ACLU
Massachusetts

PRESS PAUSE
ON FACE SURVEILLANCE

October 22, 2019

Joint Committee on the Judiciary
Sen. James Eldridge & Rep. Claire Cronin, Co-Chairs

Testimony in Support of S.1385 and H. 1538
Moratorium on Government Use of Face Surveillance Technologies

Dear Senator Eldridge, Representative Cronin, and members of the committee,

The ACLU of Massachusetts, on behalf of nearly 100,000 members and supporters across the Commonwealth, offers our strongest support for S.1385 and H.1538, legislation to establish a moratorium on government use of face recognition and emerging biometric surveillance technologies.

Face surveillance technology poses unprecedented threats to core civil rights and civil liberties, impedes racial justice, and undermines our open, free, democratic society. The technology can be used not only to identify a person in a video or a still image, but also to turn existing surveillance camera networks into inescapable dragnets, enabling the mass tracking of people's movements, habits, and associations. This this could all happen in secret, without the public's knowledge or consent, with merely the push of a button. Thankfully, the most dangerous deployments of the technology are not, to our knowledge, occurring in Massachusetts—yet. But cities from Detroit to Chicago, not to mention entire regions of countries like China, are already experimenting with this fundamentally authoritarian form of surveillance.[1] And according to documents obtained by the ACLU, the City of Boston and the surrounding metropolitan region are one software update away from doing the same.

Face surveillance technology is dangerous when it works, and when it doesn't. According to research by world-renowned MIT scientist Joy Buolamwini, even face surveillance algorithms sold by the most prominent technology companies exhibit troubling racial and gender bias. Meanwhile, smaller start-ups like Cambridge-based Suspect Technologies have been pushing their products on Massachusetts municipal police departments, despite the fact that—by the vendor's own admissions—their systems may work only 30 percent of the time.[2] And when other governments have tested face recognition technology "in the wild," on live video surveillance camera feeds, it has failed at staggering rates—upwards of 90 percent in some cases.[3]

[1] Clare Garvey and Laura Moy, "America Under Watch: Face Surveillance in the United States," May 16, 2019, Georgetown Law Center on Privacy and Technology. https://www.americaunderwatch.com/.

[2] Email from Suspect Technologies CEO Jacob Sniff to Plymouth Police Department, November 19, 2017, obtained via public records request: "I do think that with a decent database to match from, at least 30% of the time, the facial technology should work well enough…" See: https://data.aclum.org/public-records/plymouth-police-department-face-surveillance-emails/.

[3] Vikram Dodd, "UK police use of facial recognition technology a failure, says report," May 14, 2018, the Guardian. https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure.

Despite these well-known problems, face surveillance is completely unregulated in Massachusetts. The legislation before you is a critical intervention to protect basic civil rights—and Massachusetts voters know it. Over nine in ten Massachusetts voters oppose unregulated government use of the technology, and nearly eight in ten Massachusetts voters support the moratorium legislation before you. It's time to press pause now, before it's too late.

Face surveillance technology makes mistakes and, absent oversight, can upend an innocent person's life

Colorado financial analyst Steve Talley was permanently physically injured, and lost his house, his children, and his career after the police falsely accused him of bank robbery on the basis of a faulty face recognition search. Homeless, unemployed, and suffering from permanent injury due to his violent arrest, Talley later told a reporter unregulated face recognition technology in the hands of law enforcement ruined his life. "Take an individual who has a normal life and now it's destroyed," he said. "All because they relied upon facial recognition so much. Maybe someday it will be extremely accurate but at this point in time, it needs more oversight."[4]

Brown University student Amara K. Majeed woke up in the days following the Easter terrorist attack in her native Sri Lanka to dozens of messages and missed calls from people back home, warning her that the government had identified her as one of the terrorists. Her face was all over the news, they said. The *Boston Globe* reported that the error was the result of a face recognition software mistake, which was ultimately acknowledged by the police.[5] But it was too late; the damage to her reputation had been done, and she and her family received death threats.

As these two examples show, face surveillance technology is most dangerous when governments use it without clear guidelines, rules, and regulations in place. Yet this is precisely how government agencies in Massachusetts are operating. There is not a single statute on the books to set out rules of the road for the responsible use of this untested technology, or to prevent misuse, abuse, or dragnet surveillance.

Face surveillance is not ready for primetime. It poses particularly serious threats of misclassification to women, people of color, trans people, and children.

Racial and gender bias runs rampant in artificial intelligence systems

Studies have shown that face surveillance systems sold by even the most prominent technology companies can misclassify darker-skinned women up to 35 percent of the time.[6]

[4] Allee Manning, "A False Facial Recognition Match Cost This Man Everything," May 1, 2017, Vocativ. https://www.vocativ.com/418052/false-facial-recognition-cost-denver-steve-talley-everything/index.html.

[5] Jeremy Fox, "Brown University student mistakenly identified as Sri Lanka bombing suspect," April 28, 2019, Boston Globe. https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[6] Joy Buolamwini, "Gender Shades," MIT Center for Civic Media. https://www.media.mit.edu/projects/gender-shades/overview/.

Automatic gender recognition, a subfield of face surveillance technology, regularly misgenders transgender and gender-nonconforming people.[7]

Similarly, algorithms that claim to be able to identify how someone is feeling, based on their facial expressions, are complete bunk. One study used so-called "affect recognition" software to analyze images of NBA players' official portraits, and found it was more likely to classify Black players as angry and contemptuous.[8] Recent research from leading scholar Dr. Lisa Barrett at Northeastern University has shown that it is simply not possible to discern how someone is feeling based on how their face looks.[9] Nonetheless, without regulations, it's only a matter of time before companies try to sell this kind of snake-oil technology to police to use in interrogations, on our streets, and even in our schools.

Absent regulations, governments worldwide are adopting face surveillance systems even when they know about these bias problems. Just this month, the British government was exposed and pilloried for implementing a facial recognition algorithm as part of its passport examination system, even though officials knew the system made more mistakes on dark-skinned people.[10]

Face surveillance systems do not work well on children, but some police are using them to monitor youth

Face surveillance technology is not meant for children, so it makes more mistakes when scanning young people's faces. Research that tested five "top performing commercial-off-the-shelf" face recognition systems shows that these systems "perform poorer on children than on adults."[11] These systems are modeled on and optimized for use on adult faces; their use on children is particularly dangerous because as children grow, their faces change shape.

Nonetheless, public reporting has exposed police using face surveillance technology to investigate children as young as 11 years-old. According to the *New York Times*, "The New York Police Department has been loading thousands of arrest photos of children and teenagers into a facial recognition database despite evidence the technology has a higher risk of false matches in younger faces."[12]

These are precisely the kinds of abuses that can take place absent any meaningful external oversight or accountability.

Studies report astonishingly high error-rates in real-time tracking systems using artificial intelligence

Face surveillance technology works best when using front-facing, clear, high-resolution, high-light images. Even under those conditions it can fail, as discussed above. But when governments use face

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

[8] Lauren Rhue, "Emotion-reading tech fails the racial bias test," January 3, 2019, the Conversation. https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

[9] Lisa Feldman Barrett, et al. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements." *Psychological Science in the Public Interest*, vol. 20, no. 1, July 2019, pp. 1–68, doi: 10.1177/1529100619832930.

[10] "Passport facial recognition checks fail to work with dark skin," October 9, 2019, the BBC. https://www.bbc.com/news/technology-49993647.

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

[12] Joseph Goldstein and Ali Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database," August 1, 2019, New York Times. https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

surveillance technologies to try to identify or track people "in the wild," the results can be shockingly bad.

Right here in Massachusetts, for example, the CEO of Suspect Technologies was trying to sell face surveillance software to the Plymouth Police Department when he wrote that his product might properly identify people from surveillance camera videos only 30 percent of the time. That was an estimate. But when governments have actually studied the use of similar technologies in public space, the results have been even worse. In 2017, police in London used face surveillance technology to try to identify people on a hot-list at a carnival. The system wrongfully identified people 98 percent of the time.[13] Police in Wales reported similarly bad outcomes: 91 percent failure.[14] "On 31 occasions police followed up the system saying it had spotted people of concern," the Guardian reports of the test, "only to find they had in fact stopped innocent people and the identifications were false."[15]

Face surveillance technology poses an unprecedented threat to our most fundamental rights

Leading scholars have called for a total ban on government use of face surveillance technology, arguing that it is "the perfect tool for oppression."[16] The Chinese government is showing us what that looks like, and it should terrify every freedom-loving person.

According to reports, the Chinese government is using its network of surveillance cameras integrated with facial recognition technology to keep tabs on millions of Uighurs in Xinjiang. "The facial recognition technology," the *New York Times* reports, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. The practice makes China a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism."[17]

China's use of the technology enables its government to track how many people of certain ethnic backgrounds are in a location at once, to track individual people's movements and activities—including their religious worship—and even to flag that someone entered their house from the rear, instead of the front door.

Closer to home, the Detroit Police Department has been using face surveillance on its networked surveillance camera system for two years. The system was established in secret, without public debate, legislative authorization, or regulations to protect civil rights and liberties.[18]

[13] Vikram Dodd, "UK police use of facial recognition technology a failure, says report," May 14, 2018, the Guardian. https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure.
[14] Ibid.
[15] Ibid.
[16] Woodrow Hartzog and Evan Selinger, "Facial Recognition is the Perfect Tool for Oppression," August 2, 2018, Medium. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[17] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," April 14, 2019, New York Times.
[18] Clare Garvey and Laura Moy, "America Under Watch," Georgetown University, 2019. https://www.americaunderwatch.com/

Face surveillance could easily be applied to thousands of networked cameras in the metro Boston area—without any regulatory framework in place

Unfortunately, we are just a software update away from creating a similar digital dragnet right here in eastern Massachusetts, where a regional surveillance camera network already links hundreds of cameras throughout Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop. As of 2017, there were nearly 900 cameras in this regional network, and at least 1,125 people could access videos and control cameras in it.[19] The MBTA, for its part, has over 5,000 cameras in its system.[20]

For the past few years, the Metro Boston regional camera network has been supercharged with video analytics technology manufactured by a company called BriefCam. This technology allows law enforcement to apply machine learning technology to rapidly analyze large quantities of video surveillance data, in real time and retroactively. Currently, the Boston area camera network uses a version of BriefCam's software that tracks the movements of people, cars, bicycles, and other objects, enabling government agencies to automatically identify, for example, red cars traveling down a certain roadway on a certain day, or a woman riding a bicycle in a particular area.[21] But the most recent version of BriefCam's technology (version 5.3) uses facial recognition technology, creating the potential for the same kind of pervasive biometric monitoring that currently takes place in China. The city's current contract with BriefCam, which provides the government with software version 4.3, ends in May 2020.[22]

Technology moves much faster than the law. Absent a statewide moratorium on government use of face surveillance technologies, all officials in Boston would have to do to create a digital dragnet akin to China's is pay for a software upgrade.

It nearly happened in Plymouth: a case study

Emails obtained by the ACLU show technology companies are putting significant pressure on local governments to implement this China-style surveillance right here at home, including to track people in public space by their age, gender, and ethnicity.

Suspect Technologies, a Cambridge-based start-up, communicated with the police chief in Plymouth, Massachusetts for approximately two years, developing a plan to use face surveillance technology on publicly owned surveillance cameras across the municipality, the emails show. Among the most disturbing aspects of the plan were:

- The intention to upload a list of every person wanted by the Plymouth police to a Suspect Technologies database. Suspect's face surveillance algorithm would then constantly scan the

[19] Document obtained by ACLU via public records request. See: http://data.aclum.org/wp-content/uploads/2019/10/CIMS-Customer-Use-of-Video.pdf.
[20] Michael Jonas, "Big Brother is watching," Winter 2015, Commonwealth Magazine. https://commonwealthmagazine.org/criminal-justice/big-brother-is-watching/
[21] BriefCam website, "How it Works." https://www.briefcam.com/technology/how-it-works/.
[22] City of Boston contract with BriefCam, obtained via ACLU public records request. http://data.aclum.org/wp-content/uploads/2019/10/Contracts-and-Certificates.pdf.

faces of each person passing by a camera in the town and notify law enforcement immediately when one of those "wanted" people walked past a camera;
- An admission by the CEO that his technology may work only 30 percent of the time;
- An admission by the CEO that the failure rates may result in as many as one "false positive" hit per day (which could lead to wrongful arrest or even result in serious injury or death);
- The contemplated use of the face surveillance system in public schools; and
- A lack of planning to address privacy, civil rights, civil liberties, or even basic transparency regarding the implementation of the face surveillance system.

In the emails, the CEO of this company even suggested using his technology to track people by their ethnicity.[23]

This plan was developed in secret, with no regulations in place to protect privacy, and completely unbeknownst to the residents of Plymouth. The emails show that profit-motivated corporations will work overtime to push their technologies on public officials who are ill-equipped to judge the merits of experimental software.

When the ACLU alerted journalists to the existence of the plan, the Plymouth police backed off and said they wouldn't go forward with implementing this system. The people of Plymouth can therefore be confident they won't be tracked as they go about their daily lives, for the time being at least.

But the ACLU cannot act as a regulator in this space, filing records requests with the hundreds of police departments across the state to ensure schemes like this one don't materialize in secret. And we cannot expect our state and local officials to be artificial intelligence experts, able to judge the claims companies make about how their technologies work. The information asymmetry between self-interested technology companies and our public servants puts us all at risk of grave civil rights and civil liberties harms. In the absence of a statewide moratorium, we can't be sure that similar plans aren't in the works in other municipalities right now, behind closed doors.

Face surveillance technology is entirely unregulated, yet has been in use in Massachusetts since 2006

There is not a single statute or regulation on the books in Massachusetts, or at the federal level, imposing guardrails on how government agencies can use these potentially biased, inaccurate, and dangerous technologies.[24]

The lack of regulation leaves Massachusetts residents vulnerable to a host of abuses and misuses of the technology. Absent regulation, government agencies and technology companies are left to decide, in secret, which systems to deploy where and how, who can access the systems for what purposes, and what information about the use of these technologies ought to be disclosed to lawmakers, members of the public, criminal defendants, and the courts.

[23] Joseph Cox, "'They would go absolutely nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work with Cops," May 6, 2019, Vice. https://www.vice.com/en_us/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies.

[24] Indeed, this October California passed the nation's first law that prohibits the use of face surveillance technology in any context, placing a moratorium on police use of face recognition on body cameras. See Bryan Anderson, "New law bans California cops from using facial recognition tech on body cameras," October 8, 2019, Sacramento Bee. https://www.sacbee.com/news/politics-government/capitol-alert/article235940507.html.

Thankfully, to our knowledge, the kind of pervasive public monitoring in place in Detroit and China is not yet taking place in Massachusetts. But through public records requests the ACLU learned that the Registry of Motor Vehicles has been using millions of drivers' license photographs as a perpetual line-up for law enforcement searches for at least thirteen years, absent legislative authorization or any meaningful checks and balances. In addition, the State Police is also allowing state, local, and federal law enforcement to use a database of four million mugshots for similar searches. Despite this, there is no indication that criminal defendants or courts have been given the opportunity to contest these searches—because they have been kept secret.

The RMV's perpetual lineup—where everyone is a suspect

The RMV first obtained a facial recognition system with the help of a federal grant in 2006, and has since spent millions of dollars updating the technology. Initially, the RMV obtained the software to perform fraud checks, to ensure people were not able to apply for a second driver's license under an alias. But almost immediately after they got the software, the RMV sent a memo to law enforcement, offering to perform searches against the database to help police identify unknown persons in images.[25]

Due to the complete absence of regulation controlling these technologies, there are no civil rights or privacy protections in place to ensure the public's trust is not abused. The RMV drivers' license database and State Police mugshot systems, for example, can be searched by law enforcement without any prerequisites. There is no requirement to show probable cause or even reasonable suspicion of criminal activity.

For the RMV system, all a law enforcement officer at the federal, state, or local level must do is send a simple email to the RMV facial recognition unit requesting that an image be scanned against the driver's license database to look for a match. An exhaustive ACLU review of materials obtained via a public records lawsuit suggests RMV officials have never—*not once*—declined a police request to perform one of these facial recognition searches.

Hand-written logs obtained by the ACLU show the RMV has executed hundreds of searches per year on behalf of agencies including Immigration Customs Enforcement, the State Department, and the New York Police Department, as well as state and local agencies across Massachusetts. The search logs and the emails indicate that abuse and misuse may have already taken place. For instance, some of the logs merely list a first name, "Karen," where a law enforcement official's name and department should be written. Meanwhile, emails between police officers suggest the Massachusetts State Police may be using the technology to perform surveillance of First Amendment protected events like political demonstrations.[26]

The RMV, while it maintains a paper log, has never once performed an audit of how agencies have used the facial recognition system, meaning the agency has no idea whether the system has been

[25] Massachusetts Department of Transportation memorandum to law enforcement, October 31, 2006, obtained via public records request. See page 14: https://data.aclum.org/wp-content/uploads/2018/06/DOT-facial-recognition-response.pdf.

[26] State Police emails obtained via ACLU public records request, dated June 2019. http://data.aclum.org/wp-content/uploads/2019/10/large-scale-public-events.pdf. In a June 10, 2019 email, an employee of the State Police emails two other State Police officials, informing them that the facial recognition system at the RMV would be down for maintenance. "The RMV would like to confirm that there are no large scale events, etc. that will require the use of the Facial Rec software during this time frame," the official wrote. In response, a State Police official writes, "I am not aware of any large events that day."

misused or abused for personal or political reasons. We therefore also do not know whether these searches have disproportionately been performed against people of color. The State Police, for its part, confirmed to the ACLU in writing that it does not even know who has searched its facial recognition system, or how many times or for what reasons, because its system does not allow for the logging of these searches. Moreover, the State Police's use of a mugshot database for facial recognition searches raises serious racial justice concerns, because Black and Latinx people are disproportionately policed and arrested, including for low-level offenses like driving with a suspended license and drug possession.

Evidence suggests rampant due process violations are occurring right now

Despite the hundreds of police searches of the RMV's face database per year, conversations with public defenders in Massachusetts suggest criminal defendants are not given an opportunity to contest or benefit from the searches in the vast majority of cases. Without mandatory disclosure requirements, law enforcement appears to be shielding information about face surveillance searches from the courts. This practice threatens defendants' core due process rights and the integrity of our court system. Criminal defendants must be able to interrogate a digital witness against them.

If police investigate and then ultimately charge people with crimes due to facial recognition identifications, defendants must be able to access key details about those searches. For example, defendants must have access to:

- information about the face surveillance algorithm used to perform the search (including, if available, the results of accuracy and bias tests);
- depositions of face surveillance technicians who perform the searches, to find out what investigatory steps were taken subsequent to the search;
- the full results of the search, including images of other people, if these were returned; and
- information about the technical "confidence level" at which the system identified the defendant, in addition to other information critical to mount a defense.

Face surveillance raises serious constitutional concerns, but we can't wait for the courts; the legislature must act

The use of face surveillance software, especially overlaid onto existing surveillance camera infrastructure, raises grave constitutional concerns. Dragnet identification of individuals while they are exercising rights protected by the First Amendment could chill freedom of expression, freedom of speech, and exercise of religion. The technology poses a fundamental threat to our basic Fourth Amendment privacy rights and right to be left alone. And its use without disclosure to defendants jeopardizes our Fourteenth Amendment due process right to a fair trial. Furthermore, government secrecy regarding the use of face surveillance denies courts the opportunity to rule on its constitutionality.

Law enforcement officials have argued that we have no privacy in public spaces, but the Supreme Court disagrees. In an historic ruling in *Carpenter v. U.S.*, Chief Justice John Roberts held that new technologies enabling retroactive and real-time mass surveillance fundamentally change the balance of power between the government and the people. In that case, the Court ruled that law enforcement officials must get a warrant to obtain historical cell site location data from phone companies.[27]

Eventually, courts may very well apply *Carpenter*'s reasoning to ubiquitous face tracking in public space. But that case was not decided until 2018, decades after Americans began to use cell phones. We cannot wait decades for the courts to rule on the constitutionality of face surveillance technology. We must press pause now, before dragnet surveillance systems are created in the shadows.

It is also critical that we distinguish face surveillance from even the most invasive tracking technologies that the courts have considered to date. Cell phone tracking is fundamentally different from face surveillance in at least two significant ways. First, if you want to go somewhere anonymously—a political demonstration, a clinic, a bar, or a motel—you do not have to bring your phone with you. You cannot leave your face at home.

Second, for a government official to access information from your phone, they must either have possession of the device itself or request access from a third-party service provider. In either case, they must obtain a warrant. But judicial authorization and oversight become substantially less effective tools to prevent misuse and abuse if a government agency acquires face surveillance technology and can use it in-house without going through any other gatekeeper. For this reason, legislative intervention is imperative—*before* government acquisition and use of the technology become more widespread.

Time to press pause

Thankfully, we still have time to prevent the worst harms in the Commonwealth—if we act now. We don't have to allow what happened to Steve Talley or Amara Majeed to happen to someone in our commonwealth. We don't have to accept that simply because technology enabling biometric mass tracking exists, our government will inevitably monitor our every public movement.

Instead of allowing government agencies to make up the rules as they go along—in secret, absent legislative authorization or public debate—or accepting that the technology will determine the boundaries of our rights, we must chart an intentional course forward, maintaining democratic control over our society and our lives.

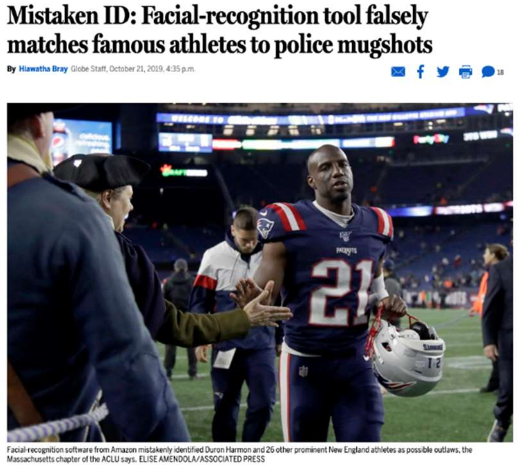
We cannot continue to put the technology cart before the policy horse. We must press pause on the use of this dangerous technology to give ourselves the time and space to make wise decisions and protect fundamental liberties.

We urge the committee to give a swift, favorable report to S.1385 and H.1538. Please don't hesitate to contact the ACLU for further information or clarification. We would welcome the opportunity to work with the committee to advance this critical legislation. Thank you.

[27] Case page for Carpenter v. United States, SCOTUSblog. https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/.

Appendix A

A Face Surveillance Case Study: Misidentifications of Famous Athletes



Mistaken ID: Facial-recognition tool falsely matches famous athletes to police mugshots

By Hiawatha Bray Globe Staff, October 21, 2019, 4:35 p.m.

Facial-recognition software from Amazon mistakenly identified Duron Harmon and 26 other prominent New England athletes as possible outlaws, the Massachusetts chapter of the ACLU says. ELISE AMENDOLA/ASSOCIATED PRESS

Boston's pro athletes are immediately recognizable to millions of sports fans across New England and the nation, but face surveillance technology confused them for people in a mugshot database.

From the *Boston Globe*, October 21, 2019:

"Duron Harmon of the New England Patriots: three-time Super Bowl champion, or candidate for a police lineup? How about Brad Marchand? Stanley Cup winner or a guy with an arrest record? And is that Chris Sale, World Series star, or somebody awaiting trial?

Apparently, Amazon can't tell the difference.

Among the Internet titan's many technology businesses is a leading facial-recognition software system called Rekognition, which Amazon has marketed to police agencies for use in their investigations. And according to the Massachusetts chapter of the American Civil Liberties Union, Rekognition mistakenly matched 27 well-known athletes from Boston sports teams to a database of mugshots of real people who had been arrested. Among the misidentified: Harmon, Marchand, and Sale.

…

"The ACLU test is similar to one it conducted last year, which found that Amazon software mistakenly matched 26 California state legislators to mugshots in a database of 25,000 photos of people who'd been arrested.

This time, the testers compared photos of 188 New England athletes from the Boston Bruins, Boston Celtics, Boston Red Sox, and New England Patriots with a database of 20,000 mugshots. The software delivered 27 false positives.

Two Boston Celtics made the list: Tacko Fall and Gordon Hayward. Rekognition also singled out six Red Sox, including Chris Sale and Hector Velazquez; five Bruins, including Sean Kuraly and Marchand; and 14 Patriots, including Stephen Gostkowski, James White, Phillip Dorsett, and Harmon.

In a statement provided by the ACLU, Harmon said: 'If it misidentified me, my teammates, and other professional athletes in an experiment, imagine the real-life impact of false matches. This technology should not be used by the government without protections.'"

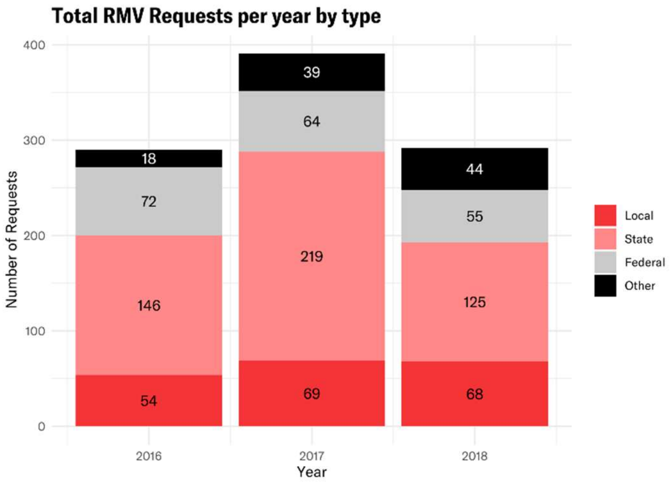
Appendix B

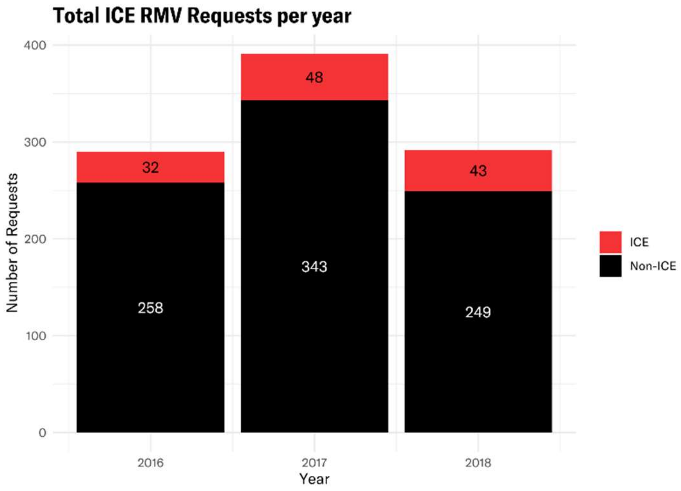
Face Surveillance in the Commonwealth: Unchecked, Unregulated, and Ripe for Abuse

Since October 2006, the Registry of Motor Vehicles has allowed law enforcement across the country to access the state's driver's license database for face recognition searches. That means every person with a state ID has been in a perpetual line-up for police searches for over a decade, absent any judicial oversight, legislative authorization, or independent oversight.

In documents obtained by the ACLU, the RMV confirms it has never once performed an audit of its face surveillance system, meaning the agency does not know if it has been misused or abused for personal or political reasons. The documents reviewed by the ACLU indicate the RMV has never once declined to perform a search on behalf of a police entity.

These charts show how often federal, state, and local law enforcement agencies have searched the RMV's face recognition system, looking to identify persons in images.


Total RMV Requests per year by type
Number of Requests
Year
Local
State
Federal
Other


Total ICE RMV Requests per year
Number of Requests
Year
ICE
Non-ICE