



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

TESTIMONY OF KADE CROCKFORD

LD 1585 – Ought To Pass Amended

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 Kade Crockford, and I am Director of the Technology for Liberty Program at the ACLU of Massachusetts, where I work to protect and expand core First and Fourth Amendment rights and civil liberties in the digital 21st century, focusing on how systems of surveillance and control impact not just the society in general but their primary targets—people of color, Muslims, immigrants, and dissidents. I urge you to vote *ought to pass*.

In June 2020, the Boston City Council unanimously voted to ban the possession and use of face recognition technology in all areas of municipal government. The unanimous vote came after dozens of community members and organizations voiced support for the measure, and after then Boston Police Commissioner William Gross testified that his department does not use facial recognition, in part due to racial bias problems with the technology. Not a single person testified against the proposed ban. Less than a week after the council's unanimous vote, then Mayor Martin Walsh—who currently serves the Biden administration as Labor Secretary—signed the measure into law.

Boston is a safer and freer community due to this historic law reform. Today, Black and brown people, immigrants, religious minorities, dissidents, students, and poor people do not have to worry that they will be wrongly accused of a serious crime, or secretly tracked by the government as they go about their business in their neighborhoods across the city, because of

facial recognition. People seeking substance use treatment or other sensitive health care services do not need to worry that their identity will be catalogued by the government, merely because they entered a facility in view of a surveillance camera. Thanks to the ban, the Boston Public Schools did not join many other school districts in using remote proctoring software that has been the subject of litigation,¹ student frustration,² and community outrage³ across the nation. Just like face recognition technology in use by policing entities, the technology built in to remote proctoring systems can fail when examining the faces of darker skinned people, leading to complaints⁴ from students of color that they have had to shine bright lights on their faces while taking remote exams, in order to be “seen” by the technology.

Boston’s face surveillance ban has likewise protected the city from litigation that can arise after police rely on faulty face recognition data to make arrests. Over the past year, the public has learned about three wrongful arrests stemming from police use of facial recognition technology—all of them Black men. One of those men, Robert Williams of Michigan, is currently suing the Detroit Police Department over his wrongful arrest.

Boston likewise doesn’t have to worry that a surveillance contractor working for any city department will be hacked, enabling untold numbers of non-official persons to tap into the city’s surveillance network and use facial recognition to track or identify ordinary people. Any sensitive data system is an attractive target for hackers. In March, reporters disclosed that a private surveillance firm called Verkada was hacked, exposing surveillance feeds from 150,000 cameras across the country to untold numbers of unidentified persons.⁵ This company offered

¹ Ella Lee, *DePaul sued over facial recognition tech used for online test proctoring*, The DePaulia (Mar. 8, 2021), available at <https://depauliaonline.com/52893/news/depaul-sued-over-facial-recognition-tech-used-for-online-test-proctoring/>.

² Meg Foulkes, *Exams that use facial recognition may be 'fair' – but they're also intrusive*, The Guardian (Jul. 22, 2020), available at <https://www.theguardian.com/law/2020/jul/22/exams-that-use-facial-recognition-are-fair-but-theyre-also-intrusive-and-biased>.

³ Shea Swauger, *Remote testing monitored by AI is failing the students forced to undergo it*, NBC News (Nov. 7, 2020), available at <https://www.nbcnews.com/think/opinion/remotetesting-monitored-ai-failing-students-forced-undergo-it-ncna1246769>.

⁴ Avi Asher-Schapiro, *Online exams raise concerns of racial bias in facial recognition*, Christian Science Monitor (Nov. 17, 2020), available at <https://www.csmonitor.com/Technology/2020/1117/Online-exams-raise-concerns-of-racial-bias-in-facial-recognition>.

⁵ Chaim Gartenberg, *Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more*, The Verge (Mar. 9, 2021), available at <https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals>.

facial recognition as a service, meaning hackers may have been able to use their unauthorized access to these systems to track and identify people—including in at least one government-run jail facility.

Boston is a safer and freer community because of our ban on facial recognition. Our communities are freer to exercise their core rights, including their First Amendment rights to worship their religion and criticize the government without interference. Surveillance isn't safety, particularly when the surveillance technology at issue exhibits racial and gender bias. I encourage the Committee to vote *ought to pass*; this bill would keep Mainers safe from using unreliable, dangerous technology.

Thank you for your time and attention. I would be happy to answer any questions.