Kade Crockford
Director, Technology for Liberty Program
(617) 482-3170 ext. 346

Emiliano Falcon-Morano,
Policy Counsel, Technology for Liberty Program
(617) 482-3170 ext. 402

June 9, 2020

Boston City Council
Committee on Government Operations
City of Boston

Re: Proposed Ordinance Banning Face Surveillance in the City of Boston

Dear Chair Edwards, members of the Committee, and Boston City Councilors,

We write on behalf of the ACLU of Massachusetts ("ACLU") and our over 10,000 members and supporters in the City of Boston to express our strongest support for the proposed ordinance introduced by Councilors Wu and Arroyo to ban the municipal government's use of a dystopian, biased, anti-democratic technology. We strongly urge the Council to work quickly to pass this crucial law reform.

Face surveillance technology poses unprecedented threats to civil rights, civil liberties, and open, democratic society. But we don't have to live in a dystopia with constant government tracking of our every movement. We can and must act now, to protect racial justice, immigrant rights, and privacy, by passing a prohibition on the City's use of this unreliable, biased, and dangerous technology.

Banning Face Surveillance in Boston is More Important Now than Ever

We are currently living in the midst of two raging crises: The Covid-19 pandemic and the epidemic of racism and white supremacy that has afflicted this country for over 400 years.

Over the past two weeks, tens of thousands of Bostonians have raised their voices in the streets, online, and in communications to the City Council. Their message has been clear: The milquetoast reforms of the past are insufficient to address these crises and to protect Black lives. Instead of tinkering around the edges, we must act boldly to divest from policing and other systems of control—like surveillance—and invest in what communities need: housing, healthcare, good jobs, education, social services, public transportation, the arts, parks, and other government programs that lift people up instead of holding them back. These protests and the protesters' cries for justice highlight the urgency of prohibiting the Boston Police Department and all other City agencies from spending tax dollars on technology that undermines our core democratic values. Face surveillance technology would—in the absence of a ban—undoubtedly be used disproportionately against Black and brown Bostonians, as well as those who protest their abuse at the hands of police and structural inequity more broadly.

Meanwhile, we collectively remain at the mercy of the Covid-19 virus, which is wreaking havoc in communities of color. As governments respond to the ongoing pandemic and its economic toll

worsens, the pull of supposedly "smart" technologies to assist with "re-opening" the economy will become stronger.[1] Already, governments in China and Russia are using face surveillance networks to enforce quarantine orders and to control access to residential areas—one piece of expansive surveillance apparatuses built to enforce social control, now used under the guise of public health.[2] Just last week, a company that contracts with the Boston Police Department announced upgrades to its software to enable pandemic related video surveillance, including automated mask and social distance detection.[3]

But as experts attest, trust in government is a requirement for effective pandemic response.[4] Face surveillance undermines that trust, making this ordinance more crucial now than ever before.[5]

Banning face surveillance in Boston is not an academic matter, or even a nice-to-have prophylactic meant to ward off possible harms in the distant future. Rather, it is an urgent necessity brought on by decades of secretive police department acquisitions of surveillance technology, accompanied by a complete absence of independent oversight and accountability. Indeed, **public records obtained by ACLU show that with one software update, the City of Boston and even surrounding cities and towns would be blanketed in exactly the type of dystopian face surveillance technology deployed by the authoritarian governments in China and Russia.** The Boston Police Department currently uses video analytics software called BriefCam, to automatically analyze video data. BriefCam's most recent software version includes facial recognition.[6] That means with one software update, Boston Police and other regional law enforcement would be able to track every City Councilor's every whereabouts across the city, in real time and through historic video data, merely with the push of a button.[7]

Under current law, the Police Department and other city agencies do not need the express permission of the City Council to implement facial surveillance technology. There is currently no law on the books in Massachusetts or federally providing civil rights or civil liberties protections

---

[1] Kirsten Grind et al., "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits," The Wall Street Journal, March 2020. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841

[2] The Independent, "CCTV: For Moscow's Quarantined, 100,000 Cameras Watching," The Independent, March 2020. https://www.independent.co.ug/cctv-for-moscows-quarantined-100000-cameras-are-watching/. See also Maya Wang, "China: Fighting COVID-19 With Automated Tyranny," Human Rights Watch, April 1, 2020. https://www.hrw.org/news/2020/04/01/china-fighting-covid-19-automated-tyranny

[3] BriefCam press release, June 4, 2020. https://www.valdostadailytimes.com/news/business/briefcam-announces-video-analytics-innovation-for-contact-tracing-physical-distancing-occupancy-management-and-face-mask/article_c26e638f-8db0-5b07-8989-8d40de2a9ca1.html.

[4] Jana Kunicova et al., "We're All In This Together: Collective Action And Trust In The Age Of Coronavirus," World Bank Blogs, April 2020. https://blogs.worldbank.org/governance/were-all-together-collective-action-and-trust-age-coronavirus

[5] A poll conducted last Spring shows that 9 in 10 Massachusetts voters oppose government tracking them using face surveillance technology. See ACLU of Massachusetts, "Massachusetts Statewide Poll," June 2019. https://www.aclum.org/sites/default/files/field_documents/press_pause_slide_deck_final.pdf

[6] BriefCam, "BriefCam Announces Real-Time Face Recognition for Enhanced Situational Awareness," BriefCam Press Release, November 2018. https://www.briefcam.com/company/press-releases/briefcam-announces-real-time-face-recognition-for-enhanced-situational-awareness/. See also BriefCam, "Best In-Class Face Recognition Technology," BriefCam. https://www.briefcam.com/technology/facial-recognition/ (last visited May 18, 2020)

[7] Unfortunately, in the absence of a ban, the Department may have already made such an upgrade; an outstanding ACLU public records request to the BPD seeking information about its current BriefCam contract has gone unanswered for weeks.

to guard against abuses or misuses of face surveillance tech. It is therefore urgent that the Council press pause now, by passing this ban. Only then can the Council and the people of Boston be sure that this technology won't creep into government use in the shadows, absent any regulation, oversight, or minimum accuracy requirements.

Thankfully, records indicate many police officials in the region agree that using face surveillance technology would not be worth the privacy violations it would unavoidably entail.[8] The ACLU applauds that attitude, and asks the City Council to enshrine it in law here in Boston.

Face Surveillance Enables Mass Tracking of Public Life

Face surveillance technology uses algorithms designed to analyze images of human faces, and can be used to identify and track people en masse, often without their knowledge or consent.[9] In one form of facial surveillance technology, a computer program analyzes an image of a person's face, taking measurements of their facial features to create a unique "faceprint." Face surveillance algorithms then use these faceprints, in combination with databases like the driver's license system at the Registry of Motor Vehicles and surveillance camera networks, to identify and track people in public, through video surveillance footage and still images.

Some companies are also selling so-called "emotion detection" facial surveillance systems, which they claim can determine whether someone is happy, sad, honest, or deceitful. But using face surveillance technology to try to determine how someone is feeling is a fool's errand. Independent research concludes it is not possible to discern how someone is feeling by judging the physical characteristics of their face.[10]

There are three primary ways face surveillance systems can be used by governments:

(1) **Identification**: Authorities have a photo, image, or even a drawing of someone they want to identify. Using face surveillance, authorities can automatically scan vast databases of labeled images (for example, a driver's license database) to find one or more faceprints that may or may not "match" their photo.

(2) **Tracking**: Governments can use networks of surveillance cameras to scan for and track individuals and groups of people, creating persistent records of every person's public movements, habits, and associations—merely with the push of a button. The People's Republic of China uses face surveillance technology in this way to control

[8] In a meeting of members of the Metro Boston Homeland Security Region's surveillance camera working group on July 15, 2015, officials including a representative from the Boston Police Department discussed the possibility of using facial recognition on the region's thousands of networked surveillance cameras. The notes from the meeting state: "Discussion on facial recognition. Most in attendance are not interested due to privacy considerations." See: Notes from Metro Boston Homeland Security Region meeting on the Critical Infrastructure Monitoring System (CIMS, the regional surveillance camera network), page 4. http://data.aclum.org/wp-content/uploads/2020/06/UASI-face-recognition-discussion.pdf.

[9] See also Joy Buolamwini et al., "Facial Recognition Technologies: A Primer," Algorithmic Justice League, May 2020. https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[10] Lisa Feldman Barrett et al., "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," Psychological Science in the Public Interest 20-1, July 2019, pp. 1–68. https://journals.sagepub.com/doi/10.1177/1529100619832930.

and oppress religious minorities. Local governments in the United States, including in Chicago and Detroit, have likewise overlaid face surveillance technologies on their public surveillance camera networks.[11]

(3) **Analysis**: So-called "emotion detection" can be used to assign emotional attributes based on a person's facial expressions. For example, a system may tell a government user that someone is agitated, anxious, or angry. (Again, research indicates this is not a scientifically sound project.[12])

Face Surveillance Is Unregulated, Biased, And A Threat To Fundamental Rights

The ACLU has three primary areas of concern regarding face surveillance technologies, pertaining to (i) unregulated use of the technology alongside aggressive company marketing; (ii) specific harms to communities of color, youth, transgender people, and immigrants; and (iii) civil rights, civil liberties, and other core constitutional concerns.

(i) Unregulated Use of the Technology Amidst Aggressive Company Marketing

Face surveillance is currently unregulated in Massachusetts. There is not a single law on the books at either the state or federal level providing guardrails for government use, or civil rights protections for individuals. Nonetheless, the spread of this technology is occurring in the dark, absent public debate or democratic oversight. Nationwide, federal, state, and local government agencies are adopting face surveillance technologies despite the absence of privacy regulations, the technology's biases and inaccuracies, and the threats it poses to free and open societies.

Behind closed doors, face surveillance companies are preying on our local governments, trying to use our families and communities as guinea pigs for their private financial gain. In Plymouth, Massachusetts, for example, emails obtained by the ACLU show the police chief was in talks with Suspect Technologies, a face surveillance manufacturer, for two years—entirely in secret.[13] The emails show the police department planned to deploy inaccurate, potentially biased face surveillance technology on public surveillance cameras throughout town, despite the fact that the company's own CEO acknowledged his product might only work about 30 percent of the time. Thankfully, the plans were scrapped after the ACLU exposed them to the public.[14]

Another company, Clearview AI, has been marketing its technology directly to individual police officers and detectives across the United States, raising serious concerns about the democratic process, the chain of command, and transparency and accountability. In some cases, individual detectives have tested the software without the knowledge or consent of their supervisors—let alone

[11] Clare Garvey & Laura Moy, "America Under Watch," Georgetown University, 2019. https://www.americaunderwatch.com/
[12] Lauren Rhue, "Emotion-reading tech fails the racial bias test," Phys.org, January 2019. https://phys.org/news/2019-01-emotion-reading-tech-racial-bias.html.
[13] See ACLU of Massachusetts, "Plymouth Police Department Face Surveillance Emails," ACLU of Massachusetts. https://data.aclum.org/public-records/plymouth-police-department-face-surveillance-emails/
[14] Joseph Cox, "They Would Go Absolutely Nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work With Cops," VICE, May 2019. https://www.vice.com/en_us/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies

the Mayor, City Council, or general public.[15] Boston's City Council must pass a clear law banning face surveillance technology in government to ensure every employee of every government agency in the City understands that their use of the technology at work is unlawful.

(ii) Face Surveillance Poses Special Risks to Black People, Youth, Elderly People, Women, Transgender People, and Immigrant Communities

Face surveillance is dangerous when it works, and when it doesn't. Facial recognition technology is not always accurate. And these inaccuracies are more likely to unfairly harm people of color, youth, the elderly, women, and transgender people.

The use of facial surveillance technologies undermines Boston's commitment to racial justice. Face surveillance in the hands of government exacerbates the disproportionate harm these communities suffer from overpolicing in at least four ways.

(1) Rigorous, academic peer-reviewed studies show certain face surveillance algorithms have high failure rates when evaluating the faces of Black women.[16] A federal government study published in December 2019 found that face recognition algorithms were much more likely to fail when attempting to identify the faces of people of color, children, the elderly, and women.[17]
(2) Renowned psychologists have found that attempting to determine a person's emotional state from their facial expressions alone is a "futile exercise."[18] Moreover, a study found that so-called "emotion detection" software inaccurately classified Black men's faces as angrier and more contemptuous than white faces, even in pictures where the men are smiling.[19]
(3) Face surveillance systems in use by law enforcement frequently compare images against mugshot databases. Numerous studies, including those examining trends in Massachusetts, have shown that Black and Latine people are many times more likely to face arrest for a variety of crimes than white people, even when whites commit those crimes at the same rates.[20] Making matters worse, arrest does not equal guilt. Using mugshot databases for face surveillance searches exacerbates historical inequities by recycling that bias through new technology, and unfairly scrutinizing people who have long been targets of disproportionate police attention.

---

[15] Ryan Mac et al., "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," Buzzfeed, February 27, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[16] Joy Buolamwini et al., "Gender Shades," MIT Media Lab, available at https://www.media.mit.edu/projects/gender-shades/overview/
[17] Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology, December 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[18] Khalida Sarwari, "You Think You Can Read Facial Expression? You're Wrong," News@Northeastern, July 2019. https://news.northeastern.edu/2019/07/19/northeastern-university-professor-says-we-cant-gauge-emotions-from-facial-expressions-alone/
[19] Rhue, supra note 8.
[20] See Shira Schoenberg, "Study tracks racial disparities in Massachusetts marijuana arrests," MassLive, April 2019. https://www.masslive.com/news/2019/04/study-tracks-racial-disparities-in-massachusetts-marijuana-arrests.html and Massachusetts Cannabis Control Commission, "A Baseline Review and Assessment of Cannabis Use and Public Safety," April 2019. https://mass-cannabis-control.com/wp-content/uploads/2019/04/1.-RR2-94C-Violations-FINAL.pdf. See also ACLU of Massachusetts, "Ending Racist Stop And Frisk." https://www.aclum.org/en/ending-racist-stop-and-frisk.

(4) Even if face surveillance systems were perfectly accurate, and even if the police did not use mugshot databases for facial recognition searches, history suggests these technologies will be disparately deployed in low-income and Black and brown communities, and against immigrants.[21] This has the impact not only of subjecting traditionally oppressed groups of people to yet more surveillance and tracking, but also of making other, less policed communities even more invisible to law enforcement.

Face surveillance is especially dangerous when it is used on children. Research that tested five "top performing commercial-off-the shelf" face recognition systems shows these systems "perform poorer on children than on adults."[22] As children grow, their faces change shape, but face surveillance systems optimized for use on adults do not account for these changes. Despite these problems, some school districts are experimenting with the use of face surveillance to track and monitor students, teachers, staff, and visitors.[23] Schools should be safe environments for students to learn, explore their identities and intellects, and play. Face surveillance technology threatens that environment. The use of face surveillance in schools transforms students into perpetual suspects, where each and every one of their movements can be automatically monitored and catalogued. Using this kind of invasive surveillance technology in our schools negatively impacts students' ability to explore new ideas, express their creativity, and engage in student dissent.

Making matters worse, face surveillance technology is prone to misgendering transgender people.[24] Research shows that automatic gender recognition, a subfield of face surveillance technology, "consistently operationalises gender in a trans-exclusive way, and consequently carries disproportionate risk for trans people subject to it."[25] At a time when transgender rights are under attack nationwide, Boston must do everything in its power to protect this marginalized group.[26]

---

[21] For example, the Boston Police Department temporarily paused its license plate reader surveillance program after a reporter obtained records indicating the cameras were largely placed in Black and brown neighborhoods. https://www.aclu.org/blog/privacy-technology/location-tracking/data-suggests-boston-police-targeted-black-working-class. The Boston Police Department also ran a discriminatory social media surveillance program, in which it searched for words associated with Muslim religious practice and Black Lives Matter. https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/. The Boston Police Department's Field, Interrogation, Observation database reflects surveillance disproportionately targeting Black Bostonians. https://www.aclum.org/sites/default/files/wp-content/uploads/2015/06/reports-black-brown-and-targeted.pdf. And the BPD's Gang Database reflects even more extreme racial disparities in BPD surveillance practices. https://www.wbur.org/news/2019/07/26/boston-police-gang-database-immigration.

[22] Nisha Srinivas et al., "Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults," The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2019. http://openaccess.thecvf.com/content_CVPRW_2019/papers/BEFA/Srinivas_Face_Recognition_Algorithm_Bias_Performance_Differences_on_Images_of_Children_CVPRW_2019_paper.pdf

[23] Tristan Greene, "Why US Public Schools' Creepy Use Of Surveillance AI Should Frighten You," The Next Web, July 2019. https://thenextweb.com/artificial-intelligence/2019/07/23/why-us-public-schools-creepy-use-of-surveillance-ai-should-frighten-you/

[24] Matthew Gault, "Facial Recognition Software Regularly Misgenders Trans People," Feb. 19, 2019. https://www.vice.com/en_us/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people

[25] Os Keyes, "The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition," University of Washington, USA, November 2018. https://ironholds.org/resources/papers/agr_paper.pdf

[26] Rebecca Klein, "Trump Admin To Transgender Kids: We Won't Deal With Your Civil Rights Complaints," The Huffington Post, January 2018, available at https://www.huffpost.com/entry/transgender-office-for-civil-rights_n_5a5688ade4b08a1f624b2144?guccounter=1

Finally, the use of face surveillance technology harms immigrant families. In this political climate, immigrants are already fearful of engagement with public institutions, including schools and local police, and face surveillance systems would further chill immigrant participation in public life.

Boston should be a city that is a safe place for all people, including immigrants, people of color, children, the elderly, women, and transgender people. A ban on the use of face surveillance ensures Boston remains a welcoming and safe place for all.

(iii) Civil Rights, Civil Liberties, and Constitutional Concerns

Face surveillance poses a threat to Boston residents' and visitors' civil rights and civil liberties. Especially concerning is how this technology affects our privacy interests, and our rights to freedom of expression and association. Face surveillance technology connected to public surveillance camera feeds in Boston would facilitate government monitoring of every person's public movements, associations, and habits—not just on one day, but on all days; in real time and retroactively—merely with the push of a button.

If the government can track everyone who goes to a place of worship, a political rally, or seeks healthcare for reproductive health or substance use, we lose our freedom to speak our minds, freely criticize the government, pray to the god we want, and access healthcare in private. Boston residents and visitors should feel free to visit the cannabis shop, the Black Live Matter protest, or the abortion clinic without fear that their attendance is secretly being tracked and catalogued by government officials.

These are not hypothetical dangers taken from a Black Mirror episode: This technology is currently being used to conduct precisely this kind of dystopian monitoring. For example, the authoritarian government in China is deploying facial surveillance to control and oppress the religious minority Uighur population. The technology is so invasive that Chinese authorities use it to track how many times and where individual people pray, whether they enter their homes through the front or back door, and their social and professional associations and contacts.[27]

Closer to home, the Detroit Police Department has been using face surveillance on its networked public surveillance camera system for over two years. The system was established in secret, without public debate, legislative authorization, or regulations to protect civil rights and liberties.[28]

Moreover, face surveillance raises significant constitutional concerns, including the following:

(1) **Face surveillance enables the government to identify individuals while they are exercising rights protected by the First Amendment**. Our rights to freedom of speech, freedom of the press, freedom of association, and free exercise of religion are all at risk when the government can easily and continuously track everyone's public movements. Persistent tracking like that facilitated by face surveillance networks can have a chilling

[27] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," April 14, 2019, New York Times. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[28] Garvey & Moy, supra note 7.

effect, as people will be less likely to exercise their rights if they suspect their every movement and association is being catalogued by the government.

(2) **Face surveillance threatens our Fourth Amendment right to be left alone**. The highest courts in the United States and the Commonwealth have both held that the government cannot use technological advancements to track our public movements via our cellphones without judicial intervention.[29] The government's use of face surveillance raises similar constitutional concerns, as this technology allows the governments to keep tabs on all of our public movements and activities easily, efficiently, and without our knowledge. But unlike cellphones, we cannot leave our faces at home. Face surveillance is even more invasive, and more inaccurate, than cell phone location tracking.

(3) **Failing to disclose the use of face surveillance jeopardizes our Fourteenth Amendment Due Process rights**. Due process requires the government to disclose potentially exculpatory information to defense attorneys. Failing to disclose to defendants how face surveillance was used violates this constitutionally protected right and threatens defendants' ability to have a fair trial. The government routinely discloses information regarding human eyewitnesses; its constitutional obligations should be no different for identifications stemming from face surveillance. Despite this, in Massachusetts law enforcement agencies including the Boston Police Department have failed to notify defendants when they have used facial recognition to identify them in a criminal investigation. This is a direct threat to due process rights and it must be addressed immediately, by banning the technology's use in government.

As Northeastern professor Woodrow Hartzog has observed, face surveillance is a perfect tool for social control.[30] People in Boston must be able to visit health clinics, synagogues and mosques, friends and family, political protests, and doctors' offices without fear that a government agent is secretly keeping tabs of their every movement.

Boston Must Chart A Different Course

Ultimately, faced with the question of whether Boston should prohibit the use of face surveillance by government actors in the City, councilors ought to consider what kind of community they want to foster into the 21st century. Constant surveillance has negative effects on health, well-being, and community trust. Surveillance increases not only our fears and uncertainty, but also personal anxiety.[31] Privacy advocates have long warned about the psychological consequences of being watched and observed by unaccountable, faceless entities.[32] Face surveillance magnifies these concerns and extends them into truly new and frightening territory, by totalizing the surveillance of our movements in public space.

Following the bans in the cities of Somerville, Cambridge, Brookline, Springfield, and Northampton here in Massachusetts, and Berkeley, San Francisco, and Oakland, in California, Boston has the chance to lead the nation by becoming the largest city on the East Coast to press pause on face

[29] See Carpenter v. United States, 138 S. Ct. 2206 (2018) and Com. v. Augustine, 467 Mass. 230 (2014).
[30] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," The New York Times, April 2019. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[31] Kaleigh Rogers, "What Constant Surveillance Does To Your Brain," Vice, November 2018. https://www.vice.com/en_us/article/pa5d9g/what-constant-surveillance-does-to-your-brain
[32] John Borland, "Maybe Surveillance Is Bad, After All," WIRED, August 2007. https://www.wired.com/2007/08/maybe-surveilla/

surveillance. The face surveillance ban before you will, if enacted, protect people from government use of a dangerous, dystopian, racially-biased technology in the City of Boston, advancing racial, economic, and immigration justice, and protecting democracy, open society, and liberty in the City. Please support it with your vote and your advocacy.

Please do not hesitate to contact us if you have any questions about the proposed ordinance or its implications. Thank you for your consideration.

Sincerely,

Kade Crockford
Director
Technology for Liberty Program
ACLU of Massachusetts

Emiliano Falcon-Morano
Policy Counsel
Technology for Liberty Program
ACLU of Massachusetts