Madalyn Letellier

From: Alex Marthews [redacted]
Sent: Monday, October 16, 2023 4:22 PM
To: Public Comments
Subject: Written testimony for Legislative Matters Committee meeting 10/17, item 23-1354 (GrayKey surveillance impact report)
Attachments: GrayKey Somerville STIR response 2023-10-16 (1).pdf

---

Hi,

Please find attached our written comments on the GrayKey surveillance impact report on the agenda for the Legislative Matters Committee meeting tomorrow (10/17), item 23-1354.

Please confirm that it will be distributed to the Committee members.

Best wishes
Alex.

Alex Marthews
Chair, Digital Fourth
[redacted]
Website
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 unconstitutional government surveillance

Legislative Matters Committee
Somerville City Council

October 16, 2023.

RE: Item 23-1354 (GrayKey surveillance impact report): OPPOSED

Dear Chair Davis, Vice-Chair Kelly, and Councilors Burnley, McLaughlin, and Scott;

Digital Fourth is a volunteer-based civil liberties organization, founded in 2012 and meeting in Cambridge, that focuses on issues of privacy, surveillance and the Fourth Amendment; we have members who live and work in Somerville, and we helped the City formulate its Surveillance Oversight Ordinance, of which this is a part. In 2021, Digital Fourth weighed in on the GrayKey Surveillance Impact Report, providing extensive comments along with suggested language that would enable Somerville PD to substantially improve the quality of the information provided to the Council regarding this invasive technology. The Report for 2023 has not adopted these suggestions, and generally provides Councilors with no better information than was provided to the Council in 2021. It is now especially important to do so because, as Somerville PD put it in comments to Council, "this technology has started to become standard in investigations," and they are using it much more than they did in 2021. The scope of the technology is now also far greater, because in 2021 it was limited to phones running Apple iOS, and now is a broader technology capable of searching "*any device used to communicate"* or *"store data."*

At Council, Chair Davis and Councilor Scott have "both requested that detail about storage, security (both physical and digital) and access protocols for the tech be added to the report." We endorse those calls, and specify below the additional information that we would like to see.

1: COSTS AND CAPABILITIES

As was the case previously, the 2023 GrayKey Surveillance Impact Report has provided you with no details on costs, merely specifying that it is provided through Boston's UASI grant - a grant that is applied for and comes to Somerville, whether people in Somerville in general want it to be applied for or not. In discussion in Council, though not in the report itself, Lt. Mitsakis is reported to have specified 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. Especially in light of this being a technology that the City itself now plans to own, it is now even more necessary to be explicit about all costs associated with it, including licensing, training and staff time.

2: WHAT HAPPENS TO INCIDENTALLY GATHERED DATA?

None of Somerville PD's responses in the Surveillance Impact Report address a key question, namely, what happens to device data that the GrayKey gives access to that is not relevant to a particular investigation? 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?

3: THE ORDINANCE REQUIRES SOMERVILLE PD TO PROVIDE THE ACTUAL TRAINING MATERIALS ON GRAYKEY, BUT THEY DON'T

Contrary to the specific language of the Ordinance, Somerville PD has consistently refused tro 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, and that the Detective and Detective Supervisor will be using the devices untrained. The question of the content of officer training is often key to the question of whether they have exceeded their authority.

4. DETAILED REVIEW OF THE SURVEILLANCE IMPACT REPORT

Now, we turn to a close review of the Surveillance Impact Report, and how it could be made adequately responsive, proceeding for each question on the STIR in turn. In general, Somerville PD did not adopt any of our recommendations for improvement to their reports from 2021 to 2023. As this is intended to be a process where Somerville PD does iteratively improve their reporting to Council, we recommend that in light of both Councilors' comments and our own, the Legislative Matters Committee return the current Surveillance Impact Report on GrayKey to Somerville PD for improvements, before considering whether to permit the continued use of this tool.

Q1. Information describing the surveillance technology and how it works:

> Lt. Sheehan's response is as follows: *"The GrayKey Digital Forensics Analysis Tool (DFAT) is used to legally access digital evidence located on electronic devices which*

include, but are not limited to, Computers, Mobile Phones, Digital Cameras, Tablets and any device used to communicate, store data and facilitate the commission of crimes. A valid search warrant 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." This question is intended for the applying agency to provide 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 devices are sold by GrayShift Technologies (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 location data, text messages, emails and other data stored on the device. 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/do not 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."

Q1a. 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):

Lt. Sheehan's response is as follows: *"A valid search warrant, 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. Similar to the search of a car or a home, search of a phone is subject to limitations laid out in case law, and the scope and terms of the warrant. 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." The information that is missing from this response is what happens if information that is collected from the device turns out in fact to not be related to the investigation. Is that information deleted? If not, why not, and what is done with it?

Q1b. 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):

Lt. Sheehan's response is as follows: *"One Detective and one Detective Supervisor will be trained on the use of the GrayKey DFAT."* In the 2021 report, Lt. DiGregorio supplied additional details, on where the individual was assigned ("General Detectives/Digital Forensics") and the fact that the individual had to attend yearly training classes. However, neither the 2021 response nor this 2023 response give the answer required by the Ordinance, which is to provide the **actual training materials**.

We believe that a response to this question that would be complete, and that would show that the training provided is adequate, would read something like as follows (note: A version of this sample answer was provided in our 2021 comments, and therefore was accessible to Somerville PD to work from if they wished):

"One detective and one supervisor have been trained in using this device, and are currently the only members of the department qualified to operate this technology. These individuals are assigned to General Detectives/Digital Forensics. Each year, each individual is expected to attend XX hours of training relating to the use of GrayKey devices; in the past 3 years, the individuals in question have attended an average of YY hours per year. The trainings in the past 3 years have been provided by [Company/Agency X], [Company/Agency Y] and [Company/Agency Z], at an annual cost to Somerville PD of $NN,NNN. The training materials [are/are not] publicly available. [If publicly available, either on the Company/Agency's website or via the results of FOIA requests,] Copies of the training materials used over the last three years are available here [link], here [link], and here [link]. The training includes information on appropriate and inappropriate uses of GrayKey. The consequences outlined in the training for misuse of GrayKey are as follows: … ."

Q2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1)

Lt. Sheehan's response is as follows: *"The technology would only be used in cases in which a search warrant has been obtained in conjunction with the investigation allowing access to the device in question or with the owner's consent. Devices that contain digital evidence must be properly collected, handled and processed. The volatile nature of the data on these devices requires proper seizure to preserve the integrity of the data and ensure their evidentiary value in legal proceedings. Devices must be processed properly,*

whether the data these devices contain are incriminating or exculpatory." This is accurate, but not complete. As with Q1a, the information that is missing from this response is what happens if information that is collected from the device turns out in fact to not be related to the particular investigation, but may be relevant to other concurrent or subsequent investigations. For example, 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?

Q3. 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)

Lt. Sheehan's response is as follows: *"This technology opens "locked" devices by overriding passcodes. The types of surveillance data obtained from these devices include photos, videos, text conversations, call logs and any data normally stored on an electronic device."* Again, it is important from a Fourth Amendment perspective to clarify here whether the GrayKey collects only the data relevant to crimes specified in the search warrant, or whether it also collects other data that Somerville PD then uses.

Q3a. 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)

Lt. Sheehan's response is the same as Lt. DiGregorio's response in the *first* draft of Somerville PD's 2021 Impact Report: *"Only the investigator and investigator's supervisor would have access to the data recovered."* However, it's important to understand that the data recovered doesn't necessarily or always stay within Somerville PD. A more accurate statement might be, **"Within Somerville PD,** only the investigator and investigator's supervisor would have access to the data recovered. Information retrieved is stored on one specific computer, under the direct control of the Digital Forensics Detective. This information is distributed to the investigating Detective and the District Attorney's Office, and to the computers of other detectives and analysts at [agencies] in the context of multi-jurisdictional investigations."

Q3b. 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)

Lt. Sheehan's response is as follows: *"The device is used by two detectives* [sic: this was later corrected to "one detective" in testimony to Council] *under the direction of their supervisor, who are both certified by GrayKey. Information retrieved is stored on one specific computer, under the direct control of the Digital Forensics Detective."* This answer is at best only partially responsive. It does specify what ought to happen in terms of access, but not what measures are taken to ensure that what ought to happen is what happens. If another person, such as Somerville's police chief or a senior investigator in the AG's office not tasked with this investigation, believes that they should access this data, what mechanisms prevent them from doing so? Is there a password specific to each user, and how does the user secure that password? Is there an admin password for the device, and who has access to that – in other words, is there a sysadmin in the AG's office who is able to access the data in question?

Q3c. 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)

Lt. Sheehan's entire response is as follows: *"Any data or evidence obtained from using this technology would be retained for the duration of the relevant investigation and pending legal proceedings."* An additional part of the response from Lt. DiGregorio in 2021 states unhelpfully, *"The length of retention time varies, based on various factors, such as: length of the investigation and the statute of limitations set by the Commonwealth."* If the governing time period is in all cases the statute of limitations, the City Council will need to know the offenses for which Somerville PD considers it appropriate to use this intrusive tool, and the length of that period for each type of offense. And Lt. Sheehan should also answer the portions of the question that Somerville PD did not see fit to answer in 2021 either, namely:

- The reason that that retention period is appropriate;
- The process by which the information is regularly deleted after that period has lapsed;
- The conditions that must be met to retain information beyond that period.
- The retention and deletion policies for this kind of data for the agencies listed in the response to 3e).

Q3d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7)

Lt. Sheehan's response is as follows: *"Data collected is not available to members of the public. Defendants can request the data through the criminal discovery process."* This response is adequate.

Q3e. 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)

Lt. Sheehan's response is as follows: *"Data may be shared with the District Attorney's Office and/or other Law Enforcement Agencies if the investigation is multi-jurisdictional."* The question (and the Ordinance itself, from which this language is directly taken) require him to include the "justification and legal standard" for such sharing, and "any obligation(s) imposed on the recipient of the surveillance data." A response that would be complete, and that would satisfy standards of Constitutional policing, would read something like as follows:

> This technology would be used specifically in named investigations and under the authority of a search warrant based on probable cause and approved by an independent judge. There would be no third party sharing (besides turning evidence over to the District Attorney's Office for prosecution) unless the investigation involved another law enforcement agency or if the crimes investigated were multi-jurisdictional. The justification for such sharing is that Somerville PD would not reasonably be able to participate in a multi-jurisdictional investigation without sharing key evidence. Not sharing it might imperil the trust and partnership between Somerville PD and agencies with which regularly conduct multi-jurisdictional investigations. A list of these agencies is as follows: … (including links to their websites). These agencies that we intend to share GrayKey data with, will be under an obligation to use that data only in connection to the investigation for which the search warrant was obtained, and will not reshare the data onward to other agencies. The agencies also have their own policies for the retention of data used in investigations, which are accessible through the websites listed above.

Q4. The location(s) it may be deployed and when

Lt. Sheehan's response is as follows: *"The technology will only be deployed when a valid search warrant is issued by the courts or if valid signed consent is presented. Detectives are required to seek their supervisor's approval prior to using the technology."* This does not attempt to answer the question. An example of a more responsive answer would be,

> "Somerville PD intends to use this device in relation to investigations of crimes committed in any location within Somerville's boundaries, or, in the case of multi-jurisdictional investigations, in relation to any location within the jurisdiction of any agency involved in the investigation."

Q5. 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

Lt. Sheehan's response is as follows: *"The device would be used by a single trained member of the department, under the authorization of a supervisor, and only with consent or a search warrant."* This is the same response as in 2021, and, as we observed then, it is strangely unresponsive to the question itself. An example of a more responsive answer would be,

> "Since the device would be used by a single trained member of the department, under the authorization of a supervisor, and only with consent or a search warrant, in the context of an authorized investigation of a specific crime or crimes, and since the data retrieved would be limited to that data that is within the scope of the search warrant, Somerville PD believes that there are no privacy or anonymity rights affected by their use of GrayKey."

Of course, if this suggested text is not in fact true, and Somerville PD reserves the right to retrieve, and prosecute on the basis of, data that is beyond the scope of the original search warrant, the phone owner's privacy rights are indeed implicated. For example, a search warrant may authorize use of a GrayKey to search a phone for evidence of fraud. While using the GrayKey, the Detective accesses photographic evidence that the phone's owner used a drug illegal under state law. A limiting rule such as that in the suggested text would bar charging the owner with a crime based on this evidence, and would serve to "protect privacy, anonymity, and limit the risk of potential abuse." 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, and we advise a cautious approach such as the adoption of the rule in the suggested text, until clearer guidance is available from the courts. **The fact that most of the changes that we are recommending to the Surveillance Impact Report, and that Somerville PD has read but has not adopted, relate to this issue of over-seized data, shows that the issue is a significant one for the Council to address.**

Q6. 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)

Lt. Sheehan's response is as follows: *"This device is used specifically in conjunction with a criminal investigation. Authority to use this technology would be granted by a valid search warrant or consent, and could not be used indiscriminately."* This is the same answer as that given in 2021, and, as then, we observe that a more helpful response would be appropriate and useful to the Council. We would recommend adding language as follows:

> "The impact on Somerville residents' privacy rights is effectively mitigated by the procedural constraints specified in other parts of this STIR on the use of GrayKey, and by the penalties for misuse of the GrayKey beyond these constraints, which are as follows: …"

Q7. 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

Lt. Sheehan responds, *"There is no cost for the device as all License costs are paid for by UASI Boston,"* which is substantially similar to the response from 2021. In comments to Council which should have been in the Report, Somerville PD specifies a license cost of $38,000, but, as we also noted to you in 2021, that is not the end of it. Here, as in every other case where this language is used in a STIR, the contention that a particular technology is costless, simply indicates that Somerville PD has not considered the full costs of the technology carefully enough. **It is 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.

Q8. 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)

Lt. Sheehan responds, "There are two Detectives, one a supervisor, trained and authorized to use the technology. Any misuse of this device would lead to department discipline up to and including termination." This language - again, identical to 2021's - is clear as far as it goes, but it is unhelpful to the Council to note only the maximum penalty for misuse of the GrayKey. It is not plausible that, for every misuse, the Detective or another person improperly accessing the information would be instantly fired. It would be much more helpful, from the perspective of knowing what kind of deterrent exists for misuse, to understand what Somerville PD has applied, or would apply, as a reasonable penalty for a first-time misuse of the GrayKey.

We appreciate your attention to this important issue. We would welcome any questions or comments, at [redacted] or [redacted]

Sincerely,
Alex Marthews, Chair.