AGENDA

6:00 pm    Possible vote to amend the previous vote on Article 33

Living Wage By-Law – “complaints by concerned citizens” – changed to “concerned members of the public.” Changed back to “resident” that went out in Supplemental mailing. Advisory Committee had it reverted back to “citizen.”

A MOTION was made and seconded to amend previous vote on Article 33. By a VOTE of 17 in favor, 1 opposed and no abstentions the Advisory Committee votes to amend the previous vote.

A MOTION was made and seconded for favorable action on petitioner’s motion now “resident.” By a VOTE of 17 in favor, 1 opposed and 3 abstentions, the Advisory Committee recommends favorable action.

6:15 pm    Discussion and vote to reaffirm the authority of the AC chair & vice chair to review executive session minutes biannually, determine whether they can be released to the public, and report to the AC on the first Tuesday of April and October

A MOTION was made and seconded to reaffirm the authority of Advisory Committee chair and vice chair to review executive session minutes biannually. By a VOTE of 19 in favor, none opposed and 3 abstentions, the motion carries.

Questions and Comments

There are guidelines that are in force and used. If something is to be released, perhaps that should come to the full Advisory Committee and be a recommendation to the AC.

6:30 pm    Possible vote to amend the previous vote on Article 25

Advisory Committee recommends referral to a Moderator’s Committee, the Select Board has recommended Favorable Action. The Moderator noted the difficulty in finding qualified people to appoint.

The Surveillance Technology and Military-Type Equipment Committee is a tool of the Police Department. Casey Hatchett, who is a police officer, is serving as a member of the community and that may sway it toward law enforcement. The Committee hasn’t met that often and the issue of Facial Recognition Technology has not been on their agenda when they have met. Since then, Bernard Greene, Chair of the Committee, has put it on their agenda but petitioner still feels they are not making much progress. Other objections to the Committee, one of the members sells security cameras. This is not a committee that seems to have a sympathy or concern for civil liberties.
Less concern which committee it is referred to, but prefer default to the warrant article that bans use of facial recognition technology and move on from there.

**Q:** How many people are on the committee?  
**A:** Seven - Bernard Greene, Chair, Scott Ananian, Susan Howards, Igor Muravyov, Casey Hatchett, Amy Hummel, Lt. Paul Campbell, Police Department and Kevin Stokes, Information Technology Department

Email sent by Salvatore D’Agostino, a member of the Security Industry Association, the largest trade organization of surveillance camera and system manufacturers and system integrator, and a member of its Privacy Advisory Board, notes that protocol and procedures based on best practices should be in place before facial recognition technology is used, lest privacy rights be violated and the technology be used ineffectively.

**Q:** It was my understanding that the Police are already using some sort of technology like this, and if it no longer is an option, what else is there?  
**A:** Revert to old mechanism for posting a picture – using pre-facial recognition technology tools that were available previously –

Concern has been raised about false positives.

We seem to be the outliers. Everyone else seems to be in favor of this. I think we should be voting for this and we should be on board.

One original issue was that we didn’t think it was completely thought out. It is our job to say this article needs more work.. Not opposing a ban, but the article and its implications need to be fleshed out further.

There is an important difference between facial surveillance – looking at people real time – versus taking a person’s photo and running it through an electronic mug shot book of sorts or scan.

There is a total ban/moratorium (no end date) in front of the State House which is much stricter than what we have before us here in Brookline.

Hard to believe the State House bill wouldn’t have addressed the difference between facial recognition versus surveillance. What other things need to be carved out that are still in use?

Some things didn’t need to be carved out but the Police could have done anyway, use a phone for authentication; National Child Search Assistance Act; not prohibitive anyway so I threw it in there. I’m not in favor of using facial surveillance but if we do use it – the use should be specific, with professionals on board, who understand importance of 3rd party auditing, and probable cause batch warrants...

No objection to any number of restrictions on bulk data collection and certain technologies but literal language defining facial recognition technology and can’t use it, but what about doorbell that shows who is at the door?

The article states specifically “Brookline or Brookline Official” – using technology at home as a private individual is ok.

Facial recognition does not work reliably and works against certain racial groups. There is no justification to say we will use it and make certain groups pay the price for that.

The public can also still post things to public forums and they will have the same bias. Eyewitness identification is also notoriously unreliable, as well. None of these things seem to be 100 percent accurate.
Due process issue – accused don’t know that there are perhaps 200 other images and possible suspects.

Q: Is the Hatchet amendment personal or on behalf of the Police Department? A: Petitioner is against it.

Difference is posting a picture for public to respond/react to.

This is a warrantless search. So there need to be clear policies and rules in place to use it. By putting this ban or moratorium in place, it will be modified down the line.

Q: What is the mechanism to get the rules and regulations in place? A: Friction and bring it to Town Meeting.

Sounds like we need a committee made up of people who know about civil liberties as well as technology.

Q: What would happen after this is adopted? A: Up the Select Board to decide next steps.

Agree this is an evolving technology, and requires further study but the Town doesn’t have any immediate plans. Let’s pass this and have it sunset in 2 years forcing the friction and the committee to take it up to decide it.

When we can say have to have a probable cause back warrant in place.

If Police are unhappy with it they can create an amendment to the by law and bring it to Town meeting. Why not slow it down.

We don’t have the technology but the police use it in other capacities (Facebook, FBI, etc.) and if this passes they won’t be able to use it further. There is a regulatory framework already in place that a Moderator’s Committee could use to be able to get a clearer understanding.

A MOTION was made and seconded to amend the Advisory Committee’s previous vote (to refer to Moderator’s Committee). By a VOTE of 15 in favor, 7 opposed and 2 abstentions, the Advisory Committee amends its previous vote.

A MOTION was made and seconded for Favorable Action on the petitioner’s motion. By a VOTE of 15 in favor, 7 opposed, and 2 abstentions the Advisory Committee recommends favorable action on Warrant Article 25.

A MOTION was made and seconded for no action on the Hatchett amendment. By a VOTE of 20 in favor, none opposed and 4 abstentions, the Advisory Committee recommends no action.

Upon a MOTION made and seconded to adjourn, and voted unanimously, the meeting was adjourned at 7 pm.

Documents Presented:
- Article 25 Motion offered by the Petitioner
- Article 25 Amendment offered by Casey Hatchett, TMM12 on behalf of the Surveillance Technology and Military-Type Equipment Study Committee
- Article 25 Statement of Bernard Green, Chair of the Select Board and Chair of the Surveillance Technology and Military-Type Equipment Study Committee but speaking for himself
Dear Town Meeting Members,

My name is Salvatore (Sal) D’Agostino and I reside at 1264 Beacon Street, #5. I am writing to support the warrant article 25 on the proposed ban (moratorium) on the use of facial recognition systems in Brookline. I have been involved in the deployment of video surveillance and automated computer vision systems for nearly 40 years including the use of facial recognition systems. I am the former (volunteer) Chair of the Intelligent Transportation Society of Massachusetts, former (volunteer) Chair and President of the Identity Ecosystem Steering Group, the public private partnership established by President Obama to develop a national strategy for trusted identities in cyberspace, a member of the Security Industry Association, the largest trade organization of surveillance camera and system manufacturers and system integrators and its Privacy Advisory Board, as well as other relevant organizations and an active security and privacy practitioner. My experience with the use of video sensors for information gathering covers large and small systems in the public and private sectors in the United States and around the world. I provide guidance to end-users, manufacturers, system integrators, trade and standards organizations and consultants in their specification, design, build, installation and maintenance of security and surveillance systems.

As part of this work I have researched and make use of the privacy policies and best practices in over 100 countries. The topics of surveillance, facial recognition and automated decision making are currently evolving and being vigorously debated in many of these countries. Privacy legislation is moving forward in Massachusetts and other states, in the US Congress and in many other countries. In nearly all of these cases the evolving best practices require clarity around the justification and purpose of the use of surveillance technology, transparency about its deployment including the nature of the sharing and further use of that information, reciprocity in the recognition of the rights of individuals and proportionality and balance in the conversations and ultimately the control of the use of these increasingly widespread and powerful technologies.

At this point the warrant article makes sense. Prior to the deployment of these technologies, and in fact in the deployment of any security system, there is necessarily a need to have in place the policies and procedures that govern their use and, in particular, a way to make operational the rights that people have with regards to these systems. Not all policy meets the needs, and other needs and best practice outlined below for the deployment of these technologies. Notice and consent, in that order, are critical to any of these policies and procedures. A point of contact needs to be in place to address issues related to individual’s rights and where inquiries can take place and receive a response in a timely manner. The systems need to be deployed in a way they adhere to cybersecurity as well as privacy best practices. This includes a risk assessment that not only considers the cybersecurity risks but importantly also the privacy risks and putting in place the security and privacy controls necessary to mitigate the risks.

The deployment of surveillance technologies without having taken these steps unduly increases the security and privacy risks as well as compromises their operational effectiveness and efficiency. The extent to which controls can be put in place and their effectiveness vary greatly depending on the components, system, its integration, operation and maintenance and the ensuing governance. There must be an understanding of the level of surveillance and identification, and under what circumstances what information generated and how it is handled. It is not necessary for systems to be automatically identifying individuals and tracking them as a default in order to meet their public safety justification
and purpose. Without these steps security systems can often end up being undue and unnecessary security vulnerabilities and privacy risks. These should be aligned with overall existing privacy and security policies for information technology across Brookline’s infrastructure.

I ask the Town Meeting to require the existence and public review of a security and privacy risk assessment, surveillance policy and best practice for the existing surveillance cameras in place as a first step and to make sure that this takes into account the existing best practice in the United States and democratic societies. This necessarily needs to take place before the deployment of more advanced technologies such as facial recognition systems and other computer based automated decision-making takes place since these technologies depend on the integrity of the underlying video management system. Once this has taken place the process then needs to move to an understanding via a risk assessment and the enactment of the associated controls of the impact of deploying more advanced technologies such as facial recognition. In doing so it should make use of the national and international standards that exist for these assessments and associated controls such as those embodied in the National Institute of Standards and Technology (NIST) Security and Privacy Controls (Special Publications 800-37 and 800-53 among others), its Cybersecurity Framework, ISO (the International Organization for Standardization) 27000 and 29000 series, as well as applicable laws and consideration of existing regulations in other parts of the United States such as the California Consumer Protection Act and in other parts of the world such as the European General Data Protection Regulation (GDPR) and best practice such as that established in the UK by their Surveillance Commissioner. The process should include outreach to other communities in the US undertaking these same challenges.

One of the greatest challenges to security and privacy governance is to find the balance between benefits of public safety and the danger of unnecessary surveillance and unnecessary generation and sharing of personally identifiable information. As a practitioner I have learned that privacy and security work hand in hand, they complement, not compete. They have the same goals of maximizing safety and enabling individuals to become active participants in managing risk and having an active role in an open and productive social space, economies and society. It is my hope that the Town Meeting will follow existing best practice and governance such as mentioned in this letter to make sure this is the case in Brookline and set an example for others to follow.

Respectfully,

Sal D’Agostino
1264 Beacon Street, #5
Brookline, MA 02446