DIGITAL FOURTH

The Massachusetts campaign to protect digital data from warrantless government surveillance

November 18, 2020.

COMMENTS ON:

AGENDA ITEMS #210907-210912, APPROVAL OF SURVEILLANCE TECHNOLOGY IMPACT REPORTS

Dear members of the Legislative Matters Committee,

This is Part II of our comments on the Surveillance Technology Impact Reports. Part I was submitted yesterday, ahead of the Legislative Matters Hearing.

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,

A Marthews

ALEX MARTHEWS, Chair.

AGENDA ITEM #210907, requesting approval of the Surveillance Technology Impact Report for Covert Device Cameras.

Our major concern with this technology, and with the STIR, is that it does not appear to take into account the established procedure under Massachusetts' wiretapping law, where law enforcement may place listening devices in people's homes with a warrant once other options have been exhausted, but only in connection with organized crime and a set of pre-specified "designated offenses."[1] The STIR makes general references throughout to such a device only being placed in accordance with Massachusetts law, but it shows no awareness of the special requirements of the wiretapping statute, does not inform the City Council on the topic, and does not specify that Somerville PD will exhaust all other alternatives before deploying this intrusive kind of technology, or limit use of it to investigations of particular offenses.

The STIR as a whole is very cursory. For example, question #3 asks for *"Information describing the kind of surveillance the surveillance technology is going to conduct and what surveillance data is going to be gathered"*, and the only response is, *"This technology would be used in criminal investigations and would gather evidence of crimes."* The response should specify that the cameras would capture video data, and at what resolution, and whether in color or in black and white; and should also specify that the cameras will capture audio data (From the same room? From a floor away?). Then, it should frankly acknowledge that besides gathering "evidence of crimes", such devices will obviously also gather a whole lot of video and audio data that is (a) not evidence of any crime, or (b) evidence of other potential crimes not mentioned as part of the warrant, which, as we say, is approved only subject to investigation of a "designated offense" or offenses. Therefore, the police department needs to have a plan, before it may gain approval from the City Council, for what to do with data gathered under these categories (a) and (b). Will it be destroyed? They don't say. Who will have access to, say, recordings of suspects having sex, including video and audio, or recordings of highly personal discussions or arguments unrelated to criminal activity, and what restrictions are in place? Once again, the Police Department seems to feel that if access to this extraordinarily invasive footage is limited to the police department

[1] *See* MGL ch. 272 s. 99, available at https://malegislature.gov/laws/generallaws/partiv/titlei/chapter272/section99.

itself, there is no real privacy intrusion requiring mitigation, or outside review that is needed. We strongly disagree.

No brand of equipment is identified, and without that information, neither the City Council nor the public can assess whether it is true that data on these covert surveillance cameras will only be accessible to law enforcement anyway. It is common for home microphone-equipped devices to transmit swathes of data to the manufacturer. The police department need to specify to the City Council what the equipment actually is that they propose to obtain, so that the City Council can assess whether these devices are in fact a secure way to obtain the information. Once again, as mentioned in our testimony on other STIRs, a designated, staffed and permanent Privacy Commission would be the best way to investigate these matters on behalf of the City Council.

In sum, there is a lot more homework that needs to be done on this STIR before the City Council can reasonably feel informed as to the Police Department's plans for this technology. This STIR should be sent back for revision.

AGENDA ITEM #210908, Requesting approval of the Surveillance Technology Impact Report for GPS and Monitor.

Once again, in the response to question #3 (type of data to be gathered), the response is that the Surveillance Technology would gather *"evidence of crimes." "Evidence of crimes"* is not a type of data. Officers might discover evidence of a crime within, say, the content of communications, communications metadata, or location data (which this is), but *"evidence of crimes"* is not a responsive answer to this question.

The fact that this is *location data* points to a defect in this STIR. Supreme Court decisions in the last ten years have imposed a warrant requirement in many circumstances for the collection of GPS data. That warrant requirement hinges in many cases on how long the data is retained, and whether that data is in the form of "case notes" on how the location changed over time, or in the form of the digital data from the device itself, the warrant requirement will be the same. So, if either form of the data is retained for longer than five days, a warrant will be required for the use of this device, that might not have been required when Somerville PD first used it. The STIR should carefully consider the application of the Supreme Court's *Carpenter* decision from 2018 to their use of this Surveillance Technology, and update and resubmit their STIR.

The writing is also at some points so unclear that it is hard to know what it means. For example, in the response to question 8a, the officer writes, *"Based on the simplicity of this technology there would be monitoring other than that done be supervisor authorizing its use."* I believe that he means, *"Based on the simplicity of this technology, there would be **no** monitoring other than that done **by the** supervisor authorizing its use."*

Our belief is that the technology in question is less invasive of personal privacy than others for which STIRs have been permitted, but the STIR still requires substantial revisions before it is in a state where the City Council should approve it.

AGENDA ITEM 210909, Requesting approval of the Surveillance Technology Impact Report for GrayKey

The request to be able to deploy this Surveillance Technology should be understood in the context of policy debates over whether the government should be able to compel private companies, like Apple or Google, to break the encryption that protects their phones in general, in order for law enforcement to access specific phones associated with criminal suspects. We strongly oppose the government having such routine access.

Since that kind of compulsion is not yet legal, what police departments sometimes do instead is to use hacking tools like GrayKey to gain access to phones whose contents they cannot access via consent or via passwords. It is proper for such extraordinary access to happen only subject to a search warrant, so as far as that goes, the constraint in the STIR is proper. However, we recommend that the STIR should include responses to the following questions:

- What is the agency from which Somerville PD has borrowed a GrayKey device?
- How much does GrayKey charge that agency for each phone accessed?
- Will that charge be passed through to Somerville PD?
- If so, with what funds does Somerville PD propose to pay the charge?
- GrayShift Technologies offers two levels of GrayKey device: a basic and less intrusive offering for around $15,000, and a premium and intrusive offering at $30,000. The more expensive offering requires no Internet connection and has no limit to the number of unlocks, and is therefore potentially much more valuable to others if stolen.[2] Which is the device that Somerville PD has used?
- If the device used is the basic offering, and the lending agency later upgrades to the premium offering, does Somerville PD intend to come back to the City Council for permission to use the premium device?
- Has Somerville PD previously, or does it intend in the future, to deploy the "Magnet AXIOM" add-on to the basic GrayKey offering, which is more intrusive?[3]
- Will Somerville PD commit to use GrayKey only to access the phones belonging personally to criminal suspects?

[2] See https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/.
[3] See, for further details on their product offerings, https://www.grayshift.com/partners/magnet-forensics.

AGENDA ITEM 210910, Requesting approval of the Surveillance Technology Impact Report for License Plate Readers.

In the response to question #1, we are not clear on what a "WMS infraction" is.

The response to question #1a should specify what kinds of consequences have been imposed in the past for how many cases of inappropriate sharing of license plate information, or accessing the system for inappropriate purposes.

The judgement of the officer in the response to question #5 that "*There is no expectation of privacy for information obtained via a registration check*" is simplistic and outdated in the light of *Commonwealth v. McCarthy* (2020).

This Massachusetts Supreme Judicial Court opinion found that *"the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPR systems."*[4] The Founders had the *"intention"*, says the Court, *"to place obstacles in the way of a too permeating police surveillance"*; too permeating surveillance would prevent *"preservation of that degree of privacy against government that existed when the Fourth Amendment [and art. 14 were] adopted."*

So, whenever Somerville PD is arguing that a given technology simply makes what they do more efficient, as they do in this and other STIRs, they are thereby underlining the responsibility of the City Council in making sure that that increase in efficiency of policing does not reduce the "*degree of privacy against government"* that the Founders themselves expected.

"It is," they continue, *"objectively reasonable for individuals to expect to be free from sustained electronic monitoring of their public movements."* The Court held that four fixed ALPRs in that case, documenting the defendant's movements across the bridges to Cape Cod, did not establish a broad enough picture of the defendant's overall movements to constitute a search under the Fourth Amendment, but they also said that more extensively deployed ALPRs could create such a picture and thereby constitute a search.

[4] See a copy of this ruling at https://www.eff.org/document/commonwealth-v-mccarthy-massachusetts-supreme-judicial-court-alprs, with particular reference to its excellent explanation of the "rapid… develop[ment]" of "[t]he constitutional jurisprudence governing the technological surveillance of public space […] in the last decade."

A technology-specific policy governing the deployment and use of these ALPRs should be agreed with the City Council before any such deployment. Model policies exist that have been developed by EOPSS, though we have not reviewed them.[5] But those model policies raise an important question that the STIR leaves out. **EOPSS, at least as of 2015, was developing a centralized Commonwealth repository of ALPR data, supplied by individual police departments**, which data would be retained for one year (more if the data is at issue in a criminal case, or at the discretion of the "ALPR administrator"). So, we believe that this STIR is inadequate, in that it treats ALPR data inaccurately as being held by the RMV and subject only to their 60-day retention policy, when we would naturally expect ALPR data collected under Somerville PD's system to in fact be transmitted to the EOPSS's centralized ALPR data repository and held there for a year or more. Such a repository would in turn be more likely to trigger the concerns of the Supreme Judicial Court in *McCarthy*. Omitting this possibility misleads the Council.

Therefore, if Somerville PD seek to revive their use of ALPRs, they must attend carefully to ensure that their system of ALPRs is not such that they could in practice develop a broad or suspicionless picture of the movements of cars around the City. The most Constitutionally suspect system, taking *McCarthy* into account, will be a system where all police cars are equipped with ALPR, and pro-actively and continuously scan a substantial portion of the City's streets within a 24-hour period, looking for "hits" of expired registrations, license suspensions, and connections to existing crimes. Cursory as the STIR is, that sounds pretty much like what Somerville PD has in mind.

Consequently, we urge the City Council to reject this STIR, and require it to be revised to take into account data transfers to and retention by EOPSS, and to take into account the Supreme Judicial Court's *McCarthy* ruling, to make sure that any ALPR system proposed by Somerville PD is not "too permeating" in its gathering of information on the vehicular movements of City residents. We are happy to work with the City on their development of appropriate policy in this area.

[5] See https://data.aclum.org/wp-content/uploads/2018/06/LPR-Policies.pdf.

AGENDA ITEM 210911: Requesting approval of the Surveillance Technology Impact Report for Pole Cameras.

Once again, we see in this STIR the assertion that surveillance “in public areas” involves “no expectation of privacy”, despite a recent court ruling binding on Somerville PD and relating to the specific technology in question that pushes back on that notion.

In this instance, the case is *US v. Moore-Bush*, a ruling from July 2020 in the First Circuit Court of Appeals.