Department, and they are funded by President Trump's DHS, through the Urban Areas Security Initiative; the same DHS that is under orders to use every available means to hunt down immigrants and dissidents. In the context of these newly intensified federal threats, it seems worthwhile to ask what the policy is and whether there is one, and for the cameras to cease operation at least until a clear policy, with substantial community buy-in, is in place.

[Police Department] Covert Device Cameras:

Covert police cameras are a serious invasion of residents' privacy. It appears that this year, as last year, the Police Department didn't use this technology, and that the Police Department expects to get a warrant if they were to use them. But it worries us to have this approval on the books nonetheless.

No information is given in this STIR about the policy governing the use of such cameras, or how they would be approved. Some transparency on that matter would be appropriate, and the process for deploying them should resemble the "super-warrant" process in the Massachusetts wiretapping law, because of the very significant Fourth Amendment issues at stake in the Police Department deciding to secretly bug people's homes.

[Police Department] GLX Cameras / Homeland Security Cameras:

We repeat our comments from 2024, because the same defects in the STIR for GLX cameras and the STIR for Homeland Security Cameras that year are reproduced here. Whether there are disparate civil liberties impacts on any particular group of people cannot be assessed without knowing exactly where the GLX/Homeland Security cameras are. Logically, the people disproportionately impacted by the deployment of fixed surveillance cameras, are the people who live and work in the areas the cameras surveil, but the Green Line Extension goes through a large part of Somerville. Somerville PD should disclose the location of these cameras to the nearest census block, as required by the Surveillance Ordinance.

In both reports, Lt. Sheehan argues that the only relevant costs are if a camera is moved, and that, as none of these cameras were moved during this year, there are no costs. This is obviously false.

Costs associated with cameras include the costs of replacement and maintenance, as well as the cost of staff time spent monitoring and reviewing camera footage that, but for the cameras, would not exist. Only if the Committee understands these cost elements, will they be able to fairly judge those costs against the benefits fairly attributable to the cameras.

Last, the same objections to the DHS-funded Fire Station Exterior Cameras are also applicable here. They are funded through the same program, and with the same threat posed by federal exploitation of every available datastream to hunt down immigrants and dissidents. In order for the City Council to approve these cameras, there needs to be a clearly stated policy governing their use, and these cameras, too, should cease operation till there is one.

Surveillance Technology Impact Reports to be accepted [6]:

[IAM] Unmanned Aircraft System:

This isolated use, to examine the state of the terracotta tiles on the Somerville High School facade, poses no ongoing threat to students' or residents' privacy.

[OPSCD] Video/Photography Drone:

This drone is reported to not have been used in the past year, and therefore poses minimal ongoing threat to residents' privacy.

[Fire Department] FLIR MC300C Marine Camera:

This camera is reported to have been used only once in the past year, and is designed for night-time marine operations only. It therefore poses no ongoing threat to residents' privacy.

[Fire Department] Thermal Imaging Cameras:

This technology seems critical for core Fire Department functions. While it is frequently used, we have no reason to doubt the Fire Department's representation in the STIR that the *"technology is not intended for law enforcement purposes or intelligence gathering, does not store data, and is only deployed in emergency response situations where it is deemed necessary to protect life or property."*

[Police Department] E-911 Services:

We have no problem with a technology that, in the event of a 911 call, more accurately triangulates the location from which the call is made. That's an improvement to the process of locating people who are seeking assistance from the City, not a general surveillance technology that harms the privacy interests of people in general.

[Police Department] GPS Monitors:

These are placed in "bait bikes" in case those bikes are stolen. As such, the only people whose privacy is implicated, are people who steal the bait bikes. The technology was apparently not used this year. As such, it poses no ongoing threat to the privacy of residents not involved in a crime.