



Statement of Alvaro M. Bedoya, Founding Director

Center on Privacy & Technology at Georgetown Law

Hearings on

The Maryland Driver Privacy Act (SB 234 & HB 23)

Wednesday, January 27, 2021 & Thursday, January 28, 2021

For more information, contact Alvaro Bedoya at amb420@georgetown.edu.

1. Introduction & Background

I am testifying on behalf of the Center on Privacy & Technology at Georgetown Law, where I am also a Visiting Professor of Law. The Center researches both government and corporate surveillance, particularly its impact on historically marginalized people. We advocate in favor of policies that protect privacy for everyone. We urge the Senate to pass the Maryland Driver Privacy Act (SB 234) to protect all Marylanders from warrantless searches and face scans by federal immigration enforcement.

I have researched and crafted policy around the government's access to people's private information for over a decade. In 2011, I was named Chief Counsel to the U.S. Senate Judiciary Subcommittee on Privacy, Technology & the Law, where I organized the Subcommittee's oversight on the National Security Agency, the Federal Bureau of Investigation, the Department of Justice, as well as companies like Apple, Google, Facebook, and Netflix.

In 2014, I founded the Center on Privacy & Technology at Georgetown Law. The Center has focused its research on: (1) government use of face recognition technology, and (2) immigration enforcement's massive investments in surveillance and data-sharing. We have written four reports on face recognition technology.¹ Among other things, those reports led Congress to enact the first federal law mandating bias-testing in an artificially intelligent federal system, and triggered a field-defining study by the National Institute of Standards and Technology that verified the existence of deep race, gender, and age bias in most face recognition systems.² We regularly consult with Democratic and Republican state legislators and members of Congress.

My wife and I live in Rockville, Maryland (District 19), with our two children.

2. Immigrants trust the MVA with their data. ICE's unfettered access to it betrays that trust.

In 2013, the General Assembly passed the Maryland Highway Safety Act, extending eligibility for driver's licenses and identification cards to all Marylanders, regardless of their immigration status. The legislation was a watershed for immigrants in our state, who no longer had to choose between obeying the law and driving a car to meet their basic needs. "I'll be able to go to school, go to work and visit my family," one Baltimore teen told the *Sun*, explaining how hard it had been to shuttle between two restaurant

¹ See Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Center on Privacy & Technology at Georgetown Law, 2016); Harrison Rudolph, Laura Moy, and Alvaro Bedoya, *Not Ready for Take-Off: Face Scans at Airport Departure Gates* (Center on Privacy & Technology at Georgetown Law, 2017); Clare Garvie, *Garbage In Garbage Out: Face Recognition on Flawed Data* (Center on Privacy & Technology at Georgetown Law, 2019); and Clare Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States* (Center on Privacy & Technology at Georgetown Law, 2019).

² See Section 1919 of the FAA Reauthorization Act of 2018; Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (National Institute of Standards & Technology, 2019) at 1.

jobs and community college classes without a license.³ By August 2014, close to 40,000 Marylanders had filed proof of two years' of tax payments and passed the necessary exams to get a new license or learner's permit.⁴

Unfortunately, not even a year after the MVA began accepting applications from undocumented Marylanders, it became clear that Immigration and Customs Enforcement (ICE) agents were accessing their information. In August 2014, residents of the Melvin Park Apartments in Catonsville reported that ICE agents were stopping nearby cars with the names or license photos of undocumented drivers in hand. In one case, they arrested the father of a three-year-old boy; the father had no criminal record beyond his prior attempts to cross the border.⁵

This happened again in February of last year in Rockville. In this instance, ICE agents knocked on the door of Maribel Cortez and José Santos Quintero, immigrants from El Salvador who have lived here for decades without any run-ins with the police or immigration authorities. One of their five children answered. The ICE agents quickly entered, arrested their father, and took him away. The agents told Mr. Quintero that they had found him using his license data.⁶

Around that time, the *Sun* and the *Washington Post* confirmed that ICE agents weren't just searching through Maryland drivers' addresses – they were also running face recognition searches on the photos of all 7 million Maryland drivers. The Department of Public Safety and Correctional Services (DPSCS) disclosed this information only after Senators Susan Lee and Clarence Lam, and Delegates Dana Stein and Joseline Peña-Melnyk wrote to the agency to ask for the information.⁷

DPSCS admitted that between 2018 and 2019, ICE agents logged 56 sessions inside the MVA system.⁸ DPSCS did not disclose the number of face scans conducted during each of these sessions, apparently because the Maryland Image Repository System (MIRS), Maryland's face recognition database, did not track that information. In other words, *DPSCS appears to have no idea of how many searches ICE has run and continues to run on Maryland drivers' faces.*

When Marylanders give the MVA their names, addresses, dates of birth, and sit for a license photo, they trust that the MVA, and by extension, our state government, will be careful stewards of that data. In this sense, getting a license is a true leap of faith for our undocumented neighbors, who volunteer their data despite the fact that its release could result in their deportation. By giving ICE unimpeded, warrantless access to scan

³ Pamela Wood, "Thousands of immigrants seek drivers licenses," *The Baltimore Sun*, Dec. 31, 2013.

⁴ John Fritze, "Raid spurs fear of driver's licenses among immigrants," *The Baltimore Sun*, Sep. 20, 2014.

⁵ *Ibid.*

⁶ Erin Cox, "Gov. Hogan opposed to ending ICE's warrantless access to driver's license database," *The Washington Post*, Feb. 27, 2020.

⁷ Kevin Rector, "ICE has access to Maryland driver's license records. State lawmakers want to limit it," *The Baltimore Sun*, Feb. 26, 2020; Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," *The Washington Post*, Feb. 26, 2020.

⁸ DPSCS Letter to Senators Lee and Lam and Delegates Stein and Peña-Melnyk, November 21, 2019.

Marylanders' faces and search through their data, our government betrays that trust. It also endangers *all* Marylanders, citizens and non-citizens alike.

3. Maryland's face recognition system is uniquely open and vulnerable to abuse by ICE.

At least 20 other states allow Federal Bureau of Investigation (FBI) agents to request scans of driver's license photographs.⁹ From our review of documents from dozens of FOIA requests, Maryland appears to be unique in allowing *any* law enforcement officer, anywhere in the country, to login directly and scan drivers' faces so long as they hold National Crime Information Center (NCIC) credentials. That is an unprecedented level of access for federal agents, including ICE deportation officers.

What's more, while nine other jurisdictions have enacted laws or policies requiring ICE to obtain a court order before obtaining license information from the DMV (i.e. California, Colorado, District of Columbia, Hawaii, New York, New Jersey, Oregon, Vermont, Washington), or requiring any law enforcement agency to get a court order prior to a face recognition search (Washington), Maryland has no such requirement. Instead, the MIRS merely requires that users access the system only for "law enforcement investigatory purposes." However, DPSCS does not seem to have any way to enforce this *de minimis* standard.

In fact, as of December 2017, DPSCS did not have any audit or review process for its face recognition system.¹⁰ In a November 2019 letter, the agency told Senators Lee and Lam and Delegates Stein and Peña-Melnik that a "user's search results are saved under their session and are not available to any other user."¹¹

In other words, DPSCS built a system that can automatically scan the faces of millions of Maryland drivers – and handed the keys to that system to ICE agents around the country, knowing that the Department would be unable to audit their searches or prevent abuse and misuse.

4. ICE face recognition searches endanger all Marylanders, not just immigrants.

One morning in April 2019, a college senior from Baltimore, Amara Majeed, woke up to 35 missed calls. The frantic messages informed her that she had been falsely identified as a suspect in the recent terror attacks in Sri Lanka, home to her extended family. The authorities there would later tell the *Boston Globe* that the false ID had stemmed from a mistake made by face recognition software.¹² American law enforcement officials have

⁹ These states include Alabama, Arizona, Arkansas, Colorado, Delaware, District of Columbia, Florida, Illinois, Indiana, Iowa, Kentucky, Michigan, Nebraska, New Mexico, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, and Utah.

¹⁰ See DPSCS Letter to Chairman Kasemeyer and Chairman McIntosh, December 1, 2017.

¹¹ See *supra* footnote 8.

¹² See Jeremy C. Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect," *Boston Globe*, April 28, 2019.

made similar mistakes. Just in 2020, press reports confirmed that three innocent Black men had been wrongfully arrested as a result of faulty face recognition searches.

Ms. Majeed and these three gentlemen have something in common: they are all people of color, a demographic that research has consistently shown is prone to misidentification by many popular face recognition algorithms.¹³ In Ms. Majeed's case, she is also a young woman, and research has verified that face recognition systems are more likely to misidentify women rather than men, and young or old people rather than the middle-aged. Indeed, a December 2019 study triggered by the Center's research, the National Institute of Standards and Technology conducted a review of 189 algorithms from 99 companies and found race, age, and gender disparities to be pervasive, albeit not universal.¹⁴

These biases make ICE's face recognition searches a direct threat to all Marylanders, not just immigrants. When it comes to ICE face scans, the operative question is not "Are you an undocumented immigrant?" The question is: "Does a biased algorithm *think* you *look like* an undocumented immigrant?"

5. We have no idea how often ICE searches Maryland drivers' data.

There appear to be no public statistics, anywhere, for how often ICE agents search for Maryland drivers' names, addresses, or license numbers *outside* of a face recognition search through the Nlets network. MVA and DPSCS do not disclose any of this data. In fact, the Department has recently received a public information request from our Center and a separate letter from Sen. Lam asking that it release the number of times ICE has run Nlets searches on Marylanders' license information. Strangely, the Department referred the Center's query to the Maryland State Police, and sent Sen. Lam's query to the MVA.

This stonewalling is not acceptable. ICE's use of a Maryland state system to find and deport Marylanders cannot be cloaked in secrecy. What's more, information about ICE searches of these systems should be pushed out regularly, automatically, and as a regular function of agency business – not solely in response to official requests from Maryland legislators.

6. The Maryland Driver Privacy Act will protect Marylanders' data from warrantless ICE searches.

The Maryland Driver Privacy Act (SB 234) will put in place four common sense privacy protections for Marylanders' data held by the MVA or other state agencies. The bill will:

¹³ Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (National Institute of Standards & Technology, 2019)

¹⁴ *Ibid.*

- Require that federal agents enforcing immigration law get a warrant before they scan Marylanders' photos or search their data held by the MVA or other state agencies.
- Prohibit private companies who receive Marylanders' data or photos from the MVA or other state agencies from selling or sharing that information to federal agents enforcing immigration law – unless if they are presented with a warrant.
- Require state agencies to report annually on the number of these requests they receive, the number that were accompanied by warrants or court orders, and the number of requests they answered and complied with.
- Prohibit ICE from having direct access to Maryland government databases (reinforcing the rule that they present a warrant to state officials to get Marylanders' information), and prohibit other law enforcement agents from accessing Maryland databases in order to enforce immigration law – unless if the database operator is presented with a warrant.

By explicitly stating that ICE and CBP agents *can* obtain Marylanders' data if they get a warrant, this bill makes it clear that serious criminal investigations can go forward without undue impediment.

7. The Maryland Driver Privacy Act will bring Maryland in line with state and federal best practices.

The Maryland Driver Privacy Act provisions will bring Maryland in line with best practices on how to protect licensed drivers who are undocumented. As discussed above, nine jurisdictions who offer undocumented residents driver's licenses now require warrants before they surrender DMV data to immigration enforcement. This bill will make Maryland the tenth jurisdiction to apply that standard (the ninth state, not counting D.C.), and also add protections against middlemen and against data held by agencies other than the DMV, like the laws in New York and the District of Columbia, respectively.

While there is no such thing as a federal DMV, similar protections apply for information given to the U.S. Census. By statute, the government is prohibited from using Census data for general law enforcement.¹⁵ To be crystal clear, ICE is walled off from accessing Census data.

Federal and state governments have recognized that some information must be protected from their own law enforcement agencies in order to discharge other government duties, like ensuring an accurate Census count, or, in this instance, ensuring safe roads for all drivers.

¹⁵ See 13 U.S.C. §8(c) ("In no case shall information furnished under this section be used to the detriment of any respondent or other person to whom such information relates, except in the prosecution of alleged violations of this title.").

8. Conclusion

Year after year, Maryland distinguishes itself as a leader in protecting all of its residents, regardless of their immigration status. But it is not enough to make our *state* government a welcoming and fair system for our immigrant community. We also need to take affirmative steps to protect them from invasions by the federal government. This is our chance to protect Maryland immigrants and make roads safer for *all* Maryland drivers -- while preventing ICE from treating our driver's license data as a deportation goldmine. What's more, given the consistent bias in face recognition, this bill will protect all Marylanders from a deeply flawed technology.

We urge you to vote in favor of the Maryland Driver Privacy Act.