AMERICAN CIVIL LIBERTIES UNION FOUNDATION
Massachusetts

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
Maine

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

Michael Kebede
Policy Counsel
ACLU of Maine
(207) 774-5444 ext. 307

TESTIMONY OF MICHAEL KEBEDE, Esq.

LD 1585 – Ought To Pass

An Act To Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials

JOINT STANDING COMMITTEE ON
CRIMINAL JUSTICE AND PUBLIC SAFETY

May 12, 2021

Senator Deschambault, Representative Warren, and members of the Joint Standing Committee on Criminal Justice and Public Safety, good afternoon. My name is Michael Kebede, and I am policy counsel for the American Civil Liberties Union of Maine, a statewide organization committed to advancing and preserving civil liberties guaranteed by the Maine and U.S. Constitutions through advocacy, education, and litigation. On behalf of our members, we urge you to vote *ought to pass.*

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. Instead of accepting that the technology will determine the boundaries of our rights, we must chart an intentional course into the 21st century, maintaining democratic control over our society and our lives. To protect residents now and into the future, the State of Maine should join our state's largest city, and cities from California to Massachusetts, in prohibiting the use of face surveillance technology by government officials.

For too long, we have accepted that new technologies will determine the boundaries of our 21st century rights. But face surveillance is too dangerous to allow that trend to continue. Imagine if you were required to tattoo a barcode to your face, which could only be read by the government—enabling officials to secretly track your every movement, habit, and association. That is the functional equivalent of this technology. Face surveillance is the final frontier of government tracking, enabling officials to track you not through a cell phone (which you can leave at home), but through your face—an immutable, physical characteristic you carry with you everywhere, and cannot easily hide. To maintain democratic control over the future of civic life in Maine, and to protect the rights of the most marginalized and oppressed, we urge you to support this crucial measure.

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, without their knowledge or consent. 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 can use these faceprints, in combination with databases like the driver's license system at the Bureau of Motor Vehicles and surveillance camera networks, to identify and track people en masse.

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. Independent research concludes it is not possible to discern how someone is feeling by judging the physical characteristics of their face.[1] 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 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.[2]

(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 user that a person is agitated, anxious, or angry. (Again, research indicates this is not a scientifically sound project.[3])

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; (ii) specific harms to communities of color, youth, transgender people, and immigrants; and (iii) civil rights, civil liberties, and other core constitutional concerns.

<u>(i) Unregulated Use of the Technology</u>

[1] 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.
[2] Clare Garvey and Laura Moy, "America Under Watch," Georgetown University, 2019. https://www.americaunderwatch.com/
[3] Ibid.

Face surveillance is currently unregulated in Maine. 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 local governments across the nation, trying to use our families and communities as guinea pigs for their private financial gain. In Plymouth, Massachusetts, for example, emails obtained[4] by the ACLU show the police chief was in talks with Suspect Technologies, a face surveillance manufacturer, for two years—entirely in secret. 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 CEO acknowledged his product might only work about 30 percent of the time. The plans were scrapped once they became public.[5]

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

Facial recognition technology is not always accurate. And these inaccuracies are more likely to unfairly harm people of color, youth, and transgender people.

First, the use of facial surveillance technologies undermines Maine's commitment to racial justice. Face surveillance in the hands of government exacerbates the disproportionate harm these communities suffer from over-policing 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.[6] Most recently, in December 2019, a federal government study by the non-partisan National Institute for Standards and Technology found that face surveillance algorithms are more likely to have trouble accurately identifying people with darker skin, women, children, and the elderly.[7]
(2) Renowned psychologists have found that attempting to determine a person's emotional state from their facial expressions alone is a "futile exercise."[8] Moreover, a study found that so-called "emotion detection" software inaccurately

[4] See Plymouth Police Department Face Surveillance Emails, ACLU of Massachusetts, available at https://data.aclum.org/public-records/plymouth-police-department-face-surveillance-emails/
[5] Joseph Cox, 'They Would Go Absolutely Nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work With Cops, VICE, May 2019, available at https://www.vice.com/en_us/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies
[6] Joy Buolamwini et al, "Gender Shades," MIT Media Lab, available at https://www.media.mit.edu/projects/gender-shades/overview/
[7] Jon Porter, "Federal study of top facial recognition algorithms finds 'empirical evidence' of bias," the Verge, December 20, 2019. https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon.
[8] 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/

classified Black men's faces as angrier and more contemptuous than white faces, even in pictures where the men are smiling.[9]

(3) Face surveillance systems in use by law enforcement frequently compare images against mugshot databases. Numerous studies, including those examining trends in Maine, have shown that Black and Latinx 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.[10] 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.

(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 communities of color, and against immigrants. 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.

Second, face surveillance is especially dangerous when it is used on children. Research[11] that tested five "top performing commercial-off-the shelf" face recognition systems shows these systems "perform poorer on children than on adults." 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.[12] 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. The use of this monitoring technology in public schools negatively impacts students' ability to explore new ideas, express their creativity, and engage in student dissent.

---

[9] Lauren Rhue, "Emotion-reading tech fails the racial bias test," Phys.org, available at https://phys.org/news/2019-01-emotion-reading-tech-racial-bias.html.

[10] See Shira Schoenberg, Study tracks racial disparities in Massachusetts marijuana arrests, MassLive, available at 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, available at 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, available at https://www.aclum.org/en/ending-racist-stop-and-frisk.

[11] Nisha Srinivas, Karl Ricanek, 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, available at 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] Tristan Greene, Why US public schools' creepy use of surveillance AI should frighten you, The Next Web, July 2019, available at https://thenextweb.com/artificial-intelligence/2019/07/23/why-us-public-schools-creepy-use-of-surveillance-ai-should-frighten-you/. See also Thomas J. Prohaska, Education Department bars Lockport schools from testing facial recognition, The Buffalo News, June 2019, available at https://buffalonews.com/2019/06/28/education-department-bars-lockport-schools-from-testing-facial-recognition/

Third, face surveillance technology is prone to misgendering transgender people.[13] 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."[14] At a time when transgender rights are under attack nationwide,[15] Maine must do everything in its power to protect this marginalized group.

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. Banning face surveillance would help ensure that Maine is a welcoming and safe place for all.

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

Face surveillance poses a threat to the civil rights and civil liberties of people who live in and visit Maine. Especially concerning is how this technology affects our privacy interests, and our rights to freedom of expression and association.

As artificial intelligence, big data, and automation continue to change every area of our lives, the pull of so-called "smart city" devices that bring more tracking and surveillance of residents will become stronger. Face surveillance technology connected to public surveillance camera feeds in Maine would facilitate government monitoring of every person's public movements, associations, and habits—not just on one day, but on all days—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 reproductive or substance use medical attention, we lose our freedom to speak our minds, freely criticize the government, pray to the god we want, and access healthcare in private. People who live in and visit Maine should feel free to visit the liquor store or the health clinic without fear that their attendance is secretly being tracked 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. Closer to home, the Detroit Police Department has been using face surveillance on its networked public 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.[16]

---

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

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

[15] 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

[16] Clare Garvey and Laura Moy, "America Under Watch," Georgetown University, 2019. https://www.americaunderwatch.com/

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**. 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 identification and tracking can have a chilling effect, as people will be less likely to exercise their rights if they know the government is tracking and identifying them everywhere they go.
(2) **Face surveillance threatens our Fourth Amendment right to be left alone**. The highest court in the United States has held that the government cannot use technological advancements to track our public movements via our cellphones without judicial intervention. The government's use of face surveillance raises the same 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.
(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 their 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. We know these technologies are in use in other states, including Massachusetts, but it is our understanding that in the vast majority of cases criminal defendants have not been given the opportunity to review or challenge information derived from face recognition searches.

As scholar Woodrow Hartzog has observed, face surveillance is a perfect tool for social control.[17] People in Maine must be able to visit substance use clinics, churches and synagogues, friends and family, political protests, and doctors' offices without fear that a government agent is secretly keeping tabs on their every movement.

Maine must chart a different course

Ultimately, faced with the question of whether Maine should prohibit the use of face surveillance by government actors, members of this committee ought to consider what kind of state 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.[18] Privacy advocates have long warned about the psychological consequences of being watched and observed by

[17] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," NYT. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[18] Kaleigh Rogers, What Constant Surveillance Does To Your Brain, Vice, Nov. 2018, available at https://www.vice.com/en_us/article/pa5d9g/what-constant-surveillance-does-to-your-brain

unaccountable, faceless entities.[19] 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 15 communities across the country—including 7 Massachusetts communities—and a ban on police use of facial recognition in the state of Virginia, Maine has the chance to lead the nation and the world by becoming the first state to ban government officials from schools to parks departments to policing entities from using face surveillance technology.

As written, this bill protects people from government use of a dangerous, racially-biased technology. If enacted, this bill will advance racial, economic, and immigration justice, and protecting democracy, open society, and liberty. Fundamentally, this proposal would enable Maine to maintain democratic control over a technology that, unattended, threatens democracy itself. We therefore respectfully ask that you support this crucial measure.

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

[19] John Borland, Maybe Surveillance Is Bad, After All, August 2007, available at https://www.wired.com/2007/08/maybe-surveilla/