June 8, 2020

Docket #0683
City Council, City Hall
5th Floor
Boston MA 02201

Testimony in Support of Ordinance
Banning Face Surveillance in Boston

Dear City Councilors,

We are writing in support of the ordinance banning face surveillance in Boston presented by Councilors Wu and Arroyo. We are professors of law and philosophy, respectively, who have been researching and writing about the risks of facial recognition technologies for over seven years. Our testimony draws from our research and we make these comments in our personal, academic capacity. We are not serving as an advocate for any particular organization.

Thanks to advances in artificial intelligence, proliferating photography, diminishing costs of storing big data sets in the cloud, and cheap access to sophisticated facial recognition technology systems, facial recognition technology has become the most dangerous surveillance tool ever invented. Despite posing substantial threats to civil liberties, privacy, and democratic accountability, it is subject to zero statutory or administrative regulation in Boston. Due to the absence of adequate policies for preventing predictable and egregious harms, we are writing to offer emphatic support for the ordinance banning facial recognition technology in Boston. This ordinance would protect against a perfect tool of oppression by instituting a citywide ban on government use of face surveillance tools in Boston. We believe the ordinance is justified and necessary.

Deep Legal Gaps

For some time, police in the United States have had access to information-rich databases that store details like names, demographic data, and license plate numbers. However, a comprehensive database of innocent Americans' biometrics has never been created. Indeed, Democrats and Republicans alike have rejected official proposals to build such a registry by adopting a national biometric ID card. Unfortunately, law enforcement agencies risk creating an equally dangerous repository by availing themselves of information stored in a patchwork of facial recognition technology databases, including ones that contain mugshot (crucially, not everyone who is arrested ends up being convicted) and driver's license photos.[1]

This consolidation is occurring because facial recognition technology is a textbook example of the speed of innovation outpacing the velocity of regulation. Congress has not restricted how the government can use facial recognition technology. Courts have not meaningfully limited the government's use of it, and are ill-equipped to regulate its use. Currently, no rule exists in Boston to protect the public from civil rights or civil liberties violations resulting from government use of face surveillance technology.

As a result, in the absence of regulation, police can take your picture and check it against a facial recognition technology database without your permission, judicial oversight, probable cause, or reasonable suspicion, even if you are engaging in lawful activities, so long as you are in public or using the open internet. Such permissiveness with facial recognition technology extends far beyond discrete interactions. It authorizes law enforcement to engage in ongoing, retrospective, and real-time face surveillance with few barriers by monitoring public places—remotely and automatically, with the push of a button.

Why does law endorsement have such extensive legal latitude for using facial recognition technology that federal rules haven't been established that are comparable to the ones in place for conducting wiretaps? Historically, the Fourth Amendment, which protects against unreasonable searches and seizures, hasn't covered what people willingly expose in public. Fortunately, the law has started recognizing problems with this view, and we believe it's a grave mistake not to take their concerns seriously. Justices in recent Supreme Court cases acknowledge that advances in surveillance technology, which make tracking people at scale incredibly cheap and easy, are challenging traditional conceptions of privacy.[2] Most recently, in the majority opinion for the 2018 Supreme Court case, *Carpenter v. United States*, Chief Justice Roberts declared, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'"[3]

[1] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition In America." https://www.perpetuallineup.org

[2] Woodrow Hartzog and Evan Selinger, "Surveillance as Loss of Obscurity" *Washington and Lee Law Review* 72, 3 (Summer 2015): 1343-1387.

[3] *Carpenter v. United States*. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

To put the massive power of facial recognition technology in perspective, it's helpful to clarify why it isn't just, as some allege, merely the new fingerprint technology. Since physical contact isn't required to take a photograph, and hiding your face is more suspicious than covering your hands in many circumstances, it is much easier to capture a probe photo than a fingerprint from far away and in bulk (group photos), with less resistance (because less physically intrusive), and through non-transparent means. Furthermore, there is more information available through facial recognition databases than ones with fingerprint information. For example, the Government Accountability Office states that the FBI can scan approximately 640 million pictures (mugshot, driver's license, and passport photos), but only has 145 million fingerprint records in its database.[5] Finally, unlike fingerprints, which can only be used to establish personal identity, faces can be analyzed for additional information (e.g., emotions and demographics) and are the linchpin between our online and offline lives that can link together our real name, anonymous, and pseudonymous activities.

Harms

There are many ways that law enforcement's use of facial recognition technology can harm people.

Historically, government surveillance has disproportionately targeted marginalized communities, specifically people of color. Without robust regulation, these communities have good reason to be concerned that history will repeat itself--that they will be excessively surveilled even while engaging in law-abiding conduct, and that some of the interactions could result in verbal abuse and physical violence. This concern is exacerbated by the lack of transparency surrounding law enforcement's use of the technology and the fact that while facial recognition systems are improving, inaccuracies

[4] Matt Rocheleau, "State Scans Mass. License Photos to Find Matches With Suspects" *Boston Globe* December 20, 2016. https://www.bostonglobe.com/metro/2016/12/20/state-scans-mass-driver-license-photos-find-matches-with-suspects/xyVIxWkPL95hQbx4sUI2WM/story.html

[5] Ronald Bailey, "Is Facial Recognition the New Fingerprinting--or Something Much Worse?" *Reason* July 8, 2019. https://reason.com/2019/07/08/is-facial-recognition-the-new-fingerprinting-or-something-much-worse/

remain. Even though their use can result in false positives or negatives that affect everyone, the mostly likely errors will be directed against women and people of color, the groups that use of the technology displays the greatest biases against.[6]

Georgetown University researcher Clare Garvie thus aptly states:

> "What happens if a system like this gets it wrong? A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn't commit. A mistake by a face-scanning surveillance system on a body camera could be lethal. An officer alerted to a potential threat to public safety or to himself, must, in an instant, decide whether to draw his weapon. A false alert places an innocent person in those crosshairs."[7]

And Jay Stanley, Senior Policy Analyst at the ACLU, rightly notes: "...a 'smart' body camera falsely telling a police officer that someone is hostile and full of anger could contribute to an unnecessary shooting."[8]

Facial recognition software has already contributed to a serious case of mistaken identity, resulting in a Brown University student and Muslim activist erroneously being identified as a bombing suspect.[9] But even if, hypothetically, facial recognition technology ever became 100 percent accurate problems would remain. In fact, accurate facial recognition might even be more dangerous to the people of Boston because it will be used more often and invested in more heavily. For starters, the lack of robust standards governing police use can contribute to mistakes. Images of photos where people have their eyes closed or only parts of their faces are visible can be modeled with proxy information that distorts the results. And proxy images can be used as probe photos when eye witness

[6] Edward Ongweso Jr., "Racial Bias in AI Isn't Getting Better and Neither Are Researchers' Excuses." *Motherboard* June 29, 2019.
https://www.vice.com/en_us/article/8xzwgx/racial-bias-in-ai-isnt-getting-better-and-neither-are-researchers-excuses

[7] Clare Garvie, "Facial Recognition Threatens Our Fundamental Rights." *The Washington Post* July 19, 2019.
https://www.washingtonpost.com/opinions/facial-recognition-threatens-our-fundamental-rights/2018/07/19/a102703a-8b64-11e8-8b20-60521f27434e_story.html

[8] Jay Stanley, "The Dawn of Robot Surveillance: AI,Video Analytics, and Privacy." June 17, 2019.
https://www.aclu.org/report/dawn-robot-surveillance

[9] Jeremy Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect." *The Boston Globe* April 28, 2019.
https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html

descriptions describe what a suspect looks like--as was the case when an image of the celebrity Woody Harrelson served that role.[10]

Furthermore, law enforcement use of facial recognition technology could create a pervasive atmosphere of chill. By making it easier for the police to engage in surveillance, more surveillance can occur, the mere prospect of which could routinely prevent citizens from engaging in First Amendment-protected activities, such as free association and free expression (from protesting to worshipping), for fear of ending up on government watchlists. It's also reasonable to expect that due process ideals could be weakened through a technologically-induced shift whereby citizens stop being presumed innocent and become coded as risk profiles with varying potential to commit crimes. Should this happen, the government will find it too easy to excessively police minor infractions as pretexts to cover up more invasive motives and secretly monitor gadflies, like journalists and whistleblowers. The net result would be anxious and oppressed citizens who are denied fundamental opportunities and rights.

For all the reasons outlined above, we strongly support the ordinance banning face surveillance in Boston. It's the best approach for preventing an Orwellian future and ensuring that the city of Boston remain a place where core constitutional rights and liberties remain protected.

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University

Evan Selinger
Professor of Philosophy
Rochester Institute of Technology

[10] Clare Garvie, "Garbage In, Garbage Out." May 16, 2019. https://www.flawedfacedata.com/