ARTICLE 25

ARTICLE 25

Submitted by: Amy Hummel, TMM12

To see if the Town will adopt the following version of a new Article 8.39 of the Town By-
Laws,

ARTICLE 8.39
BAN ON TOWN USE OF FACE SURVEILLANCE

SECTION 8.39.1 DEFINITIONS

1. "Face surveillance" shall mean an automated or semi-automated process that assists in identifying an individual, or in capturing information about an individual, based on the physical characteristics of an individual's face.
2. "Face surveillance system" shall mean any computer software or application that performs face surveillance.
3. "Brookline" shall mean any department, agency, bureau, and/or subordinate division of the Town of Brookline.
4. "Brookline official" shall mean any person or entity acting on behalf of Brookline, including any officer, employee, agent, contractor, subcontractor, or vendor.

SECTION 8.39.2 BAN ON TOWN USE OF FACE SURVEILLANCE

1. It shall be unlawful for Brookline or any Brookline official to:
    a. obtain, possess, access, or use (i) any face surveillance system, or (ii) information derived from a face surveillance system;
    b. enter into a contract or other agreement with any third party for the purpose of obtaining, possessing, accessing, or using, by or on behalf of Brookline or any Brookline official, (i) any face surveillance system, or (ii) data derived from a face surveillance system; or
    c. issue any permit or enter into a contract or other agreement that authorizes any third party to obtain, possess, access, or use (i) any face surveillance system, or (ii) information derived from a face surveillance system.

SECTION 8.39.3 ENFORCEMENT

1. Face surveillance data collected or derived in violation of this By-Law shall be considered unlawfully obtained and shall be deleted upon discovery, subject to applicable law.

2. No data collected or derived from any use of face surveillance in violation of this By-Law and no evidence derived therefrom may be received in evidence in any Town proceeding.
3. Any violation of this By-Law constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this By-Law. An action instituted under this paragraph shall be brought against the respective Town department, and the Town and, if necessary to effectuate compliance with this By-Law, any other governmental agency with possession, custody, or control of data subject to this By-Law.
4. Violations of this By-Law by a Town employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and provisions of collective bargaining agreements.
5. Nothing in this Article shall be construed to limit any individual's rights under state or federal law.

or act on anything relative thereto.

PETITIONER'S ARTICLE DESCRIPTION

Summary

- Face surveillance technology is an affront to a free society, effectively forcing everyone to wear a permanent ID badge in public;
- The software disproportionately misclassifies women and people of color;
- Face surveillance technology poses unprecedented threats to civil liberties; examples include:
    - Creating due process harms, such as shifting the current principle of "presumed innocent" to "people who have not been found guilty of a crime, yet;"
    - Normalizing the elimination of practical obscurity; and
    - Chilling the exercise of constitutionally protected free speech.
- There is no state or federal law regulating government use of face surveillance technology, meaning there are no civil rights protections in place.
- Facial surveillance supports and amplifies surveillance capitalism and the monetization of individuals' privacy.
- This warrant article furthers the goals of bills currently before the Massachusetts House and Senate (Senate Bill 1385, and House Bill 1538) which seek to place a moratorium on government use of face surveillance technology statewide. Senator Cindy Creem is the lead sponsor of the Senate bill.

Explanation

1. Facial Recognition Technology is an affront to a free society

The fundamental effect of facial recognition technology is that it is tantamount to forcing **everyone** to **wear a personal ID badge at all times**. Free people do not and should not be compelled to wear ID badges, let alone ones that are permanent, immutable and biometric.

Ordinary people who want to seek treatment for substance use disorder, visit AA meetings, seek reproductive health care, visit friends and family, attend political protests, and more cannot leave their faces at home. This technology makes it easy to track every person's public movements, habits, and associations—with the push of a button.

Facial recognition technology uses statistical measurements of people's facial features to digitally identify them in still photos, videos and in real-time footage. Tech companies claim these systems can also determine age, gender, mood, and other personal characteristics. The data gathered can easily be stored, shared and aggregated to map out individuals' activities, liaisons, patterns and preferences.

These capabilities are an anathema in a free society.

2. The Software is badly flawed and disproportionately misclassifies women and people of color

Compounding the problems inherent in facial recognition technology is that it is also highly inaccurate in classifying the faces of women, young people, and people of color. These inaccuracies disproportionately put some individuals and groups at a greater risk of harmful and traumatic "false positive" identification. The problem is exacerbated by the fact that racial and other biases are often already baked into existing databases. For example mugshots images, which are taken upon arrest, include the faces of individuals who may be entirely innocent. Moreover, when there are false positives, the trauma and the stigma impacting victims of the mistake continues long after errors are officially corrected.

3. Legislation and policies are either wholly absent or inadequate.

Like many new and emerging technologies, the use of facial recognition software is quickly becoming ubiquitous in both public and private sectors, long before most communities are able to respond with legislation. And, the monetization and ease of acquisition of surveillance technology, including facial recognition technology, make the spread of unregulated use not only certain, but swift. For example, Ring doorbell, now owned by Amazon, has partnerships with a variety of police departments, which is turning many communities in police surveillance surrogates, without meaningful civil rights and civil liberties protections. This past summer, at least one police department raffled off Ring doorbells in exchange for information sharing. The surveillance infrastructure, created entirely outside of any regulatory oversight or framework, is bad enough in-and-of-itself. Permitting unregulated facial recognition —for which Ring already has a patent—only compounds this problem,

encouraging the proliferation of a surveillance state, predicated on suspicion and distrust of everyone in our community.

4. Facial recognition technology unequivocally threatens civil liberties

According to privacy scholars Woodrow Hartzog and Evan Selinger: "facial recognition technology enables a host of other abuses and corrosive activities:

- Disproportionate impact on people of color[1] and other minority and vulnerable populations[2].
- Due process harms, which might include shifting the ideal[3] from "presumed innocent" to "people who have not been found guilty of a crime, yet."
- Facilitation of harassment[4] and violence.
- Denial of fundamental rights and opportunities, such as protection against[5] "arbitrary government tracking of one's movements, habits, relationships, interests, and thoughts."
- The suffocating restraint[6] of the relentless, perfect enforcement of law.
- The normalized elimination of practical obscurity[7],[8].
- The amplification of surveillance capitalism[9]."[10]

It's also important to know that the federal government has access to over 400 million non-criminal photos, which include state DMV and State Department photos. A 2016 Georgetown Law Center on Privacy & Technology publication, entitled The Perpetual Line-up, reported that one in two adults in America appear in government face recognition networks.[11]

How we protect our civil rights and civil liberties is up to us. By banning the Town's use of facial surveillance technology, we act to meaningfully protect our civil rights and civil liberties, and protect our fundamental freedoms to come and go about our lives in relative anonymity, free from overreaching surveillance and without a compulsory biometric ID badge.

---

[1] https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/
[2] https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/
[3] https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-slaughter-and-stephanie-hare-2018-07
[4] https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/
[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394838
[6] http://www.businessinsider.com/how-china-uses-facial-recognition-technology-surveillance-2018-2
[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866
[8] https://idlewords.com/2019/06/the_new_wilderness.htm
[9] http://www.shoshanazuboff.com/new/recent-publications-and-interviews/big-other-surveillance-capitalism-and-the-prospects-of-an-information-civilization/
[10] https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66
[11] https://www.perpetuallineup.org

5. What Brookline Can Do: Ban facial recognition technology in our town – and support state legislative action

Without a ban on facial recognition**,** the technology is likely to become entrenched without meaningful public knowledge or input, and it will become increasingly difficult to legislate and regulate the longer it is unfettered.

Some communities are beginning to respond and Brookline should be among these leaders. This particular technology threatens civil rights and civil liberties so profoundly that the tech hub of San Francisco in May became the first city in the nation to ban its government from using it; Somerville followed shortly after, and Cambridge is now considering a ban, which seems likely to pass this fall. Other forward thinking communities are working to do the same.

The Massachusetts state legislature is currently considering Senate Bill 1385, (an Act Establishing A Moratorium On Face Recognition and Other Remote Biometric Surveillance Systems), and House Bill 1538, (an Act Relative To Unregulated Face Recognition and Emerging Biometric Surveillance Technologies). The bills would make it unlawful for government entities in the Commonwealth to acquire, possess, access, or use face recognition or any at-a-distance biometric surveillance system, or acquire, possess access, or use information derived from a facial recognition system or from biometric surveillance systems operated by another entity.

These bills also create a private right of action with both legal and equitable remedies, as well as sanctions against government officials who violate the provisions contained therein.

By passing a similar law locally, we can join our neighbors who recognize the dangers the technology presents to a free society, and demonstrate our support for the aforementioned House and Senate Bills seeking to do the same. We do not have to wait for digital dystopia; we can and must act now to protect and preserve our freedoms for the next generation of Brookline residents.

_____

SELECT BOARD'S RECOMMENDATION

ADVISORY COMMITTEE'S RECOMMENDATION

XXX