Senate Finance Committee

SUPPORT SB857

Testimony of Benjamin Orlebeke, CASA
March 11, 2020

The Georgetown Law Federal Legislation Clinic is submitting this testimony in support of SB857 on behalf of CASA. CASA is the largest membership-based immigrant rights organization in the mid-Atlantic region. Our Clinic has worked extensively with CASA to research how Maryland resident data could be shared with Immigration and Customs Enforcement ("ICE"). CASA's members are particularly vulnerable to surveillance abuses by law enforcement, which are exacerbated by unrestricted use of face recognition technology. This is a real threat: the *Washington Post* revealed last month that ICE has in fact repeatedly scanned the faces of all Maryland drivers, necessarily including thousands of CASA members.[1] By hitting "pause" on use of this technology, SB857 offers an important first step in protecting the privacy of Maryland residents.

Face recognition technology is an unprecedented, dangerous mode of surveillance.

Face recognition technology identifies faces by comparing an individual's facial features to those in a reference database.[2] Face recognition technology compares each face it receives with a database of faces, which may include driver's license records, government identification records, mugshots, or social media accounts. A face recognition system, or a human relying on the system's comparisons, determines whether the original face matches a face from that database.

Face recognition technology can reveal "who is where, doing what, at any point in time."[3] In practice, this means that the government could learn very personal data without much investigation—where an individual goes to church or synagogue, whether they visit a women's health center, or if they attend a gun show. For immigrants, those effects are even more serious. To avoid being swept up in surveillance, immigrants and people with close relationships to someone vulnerable to deportation may avoid going to a doctor, taking their child to school, or

[1] Drew Harwell & Erin Cox, *ICE has run facial-recognition searches on millions of Maryland drivers*, The Washington Post (February 26, 2020).
[2] Dr. Charles H. Romine, Director Information Technology Laboratory, National Institute of Standards and Technology, Testimony before the U.S. House Committee on Oversight and Government Reform, March 22, 2017, https://www.nist.gov/speech-testimony/facial-recognition-technology-frt.
[3] Clare Garvie & Laura Moy, *America Under Watch*, The Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.americaunderwatch.com.

reporting domestic violence to law enforcement for fear of being identified and exposed or exposing loved ones to ICE.

Face recognition technology can have a chilling effect on free expression

Given this unprecedented surveillance power, face recognition technology implicates unique First Amendment concerns. The right to free speech and peaceful assembly are inherent American values. Particularly where the technology is used on public gatherings, individuals might be afraid to exercise their constitutional rights to speak, assemble, and express themselves. In other words, face recognition technology could chill First Amendment activity. The Nlets Facial Recognition Workgroup, which is made up of law enforcement practitioners from all over the nation, has recognized this possibility as well, warning: "The public could consider the use of facial recognition in the field as a form of surveillance …. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."[4]

This is of particular concern to CASA's members, many of whom are undocumented and known for their political organizing. In 2018, for example, CASA members advocated for 20 pro-immigrant policies at the state and local level, of which 14 passed including several local TRUST Acts.[5] CASA's 2020 organizing campaigns are aimed at achieving comprehensive immigration reform, protecting local families by challenging unjust immigration enforcement policies, preserving low-income housing and improving job opportunities related to the construction of a new metro line, and tenants' rights and workers' rights.[6] Unfettered use of face recognition technology acts as a barrier to these goals, as CASA members may be less likely to join demonstrations or other peaceful First Amendment-protected activities if they know that their faces may be scanned and identified.

Face recognition technology is least accurate on populations that need the most protection.

The technology underperforms on women and people of color,[7] and its inaccuracies compound at the intersection of these characteristics.[8] A study of face analysis software (a branch of face

[4] The International Justice and Public Safety Network, *Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (June 30, 2011), Document p. 016632.

[5] 2018 Annual Report, CASA (2019), https://wearecasa.org/wp-content/uploads/2019/08/2018-CASA-Annual-Report.pdf.

[6] CASA, *Community Organizing,* We Are Casa, https://wearecasa.org/programs/community-organizing/.

[7] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[8] Clare Garvie, Alvaro Bedoya, and Johnathan Frankle, *The Perpetual Line-Up*, The Center on Privacy & Technology at Georgetown Law (October 18, 2019), https://www.perpetuallineup.org; Clare Garvie, *Garbage In, Garbage Out*, The Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.flawedfacedata.com; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1-15 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

recognition that doesn't involve identification) found that when race and gender are combined, the results are even worse. In a study of three different algorithms, face recognition technology failed between 20% and 35% of the time on African-American women.[9] For context, the same study found that the comparable maximum error rate for lighter skinned men was 0.8%.[10] Error-prone face recognition technology is thus uniquely dangerous for communities of color, who are already over-policed and over-surveilled. For CASA's members the stakes are even higher as misidentification could mean they or a loved one could be deported.

Maryland residents have already suffered because of the technology's inaccuracies. Amara Majeed, a Maryland resident and student at Brown University, was misidentified by the Sri Lankan government using face recognition technology as a suspect in the April 2019 Easter Day bombings.[11] A photo of Majeed was used incorrectly to identify the suspect, Abdul Cader Fathima Qadiya.[12] Majeed was bombarded with vitriol and death threats online from people who believed she had committed the crime.[13] The police confirmed their release of the picture was a mistake and said they "regret any inconvenience caused by sharing."[14]

ICE is using face recognition technology to target Maryland residents

The Department of Public Safety and Correctional Services' Dashboard ("Dashboard") is the main conduit through which ICE accesses Maryland's data. Dashboard currently receives 60,000 – 80,000 queries per day from various federal and cross-border agencies.[15] Dashboard has mapping, graphing, and face recognition capabilities. Over 2 million photos have been uploaded into the Dashboard from the Maryland Image Repository System ("MIRS").[16] MIRS is a database that includes MVA photos, inmate case records, and mugshots.[17] Law enforcement

[9] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1-15 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[10] *Id.*

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

[12] *Id.*

[13] Sameer Rao, *Maryland woman says she received death threats after Sri Lanka misidentified photo of her as a bombing suspect*, Baltimore Sun (Apr. 26, 2019), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-amara-majeed-cair-20190426-story.html.

[14] Lillian Reed, *Sri Lankan government misidentifies Towson woman's photo as depicting terrorism suspect*, Baltimore Sun (Apr. 25, 2019), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-sri-lanka-amara-majeed-20190425-story.html.

[15] *The Criminal Justice Dashboard (The Dashboard)*, State of Maryland (June 1, 2011), https://drive.google.com/open?id=1D8AlJO6q-pMptFSycG6khuZA3eqtRr3o

[16] *Id.*

[17] Department of Public Safety and Correctional Services, https://drive.google.com/file/d/1tus_FlmAevIytlja0SIU53qNpPVn3qc6/view?usp=sharing.

agencies can use face recognition technology on the images within this database to identify individuals.[18]

Through Dashboard, MIRS is accessible to agencies outside of Maryland, and ICE is in fact using MIRS to conduct face recognition searches of MVA photos.[19] In a November 21, 2019, letter to Maryland legislators, the Department of Public Safety and Correctional Services indicated that ICE users saved 56 sessions in the MIRS system in 2018 and 2019.[20] The *Post* explained that each saved session could have included multiple face recognition search queries.

Not only does this violate the trust of immigrant communities who rely on driver privilege cards, but it allows ICE to use a law enforcement tool for civil immigraton enforcement. Additionally, these searches implicate not just immigrants but any Maryland resident who has a driver's license. The nature of face recognition technology requires that law enforcement compares a face against every face in the dataset. By allowing anyone to use face recognition technology on MVA photos, *every* Marylander with a driver's license becomes part of a perpetual line-up.

SB857 is a good start, but it's not enough to protect Maryland residents.

A "pause" on face recognition technology use in Maryland is desperately needed. A moratorium of any kind is powerful in its simplicity. Law enforcement will not have to guess when they can use the technology, and Maryland residents will not have to wonder when their face will be used against them.

However, the bill as written is only a first step in protecting Maryland residents from this dangerous surveillance. During this pause, Maryland should not pause in its deliberations about how to protect its residents from face recognition technology. While the moratorium is in place, this legislature should consult with privacy experts, civil rights advocates, and—most importantly—the communities most impacted by and vulnerable to the use of surveillance technologies like face recognition.

Eight other states (California, Colorado, Maine, Michigan, New Hampshire, Oregon, Vermont, and Washington) have chosen to regulate face recognition technology through a variety of means. New Hampshire, Oregon, Vermont, and Washington have all restricted the use of face

[18] *Id.*

[19] *Maryland Gives Federal Law Enforcement Access To MVA Records, Kojo Nnamdi Show* (Mar. 4, 2020), https://thekojonnamdishow.org/shows/2020-03-04/maryland-gives-federal-law-enforcement-access-to-mva-record; Department of Public Safety and Correctional Services, https://drive.google.com/file/d/1tus_FlmAevIytlja0SIU53qNpPVn3qc6/view?usp=sharing; Drew Harwell & Erin Cox, *ICE has run facial-recognition searches on millions of Maryland drivers*, The Washington Post (February 26, 2020)

[20] Letter from Kevin Combs, Chief Information Officer, Information Technology and Communications Division, Department of Public Safety and Correctional Services, to Sen. Susan C. Lee et al., Nov, 21, 2019.

recognition technology on photos taken in collection with a driver's license.[21] Oregon and California both prohibit the use of face recognition technology on surveillance taken from law enforcement body-worn cameras.

Six cities (Oakland, CA, San Francisco, CA, Somerville, MA, Brookline, MA, Northampton, MA, and Cambridge, MA) have outright banned the use of the technology.[22] It is up to the Maryland legislature to decide how they want to regulate or ban this technology.

Jurisdiction	**Regulation of Face Recognition Technology**
California[23]	Prohibits biometric surveillance in police officer cameras.
Oakland, CA[24]	Amends Oakland's existing "Regulation on City's Acquisition And Use Of Surveillance Technology" to add the definition of face recognition technology and make it illegal for any city staff to use any face recognition technology.
San Francisco, CA[25]	Bans city staff from using face recognition technology. Includes exceptions for federally controlled facilities at San Francisco International Airport and the Port of San Francisco.
Colorado[26]	Requires the Department of Revenue to promulgate rules that ban access to and use of face recognition technology unless to aid federal, state, or local government when they have reasonable suspicion a crime has been committed.
Maine[27]	Mandates the Board of Trustees of the Main Criminal Justice Academy, in consultation with the Attorney General, to establish minimum standards for law enforcement's use of unmanned aerial vehicles that restrict the use of face recognition technology.
Michigan[28]	Requires the deletion of biometric data collected from people who are arrested if charges are not brought.

[21] See table below.

[22] See table below.

[23] The Body Camera Accountability Act, Assem. Bill 1215, 2019-2020 Reg. Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

[24] City of Oakland, Adopt An Ordinance Amending Oakland Municipal Code Chapter 9.64 To Prohibit The City Of Oakland From Acquiring And/Or Using Face Recognition Technology (2019), https://oakland.legistar.com/LegislationDetail.aspx?ID=3976661&GUID=CB1D4794-7549-485A-A345-B7B38B38E191.

[25] San Francisco, CA, Ordinance No. 103-19 (2019), https://sfbos.org/sites/default/files/o0103-19.pdf.

[26] C.R.S. § 42-2-114(V)(A).

[27] Me. Rev. Stat. Ann. tit. 25 § 4501(5)(D).

[28] Mich. Comp. Laws Ann. § 28.243(7)-(8).

New Hampshire[29] [30]	Prohibits use of face recognition technology on recordings from police body-worn cameras. Prohibits the Department of Public Safety from using face recognition technology in connection with taking or retaining photos for the purposes of motor vehicle registration or driver licensing.
New Hampshire[31]	Prohibits the state from collecting, obtaining, and retaining any biometric data, including face features pattern characteristics, in connection with motor vehicle registration or driver licensing.
Oregon[32] [33]	Prohibits law enforcement use of biometric technologies to analyze recordings obtained from officer body cameras. Prohibits the Department of Transportation from sharing biometric data collected the course of issuing driver licenses, driver permits, and identification cards.
Vermont[34] [35]	Prohibits the use of face recognition technology on any data collected by a drone on a person, home, or area other than the target of surveillance. Prohibits procedures or policies by the Department of Motor Vehicles that utilize biometric technology to identify applicants for licenses, learner permits, or non-driving identification cards.
Washington[36]	Restricts face recognition technology use on drivers' licenses, permits, and "identicards" for verification of the identity of an applicant for such identification cards. Results of the face recognition technology use may only be disclosed with a court order or to a government agency if the individual has committed certain prohibited practices. Requires the department to post notice at all drivers' license offices regarding the use of face recognition technology.
Somerville, MA[37]	Bans city staff from using face recognition technology.
Brookline, MA[38]	Bans city staff from using face recognition technology.

[29] N.H. Rev. Stat. Ann. § 105-D:2(XII).

[30] N.H. Rev. Stat. § 260:40-b.

[31] N.H. Rev. Stat. § 260:10-b.

[32] Or. Rev. Stat. § 133.741(1)(b)(D).

[33] Or. Rev. Stat. § 807.026.

[34] Vt. Stat. Ann tit 20 § 4622(d)(2).

[35] Vt. Stat. Ann. tit. 23, § 634(c).

[36] R.C.W. 46.20.037.

[37] Somerville, MA, Code of Ordinances, Ordinance No. 2019-16 (2019), https://library.municode.com/ma/somerville/ordinances/code_of_ordinances?nodeId=966223.

[38] Brookline, MA, Town By-Laws, Article 8.39 (2020).

Northampton, MA[39]	Prohibits the city from collecting biometric information through surveillance cameras.
Cambridge, MA[40]	Bans city staff from using face recognition technology.

SB857 provides a much needed "pause" on the use of face recognition technology.

A moratorium will allow this body time to better understand face recognition technology and its impacts on vulnerable communities, and to reconsider how—if at all—the technology should be used in Maryland. Face recognition technology has real, tangible effects on CASA members' ability to move about the world. Rather than receiving medical help or police assistance or an education, CASA members may avoid being seen in public for fear that ICE could use their face to deport them or a loved one. We urge this legislature to pass SB857 as a first step in protecting the privacy of Maryland's immigrant communities from dangerous technology.

[39] Northampton, MA, Code of Ordinances, Ord. No. 19.176 (2019).
[40] Cambridge, MA, Code of Ordinances, Ch. 2.128.075 (2020).