OUT OF THE SHADOWS: REGULATING ACCESS TO DRIVER'S LICENSE DATABASES BY GOVERNMENT AGENCIES

ABSTRACT

You post a photo to Facebook and the social media site automatically asks if you want to tag yourself and your three friends by name. If Facebook can use facial recognition technology to identify us, should the government be allowed to do the same? While the commercial use of facial recognition technology is an issue in and of itself, this Note will be limited in scope to use by government agencies. Popular crime investigation shows on television might lead us to believe law enforcement agencies already employ this technology, but from where do we assume their databases are generated? Does law enforcement only run suspect photos against a repository of persons already convicted of crimes or are our driver's licenses and other identity card photographs included in the mix? And which government agencies have access? Perhaps you would assume the Federal Bureau of Investigation (FBI) does, but what about Immigration and Customs Enforcement (ICE)?

This Note will address the evolving world of facial recognition technology with a specific focus on driver's license photographs used and shared across government agencies. By surveying the current regulatory landscape in this field—or lack thereof—and the concerns presented by the growing use and unchecked sharing of this technology, opportunities for its regulation will be revealed. Ultimately, this Note supports a national moratorium on the sharing of Department of Motor Vehicle (DMV) data for facial recognition searches to allow the public a chance to engage in critical review of how, why, and whether this technology should be employed by government agencies.

TABLE OF CONTENTS

I. INTRODUCTION

You post a photo to Facebook and the social media site automatically asks if you want to tag yourself and your three friends by name. If Facebook can use facial recognition technology to identify us, should the government be allowed to do the same? While the commercial use of facial recognition technology is an issue in and of itself, this Note will be limited in scope to use by government agencies. Popular crime investigation shows on television might lead us to believe law enforcement agencies already employ this technology, but from where do we assume their databases are generated? Does law enforcement only run suspect photos against a repository of convicted criminals or are our driver's licenses and other identity card photos included in the mix? And which government agencies have access? Perhaps you would assume the Federal Bureau of Investigation (FBI) does, but what about Immigration and Customs Enforcement (ICE)?

A bombshell report by *The Washington Post* released in the summer of 2019 suggests most people did not imagine driver's licenses were included in this repository.[1] Reactions from fear and confusion to denial and calls to action ran rampant.[2] The reporting relayed findings by Georgetown Law's Center on Privacy and Technology revealing federal agencies—including the FBI and ICE—have not only had access to states' department of motor

1. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [hereinafter Harwell, *Gold Mine*].

2. *See, e.g.*, *Lawmakers Concerned by Agents Use of Driver's Licenses to Track Migrants*, NPR (July 9, 2019), https://www.npr.org/2019/07/09/739809036/lawmakers-concerned-by-agents-use-of-drivers-licenses-to-track-migrants [https://perma.cc/H8MS-Y8U5] [hereinafter *Lawmakers Concerned*]; Lee Davidson, *Utah Officials Deny Reports of Wholesale ICE and FBI Facial Recognition Sweeps Through State Driver License and Driving Privilege Card Databases*, SALT LAKE TRIB. (July 9, 2019), https://www.sltrib.com/news/politics/2019/07/08/utah-officials-deny/.

vehicles (DMV) databases but also have been able to use this data for facial recognition scans.[3] In fact, this "breaking news" in July 2019 was not even news to many individuals who have faced its consequences in the immigration context.[4] In 2016, the National Immigration Law Center (NILC) reported ICE had been accessing driver's license data and facial recognition scans for years.[5] In fact, a Government Accountability Office (GAO) report from January 2005 indicates ICE prefers turning to DMV records because it considers this information more accurate and reliable than its own agency database.[6] After first having to file a lawsuit to compel ICE to respond to its Freedom of Information Act (FOIA) inquiry, NILC maintains, "ICE's explanations of when and how it uses DMV information are [still] incomplete or misleading."[7] As a result, government watchdogs are continuing to try to piece together the full picture of the federal government's facial recognition capabilities and practices.[8] Two of the latest lawsuits alleging failure to comply with FOIA requests regarding facial recognition were filed in the fall of 2019 by The Project on Government Oversight against ICE and by the American Civil Liberties Union (ACLU) against the Department of Justice (DOJ), FBI, and Drug Enforcement Agency (DEA).[9]

This Note will address the evolving world of facial recognition technology with a specific focus on driver's license photographs used and shared across government agencies. By surveying the current regulatory landscape in this field—or lack thereof—and the concerns presented by the

3. Harwell, *Gold Mine*, *supra* note 1.

4. *How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information*, NAT'L IMMIGR. L. CTR. (May 2016), https://www.nilc.org/issues/drivers-licenses/ice-dmvs-share-information/ [https://perma.cc/8WDC-U4AA] [hereinafter *How ICE and State Dept's Share*, NILC].

5. *Id.*

6. *Alien Registration: Usefulness of a Nonimmigrant Alien Annual Address Reporting Requirement Is Questionable*, U.S. GOV'T ACCOUNTABILITY OFF. (Jan. 28, 2005), https://www.gao.gov/assets/250/245209.html [https://perma.cc/B9L3-K4KB].

7. *How ICE and State Dept's Share*, NILC, *supra* note 4.

8. Taylor Telford, *ICE Refuses to Turn over Internal Documents on Facial Recognition Tech and Detention Tactics, Lawsuit Says*, WASH. POST (Nov. 7, 2019), https://www.washingtonpost.com/business/2019/11/07/ice-refuses-turn-over-internal-documents-facial-recognition-tech-detention-tactics-lawsuit-says/; Drew Harwell, *ACLU Sues FBI, DOJ over Facial-Recognition Technology, Criticizing 'Unprecedented' Surveillance and Secrecy*, WASH. POST (Oct. 31, 2019), https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/ [hereinafter Harwell, *ACLU Sues*].

9. Telford, *supra* note 8; Harwell, *ACLU Sues*, *supra* note 8.

growing use and unchecked sharing of this technology, this Note will reveal opportunities for its regulation.

To begin, Part II provides a foundation for why DMVs use facial recognition technology. Part III identifies which additional government agencies have general access to DMV data for facial recognition purposes. Part IV then details the concerns raised by such practices through consideration of its repercussions for privacy, civil rights, and the unique circumstances of undocumented immigrants. Turning to the current regulatory landscape, Part V samples the primary regulatory approaches to DMV data sharing employed by various states. Part VI proposes recommendations for legislative change, including instituting stringent accuracy standards, requiring a court order, and providing public notice while Part VII offers final conclusions. Ultimately, this Note supports a national moratorium on the sharing of DMV data for facial recognition searches to allow the public a chance to engage in critical review of how, why, and whether this technology should be employed by government agencies.

II. WHY IS FACIAL RECOGNITION TECHNOLOGY USED BY DMVS?

Many states have implemented facial recognition software within their DMVs to combat fraud and identity theft.[10] When a person comes in to apply for or renew a driver's license, that individual's photograph is run through facial recognition to determine if it matches any already in the database and identifies people with two or more identities.[11] The success of the software for these purposes cannot be ignored.[12] For instance, New York reported in 2017 having initiated over 21,000 investigations for fraud or identity theft through the Department of Motor Vehicles' Facial Recognition Technology

10. *See* Harwell, *Gold Mine*, *supra* note 1 (reporting the state of Washington's technology "is designed to be an accurate, non-obtrusive fraud detection tool"); *see also ACLU Demands Immediate End to DMV Facial Recognition Program*, ACLU VT. (May 24, 2017), https://www.acluvt.org/en/press-releases/aclu-demands-immediate-end-dmv-facial-recognition-program [https://perma.cc/9JPL-W74Q] [hereinafter ACLU VT.] (acknowledging the state of Vermont's claim the software was intended to be used for identity theft and fraud prevention).

11. *See, e.g.*, *Governor Cuomo Announces Major Facial Recognition Technology Milestone with 21,000 Fraud Cases Investigated*, N.Y. STATE (Aug. 21, 2017), https://www.governor.ny.gov/news/governor-cuomo-announces-major-facial-recognition-technology-milestone-21000-fraud-cases [https://perma.cc/92MN-SH2Q].

12. *Id.*

Program since its inception in 2010.[13] These investigations have resulted in over 4,000 arrests and more than 16,000 individuals facing administrative action.[14] The importance of identifying these fraudulent applications is underscored by the reality that many drivers applying for multiple licenses have had their license revoked or suspended under their true identities for traffic safety reasons.[15]

In a similar effort, the state of New Jersey reported in 2013 having charged its first 38 defendants with trying to obtain fraudulent driver's licenses under its facial recognition program known as "Operation Facial Scrub."[16] New Jersey's then-Attorney General Jeffrey Chiesa justified the program stating, "We know the 9/11 terrorists had fraudulent licenses from other states. By detecting individuals who have false licenses, law enforcement can potentially uncover other types of crime that these individuals may be involved in, including identity theft, financial fraud and even terrorism."[17] Here in Iowa, the state's use of a biometric recognition system enabled the State Department of Motor Vehicles to flag an applicant's photograph for a driver's license and ultimately catch a North Carolina prison escapee.[18]

III. WHO ELSE CAN ACCESS DMV DATABASES?

The government agencies with access to DMV systems varies by state.[19] For instance, the FBI has an internal facial recognition unit—known as

13. *Id.*

14. *Id.*

15. *Id.*

16. *Attorney General and MVC Chief Showcase High-Tech Program "Operation Facial Scrub" to Detect False Driver's Licenses*, STATE N.J. OFF. ATT'Y GEN. (Feb. 12, 2013), https://www.nj.gov/oag/newsreleases13/pr20130212a.html [https://perma.cc/JQ3C-F4RP].

17. *Id.*

18. Jeff Reinitz, *Suspected NC Fugitive from 1970s Caught in Waterloo*, THE COURIER (Apr. 16, 2014), https://wcfcourier.com/news/local/crime-and-courts/suspected-nc-fugitive-from-s-caught-in-waterloo/article_cb4c10ba-e84c-5e5d-9395-ccfec0f78d83.html. The individual's image was flagged because he had applied for an Iowa driver's license a year earlier using a different name—not because of his escapee status. *Id.*

19. *See, e.g.*, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains*, U.S. GOV'T ACCOUNTABILITY OFF. 3 (June 4, 2019), https://www.gao.gov/assets/700/699489.pdf [https://perma.cc/KJF3-TRSE] [hereinafter *DOJ and FBI Have Taken Some Actions*].

Facial Analysis, Comparison, and Evaluation (FACE)—that has the ability to search or request to search the driver's license databases of 21 states.[20] FBI officials cite the law enforcement exception in the Driver's Privacy Protection Act (DPPA) as legal authority for the states to share these photos with the FBI.[21] However, no state has adopted legislation affirmatively authorizing this kind of sharing by its agents.[22] As a result, administrative officials have unilaterally entered into privacy agreements with federal agencies, such as the FBI and ICE, to memorialize the access being granted for government purposes.[23] Lawmakers have raised concerns over the origination of these privacy agreements because they are generated administratively between the state DMV or Department of Transportation (DOT) and the other agency—FBI, ICE, etc.—interested in obtaining access, often without any express legislative authority for the action.[24] Iowa's state law prohibits the release of personal information from driver's licenses.[25] Although, an exception is carved out for release to employees of government agencies "in the performance of the employee's official duties."[26] Therefore, obtaining access is as simple as completing the proper form and identifying oneself as a government agent carrying out official functions.[27] Moreover, this access is often completely unchecked such that

20. *Id.*; *see also* Alexis Arnold, *What States Do to Protect Undocumented Immigrants' Driver's License Information*, HUFFPOST (July 12, 2019), https://www.huffpost.com/entry/undocumented-immigrants-drivers-license-state-privacy-laws_n_5d2788cae4b0bd7d1e197225.

21. *DOJ and FBI Have Taken Some Actions*, *supra* note 19, at 4; *see also* 18 U.S.C. § 2721 (2018).

22. *See* Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

23. *See, e.g.*, *Documents Obtained Through the 2014 FOIA Request & Lawsuit*, NAT'L IMMIGR. L. CTR. 240–62, https://www.nilc.org/wp-content/uploads/2016/05/driver-license-info-sharing-pp192-444.pdf [https://perma.cc/Z4TC-A88V] [hereinafter *Documents Obtained*, NILC] (disclosing three exchanges in which an Iowa DOT agent provides a privacy agreement for an ICE agent to complete to access the Iowa DOT's Driver License/ID image retrieval system from which users can access color driver's license and ID photos and signatures. This agreement acknowledges it is made pursuant to the DPPA and any further disclosure of the information obtained must be recorded and made available to the Iowa DOT).

24. *See, e.g.*, *Lawmakers Concerned*, *supra* note 2 (transcribing an interview with the House Oversight Committee's top Republican—Ohio Representative Jim Jordan).

25. IOWA CODE § 321.11(4) (2019).

26. *Id.*

27. *See Documents Obtained*, NILC, *supra* note 23, at 251–55.

federal agents are not required to record when or why they access the database.[28] Rather—as seen in the Iowa agreement—federal agents only have to take steps to record instances when they share the photograph or data obtained from the state database.[29] Sharing the photo is not necessary when it is used internally to locate an individual.

Moreover, the Georgetown investigation revealed federal law enforcement agencies are often able to use driver's licenses through informal e-mails to state agency employees asking them to run facial recognition searches.[30] "[M]any requests for searches involved nothing more than an e-mail to a DMV official with the target's 'probe photo' attached. The official would then search the driver's license database and provide details of any possible matches."[31]

The NILC has likewise reported based on its FOIA findings that ICE can obtain photos from state DMV databases through simple e-mail requests, as well as through automated systems, such as Nlets Photo Sharing, and state networks, such as Cal-Photo.[32] While Cal-Photo is a California driver's license repository similar to the Iowa DOT database accessible after administrative approval,[33] the e-mail exchanges between ICE agents and DMV or DOT employees offer another efficient avenue for accessing this information.[34] These e-mails have extended to providing ICE agents with an individual's vehicle registration, home address, and complete driver history

28. *See id.*

29. *See id.*

30. Harwell, *Gold Mine*, *supra* note 1.

31. *Id.*

32. *Backgrounder: Face Recognition and Driver's License Photo-Sharing*, NAT'L IMMIGR. L. CTR. (Oct. 2019), https://www.nilc.org/issues/drivers-licenses/face-recognition-and-dl-photo-sharing/#_ftnref1 [https://perma.cc/YXP6-HUKF].

33. *Compare How California Driver's License Records Are Shared with the Department of Homeland Security*, NAT'L IMMIGR. L. CTR. (Dec. 2018), www.nilc.org/wp-content/uploads/2019/01/DMV-PRA-report-2018-12.pdf [https://perma.cc/4YQH-AMBG], *with Documents Obtained*, NILC, *supra* note 23, at 251–55; *see also* Spencer Woodman, *Despite Their Liberal Politics, Connecticut and California Are Sharing Immigrant Data with ICE*, VERGE (Feb. 22, 2017), https://www.theverge.com/2017/2/22/14692842/ice-immigration-trump-data-connecticut-california [https://perma.cc/5P8M-FZ2E] (providing another example of a state database to which ICE has access—Connecticut's police database provides ICE with access not only to state DMV data but also court data, probation information, protective orders, boating certifications, hunting and fishing licenses, and other data).

34. *See Documents Obtained*, NILC, *supra* note 23, at 263–88 (revealing e-mail exchanges between Iowa DOT employees and ICE agents).

(including relevant convictions and license revocations).[35] The Iowa DOT has even advised ICE of arrests it makes for identity theft without any apparent inquiry from the federal agency.[36] As for Nlets Photo Sharing, according to its website:

> Nlets, is a private not for profit corporation owned by the States that was created more than 50 years ago by the 50 state law enforcement agencies. The user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community . . . .[37]

Nlets reports driver's license photo sharing among its members extends to 36 states and Puerto Rico fully sharing and receiving, 2 states with limited sharing, 4 states plus the District of Columbia and Canada only receiving photos, and 8 states as well as Guam and the U.S. Virgin Islands not participating.[38]

States must also provide means for all other states to electronically access their driver's licenses databases pursuant to the REAL ID Act passed by Congress in 2005.[39] However, the REAL ID Act does not address federal agency access and would therefore not require the kind of sharing enabled by systems such as Nlets.[40]

35. *See id.*

36. *See id.* at 273. An October 2011 e-mail from the Iowa DOT reads, "Today I arrested [redacted] and transported her to the Muscatine County Jail for Identity Theft, Class D Felony. She was working under the identity of [redacted]. She advised she also used the identity of [redacted]. She advised she is from Durango Mexico and has been in the US for about 15 years. FYI." *Id.*

37. *Who We Are*, NLETS, https://www.nlets.org/about/who-we-are [https://perma.cc/L9R8-B937].

38. *Our Members*, NLETS, https://www.nlets.org/our-members/grantmaps?mapid=d26b4e70-934e-11e3-9a61-00155d003202 [https://perma.cc/8F2B-4YP8].

39. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 312. The Act provides, "To meet the requirements of this section, a State shall adopt the following practices in the issuance of drivers' licenses and identification cards: . . . (12) Provide electronic access to all other States to information contained in the motor vehicle database of the State." *Id.* It goes on to require states to maintain a motor vehicle database containing all fields printed on driver's licenses and driver histories including violations, suspensions, and points on licenses. *Id.*

40. *See id.*; *Our Members*, *supra* note 38.

IV. WHAT IS THE PROBLEM WITH THIS USE AND ACCESS?

The use of facial recognition technology has raised substantial concerns about civil rights, privacy, and the impact on immigrants—particularly those who are undocumented in states permitting them to obtain driving privileges.[41] Many U.S. residents would be alarmed to learn about the opportunities this technology presents for the government's ability to track individuals, the increasing impossibility to remain anonymous, and the potential for biased and inaccurate results.[42] As Jay Stanley, a senior policy analyst at the ACLU pointed out, "Face recognition technology—accurate or not—can enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale."[43]

A. *Constitutional Rights: Protest and Privacy*

Critics of the current government use of facial recognition technology worry its use will exacerbate inequalities and threaten civil liberties protected by the First and Fourth Amendments to the U.S. Constitution.[44] With regard to inequalities, the technology has been widely criticized for its gender and racially biased results.[45] Civil rights advocates and researchers

41. *State Laws Providing Access to Driver's Licenses or Cards, Regardless of Immigration Status*, NAT'L IMMIGR. L. CTR. (Apr. 2020), https://www.nilc.org/wp-content/uploads/2015/11/drivers-license-access-table.pdf [https://perma.cc/HR5G-5K3M] [hereinafter *State Laws*, NILC]. The following jurisdictions provide driver's licenses or cards to state residents without regard to immigration status: California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, New Jersey, New Mexico, New York, Nevada, Oregon, Utah, Vermont, and Washington, as well as the District of Columbia and Puerto Rico. *Id.*

42. *See* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/ [https://perma.cc/6EVN-LL3Y].

43. Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [hereinafter Harwell, *Federal Study*].

44. *See* Jason Tashea, *As Facial Recognition Software Becomes More Ubiquitous, Some Governments Slam on the Brakes*, A.B.A. J. (Sept. 24, 2019), www.abajournal.com/web/article/facial-recog-bans [https://perma.cc/Z667-PFYR]; Tori Bedford, *Mass. ACLU Sues MassDOT over Sharing RMV Photo Database with ICE, FBI*, WGBH NEWS (July 10, 2019), https://www.wgbh.org/news/local-news /2019/07/10/mass-aclu-sues-massdot-over-sharing-rmv-photo-database-with-ice-fbi [https://perma.cc/96P7-RGQX].

45. *See* Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), http://news.mit.edu/2018/st

have warned—accurately or not—the technology "could easily be misused to surveil immigrants or unfairly target African Americans or low-income neighborhoods."[46] Moreover, the technology's use of driver's license databases essentially subjects every ID holder in those systems to a perpetual police lineup without their consent—arguably constituting an unreasonable search and seizure.[47] Moreover, its surveillance potential calls into question whether U.S. residents have constitutional rights to freely attend protests and maintain expectations of privacy or anonymity.[48] The Fourth Amendment protects a person's reasonable expectation of privacy,[49] and scholars have speculated one's face in public would fall within this realm should facial recognition be taken up by the U.S. Supreme Court in this context.[50]

In Massachusetts, the ACLU has sued the state DOT alleging the unregulated sharing of its driver's license database violates the freedoms protected by the First and Fourth Amendments.[51] Specifically, the complaint alleges that "face surveillance technology permit[s] government agencies to monitor the location, movement, and habits of law-abiding residents with a scope not before seen," which is "thanks, in part, to those residents doing nothing more than obtaining a driver's license or photo ID through the Registry of Motor Vehicles."[52] While maintaining that this degree of tracking threatens the reasonable expectation of privacy under the Fourth Amendment, the ACLU goes on to argue it also jeopardizes the First Amendment-protected right "to engage in political protest, as well as intimate and expressive association, speech, and the free exercise of religion

udy-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [https://perma.cc/EE9V-LM5U].

46. Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14 /us/facial-recognition-ban-san-francisco.html.

47. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. PRIV. & TECH. at Section V.B *Fourth Amendment* (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/3K32-2YE6] [hereinafter Garvie, *The Perpetual Line-Up*].

48. *See id.*; Conger et al., *supra* note 46; Bedford, *supra* note 44.

49. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

50. *See* Tashea, *supra* note 44.

51. Bedford, *supra* note 44.

52. Complaint ¶¶ 4–5, ACLU of Mass., Inc. v. Mass. Dep't of Transp., No. 1984-cv-02193D (Mass. Dist. Ct. July 10, 2019).

without undue interference by the government."[53] The pleading even provides an example of law enforcement already employing this technology against individuals exercising their right to protest—it points out that "the face surveillance technology company Geofeedia advertised that law enforcement used its technology to identify and arrest protestors with outstanding warrants during the Baltimore protests surrounding the death of Freddie Gray. The advertisement notes that its archive data can be used to arrest and prosecute as many of the protestors as possible."[54]

Given the U.S. government's history of surveillance of civil rights protests, the risk of this technology being used to stifle free speech is not unimaginable.[55] This concern is reflected in the fact that the Ohio Bureau of Criminal Investigation was the only agency—of the 52 agencies identified with facial recognition capabilities by the Georgetown study—found to have a policy precluding facial recognition technology from being used "to track individuals engaging in political, religious, or other protected free speech."[56] Even if such a policy existed, the FBI has continued to employ questionable tactics demonstrating why the agency should not be entrusted with these database-search capabilities to this day.[57] In fact, the FBI continues to target so-called "black identity extremists" in its domestic terrorism operations.[58]

53. *Id.* at ¶ 9.

54. *Id.* ¶ 10 (internal citations omitted).

55. *See Federal Bureau of Investigation (FBI)*, STAN. UNIV., https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi [https://perma.cc/9N68-QFE8] (detailing the FBI's surveillance of Martin Luther King, Jr., among other Black civil rights activists); *#ProtectBlackDissent: Campaign to End Surveillance of Black Activists*, ACLU, https://www.aclu.org/issues/racial-justice/protectblackdissent-campaign-end-surveillance-black-activists [https://perma.cc/F8WW-SXQX] (explaining the organization's FOIA lawsuit against the FBI "demanding that it turn over documents related to the modern-day surveillance of Black activists and Black-led organizations, including through the Bureau's fabrication of a 'Black Identity Extremist' threat category that is based on racial stereotypes rather than evidence of a true security threat").

56. Garvie, et al., *The Perpetual Line-Up*, *supra* note 47, at Section I.A *Key Findings*.

57. Sam Levin, *Black Activist Jailed for His Facebook Posts Speaks out About Secret FBI Surveillance*, THE GUARDIAN (May 11, 2018), https://www.theguardian.com/world/2018/may/11/rakem-balogun-interview-black-identity-extremists-fbi-surveillance (detailing the surveillance of a black activist through the FBI's "domestic terrorism" operations, which led to the activist's home being stormed by armed agents in tactical gear in December 2017 while his sole charge—illegal firearm possession—was later found inapplicable).

58. *See id.*

The Guardian reported, "In a leaked August 2017 report from the FBI's Domestic Terrorism Analysis Unit, officials claimed that there had been a 'resurgence in ideologically motivated, violent criminal activity' stemming from African Americans' 'perceptions of police brutality.'"[59] This report found "it is very likely Black Identity Extremist (BIE) perceptions of police brutality against African Americans spurred an increase in premeditated, retaliatory lethal violence against law enforcement and will very likely serve as justification for such violence."[60] Notably, the FBI's perception of this threat is undermined by the government's own crime data, which finds, "In addition to an overall decline in police deaths, most individuals who shoot and kill officers are white men, and white supremacists have been responsible for nearly 75 [percent] of deadly extremist attacks since 2001."[61]

In addition, facial recognition technology has repeatedly been found "both unreliable and biased, putting people at risk of being falsely connected to a crime or investigation."[62] This risk became all too real for Michigan resident Robert Julian-Borchak Williams, who found himself in an interrogation room professing to officers, "No, this is not me . . . . You think all black men look alike?"[63] Williams was arrested on his front lawn in January 2020 in front of his young children after his driver's license photo was falsely matched by a facial recognition algorithm employed against grainy surveillance camera footage.[64] While Williams's arrest resulted in 30 hours in detention, no one knows how many people like him have ultimately taken a plea bargain or even been incarcerated for crimes they did not commit.[65]

59. *Id.*

60. *Black Identity Extremists Likely Motivated to Target Law Enforcement Officers*, FBI (Aug. 3, 2017), https://assets.documentcloud.org/documents/4067711/BIE-Redacted.pdf [https://perma.cc/AP5L-BBDS].

61. Levin, *supra* note 57.

62. Bill Chappell, *ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa [https://perma.cc/9KKK-B2J7].

63. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

64. *Id.*

65. Clare Garvie, *The Untold Number of People Implicated in Crimes They Didn't Commit Because of Face Recognition*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/the-untold-number-of-people-implicated-in-crimes-they-didnt-commit-because-of-face-recognition/ [https://perma.cc/MS5G-6694].

Statistics demonstrate Williams's story is likely a reality for an untold number of people.[66] For instance, an ACLU study of Amazon's facial recognition technology—known as Rekognition—incorrectly matched 28 members of Congress with mugshots of individuals who had been arrested.[67] Another study conducted on three leading facial recognition programs by the M.I.T. Media Lab found the technology had an error rate of less than one percent for light-skinned men.[68] However, when it came to dark-skinned women, the error rate jumped to over 20 percent in one case and over 34 percent for the other two programs studied.[69] A federal study by the National Institute of Standards and Technology (NIST) found, "Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search."[70] Beyond racial and gender disparities, the potential for false arrest is a new risk given that searches prior to facial recognition technology's development were limited to criminal records rather than including all law-abiding residents with driver's licenses.[71] The lack of guidelines regarding images to be searched in a facial recognition scan multiplies the risk of inaccurate results and false arrests.[72] When law enforcement officials find themselves with a substandard photo incapable of returning a facial recognition match, the lack of parameters means they can often insert any image they choose—even that of a perceived celebrity doppelgänger—to enhance the likelihood of returning a match.[73] However, researchers caution against utilizing these

66. *See id.*

67. Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, N.Y. TIMES (July 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

68. Hardesty, *supra* note 45.

69. *Id.*

70. Harwell, *Federal Study*, *supra* note 43.

71. Chappell, *supra* note 62; *see also* Bedford, *supra* note 44 (reporting, "In April, Brown University student and Muslim activist Amara Majeed was falsely identified as one of the Easter bombing terrorists by Sri Lankan police, after an error with facial recognition technology," regarding which Kade Crockford, the program director of the ACLU's Technology for Liberty Project, said, "We really have no guarantees that those types of abuses won't happen here [in the U.S.]").

72. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/77F4-WEH9] [hereinafter Garvie, *Garbage In*].

73. *See id.* (explaining how New York law enforcement have inserted celebrity photos—like those of actor Woody Harrelson and of a New York Knicks player—in order to achieve a facial recognition match that was not otherwise attainable).

and other unreliable images—such as composite sketches and computer-generated images—when it comes to criminal investigations that could ultimately result in prosecution and deprive someone of their liberties based on a match.[74]

B. *Special Implications for Immigrants*

Sixteen states, as well as D.C. and Puerto Rico, currently allow undocumented immigrants to obtain driver's licenses or driving privilege cards.[75] States have asked undocumented immigrants to come out of the shadows by inviting them to obtain driver's licenses in order to make the roads safer, boost state revenue, increase economic participation, and realize insurance premium savings.[76] However, some states have abandoned the goodwill of those invitations to undocumented immigrants by allowing ICE access to their driver's license databases without the driver's knowledge or consent.[77] Turning this information over to ICE has the potential to result in false arrest if/when ICE relies on this information because it is only a snapshot of a person's immigration history and does not necessarily reflect whether the individual's status has changed.[78]

74. *See id.* (noting the substantial room for error in: (1) sketches because they are based on an eyewitness's memory, ability to communicate that memory, and the artist's ability to accurately translate that memory; and (2) computer-generated facial features because they fabricate identity points—such as eyes, cheeks, and chins—not present in the original photo).

75. *State Laws*, NILC, *supra* note 41.

76. *See Benefits of Expanding Access to Driver's Licenses*, NAT'L IMMIGR. L. CTR., https://www.nilc.org/issues/drivers-licenses/dlaccesstoolkit3a/#benefits [https://perma.cc/V8H3-MGZF] (providing a list of resources explaining the state-specific benefits to permitting undocumented immigrants to obtain driver's licenses).

77. *See, e.g.*, Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/ (reporting ICE can independently search the Maryland driver's license database, which contains more than 275,000 special driver's licenses issued to undocumented immigrants since 2013); *see also* Arnold, *supra* note 20 (detailing the varying degrees of reported access provided by states issuing licenses to undocumented immigrants).

78. *See* Gonzalez v. I.C.E., 416 F. Supp. 3d 995, 999, 1001, 1020 (C.D. Cal. 2019), *aff'd in part, rev'd in part, vacated in part*, 975 F.3d 788 (9th Cir. 2020) (enjoining ICE from issuing a removal order for individuals in that jurisdiction based solely on a review of electronic databases with biometric confirmation, such as facial recognition matching, of the individual's identity because of the potential for inaccuracy).

V. HOW ARE THESE CONCERNS BEING ADDRESSED?

At the federal level, there is no meaningful legislation regulating how agencies may obtain information from state DMVs. For instance, the Privacy Act of 1974 "regulates the way federal agencies collect, maintain, use or disseminate the personal information of individuals," but the Act does not apply to state or local agencies, and most states do not have comparable statutes.[79] Moreover, the "collection" referred to in the Privacy Act pertains to collecting information directly from the individual and does not elaborate on indirect collection from other agencies—such as what is at issue here when the FBI and ICE collect information from state agencies.[80] In addition, the federal Driver's Privacy Protection Act (DPPA), passed in 1994, sets out strict requirements on the use and disclosure of personal information by state DMVs.[81] Even though the DPPA defines a person's photograph or image as "highly restricted personal information"[82] prohibited from disclosure without the individual's express consent, the Act carves out exceptions whereby this information may be disclosed for use by any government agency to carry out its functions.[83] Therefore, the DPPA provides permissive authority for state DMVs to share photographs and any other personal information with any local, state, or federal agency without consent but does not require a disclosure as it does for other purposes, such as motor vehicle emissions, recalls, etc.[84] This gap between permission and required sharing would allow states to regulate further and stop the flow of DMV data to federal agencies, if they so choose.

More specifically, ICE is not subject to any policies regarding its use of or access to DMV data.[85] A Department of Homeland Security (DHS) agent acknowledged this relatively free reign in an e-mail obtained via NILC's FOIA request, stating:

> We don't have any specific policy guidance on when or how to request DMV data and I'm not aware of anything in the works to document beyond the common thread of having an information need based on a

79. Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1963, 1981 (2018).

80. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

81. 18 U.S.C. § 2721.

82. *Id.* § 2725(4).

83. *Id.* § 2721(a)(2), (b)(1), (b)(4), (b)(6), (b)(9).

84. *See id.* § 2721.

85. *How ICE and State Dept's Share*, NILC, *supra* note 4.

> need-to-know, which flows from an ongoing investigation or seeking a particular wanted individual.[86]

This exchange suggests any policy concerning collaboration with other local, state, or federal agencies would be most appropriate coming from the DMV.[87]

The three states identified by Georgetown as having run facial recognition scans of state driver's license photographs—Vermont, Washington, and Utah—have since offered additional information regarding their practices in response to the public outcry.[88] These three states present distinct approaches to the information-sharing in question that is not altogether clear from other agencies which either ignored the Georgetown inquiry or provided incomplete responses.[89]

A. *Banning Biometrics Altogether*

Vermont has a 2004 law banning the use of biometric identifiers that officials now claim is being followed after a 2017 ACLU complaint about the use of facial recognition software on driver's licenses.[90] Biometric identifiers include personal identifiers such as an individual's photograph, DNA, and fingerprints.[91] Contrary to its implementation for fraud prevention, Vermont's facial recognition software, while in use, was offered up to government agencies around the country for inquires unrelated to fraud and identity theft.[92] "According to DMV records, the agency has conducted searches involving people merely alleged to be involved in 'suspicious circumstances.' Other requests have been submitted on the basis of minor offenses such as trespassing or disorderly conduct, while others fail to reference any criminal conduct."[93] Although Vermont has since stopped sharing its facial recognition searches with ICE,[94] the consequences of its earlier collaboration are enlightening for what the consequences could be if

86. *Id.*

87. *See id.*

88. Harwell, *Gold Mine*, *supra* note 1.

89. Garvie, et al., *The Perpetual Line-Up*, *supra* note 47, at Section V *Findings & Scorecard*.

90. Harwell, *Gold Mine*, *supra* note 1.

91. *Id.*

92. ACLU VT., *supra* note 10.

93. *Id.*

94. *Vermont Governor: DMV Stopped Sharing Info with ICE in '17*, ASSOCIATED PRESS (July 8, 2019), https://apnews.com/01f7d3dbfbe546d18eae2e7ed00015e6.

used in other states. For instance, the ACLU highlighted the disproportionate impact on people of color in its complaint calling for the program's end, noting, "DMV's records indicate that since 2012, searches for African-Americans occurred seven times more frequently, and searches for Hispanics were nearly twelve[] times more frequent, relative to those groups' respective share of Vermont's driving population."[95] Other government agencies recognizing the risks associated with law enforcement's use of this technology have also banned facial recognition software, including the cities of San Francisco and Oakland, California, as well as Somerville, Massachusetts.[96] Notably, these local bans only restrict city departments—including police—from employing the technology, and consequently, do not affect whether state and federal agencies choose to do so with regard to their residents' driver's licenses.[97]

B. *Court Order Required*

The state of Washington passed a law in 2012 stipulating the Department of Licensing could disclose results from its facial recognition matching system only in specific circumstances.[98] These circumstances include by court order, when required by federal law, or when the individual had committed a violation identified in Washington Revised Code § 46.20.0921 (relating to fraudulent and stolen driver's licenses) and a hearing examiner confirmed the violation.[99] Despite being identified as a state which gave access to ICE in the Georgetown study released in summer 2019, a Washington State Department of Licensing representative said the agency does not provide data "to any law enforcement entity for immigration purposes or without a judicial court order or subpoena."[100] In a separate interview, a spokesperson acknowledged the Washington State Department of Licensing complied with immigration-related requests until its policy

95. ACLU VT., *supra* note 10.

96. Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRON. (July 17, 2019), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

97. *See id.*

98. WASH. REV. CODE § 46.20.037 (2020).

99. *Id.* §§ 46.20.037, 46.20.0921.

100. Jason Pagano & Gil Aegerter, *ICE Used Washington Drivers Licenses to Hunt Immigrants, Researchers Say*, KUOW (July 8, 2019), https://www.kuow.org/stories/ice-uses-washington-drivers-licenses-to-hunt-immigrants-for-deportation-researchers-say [https://perma.cc/JK67-6S9Q].

changed in 2018.[101] In January 2018, Washington Governor Jay Inslee ordered the Department of Licensing to only release information to ICE under court order.[102]

C. *No Legislative Directives*

Most state legislatures have been silent when it comes to the circumstances necessary to justify sharing driver's license information with federal agencies. Despite being the third state identified by the Georgetown study for complying with ICE requests, Utah officials have claimed the state did not comply with ICE requests for facial recognition scans except for criminal suspects.[103] A spokesperson for the Utah Department of Public Safety indicated database searches are conducted on a case-by-case basis for criminal suspects—both citizens and noncitizens—at the request of outside agencies, including ICE.[104] However, no blanket authority to search databases is granted to federal agencies.[105] Similarly, Illinois claims it turns down ICE requests that are not for a criminal suspect but points to no policy enforcing this practice.[106]

VI. RECOMMENDATIONS FOR LEGISLATIVE AND AGENCY CHANGE

The federal government—either through executive order or congressional action—should adopt a moratorium on the use of driver's license databases for facial recognition scanning by government agencies, at least until certain procedural safeguards can be put in place. These safeguards should, at a minimum, include establishing accuracy standards, requiring a court order, and providing public notice of any government intent to use and share driver's licenses for facial recognition purposes.

101. Esmy Jimenez, *Washington Licensing Says It Hasn't Shared Info with ICE Since 2018*, KUOW (July 9, 2019), https://www.kuow.org/stories/wa-said-it-doesnt-share-residents-info-with-ICE [https://perma.cc/MF4W-R9LP].

102. Pagano & Aegerter, *supra* note 100.

103. Davidson, *supra* note 2.

104. *Id.*

105. *Id.*

106. Ally Marotti, *ICE Used Facial Recognition to Scan Driver's License Photos in Some States. Illinois Says It Has Turned Down ICE Requests*, CHI. TRIB. (July 9, 2019), https://www.chicagotribune.com/business/ct-biz-ice-facial-recognition-drivers-license-photos-20190708-ijsj2yealvdo3ftjjughzetwsq-story.html.

A. *Establish Accuracy Standards*

In light of the serious concerns regarding the potential for false matches, accuracy standards should be adopted prior to the continued use of facial recognition technology on driver's license photographs by any government agency.[107] Even motor vehicle departments need to ensure fraud detection methods are achieving appropriate levels of accuracy before causing residents unnecessary strife should their photograph mistakenly flag a second identity when attempting to obtain a driver's license.[108]

These accuracy standards should also include rules regarding photographic inputs entered for facial recognition scanning. Bans should be instituted on agency use of composite sketches, computer-generated facial features, and celebrity doppelgängers.[109]

B. *Require a Court Order*

The U.S. Congress should adopt legislation similar to that introduced in the House of Representatives in July 2019 by New York Congressman Eliot Engel and co-sponsored by seven other Democratic representatives.[110] This bill prohibits federal agencies from using facial recognition technology on any photograph in the government's possession—including photographic identification issued by a state or the federal government—without a federal court order determining there is probable cause to apply the technology.[111] While this federal bill appears stuck in the House Committee on Oversight and Reform,[112] Senators Jeff Merkley (D-Or.) and Cory Booker (D-N.J.) introduced a bill in February 2020 that could bridge the gap until Congress passes more substantive regulations.[113] The Senators' bill places a moratorium on the federal government's use of facial recognition technology "until a Commission recommends the appropriate guidelines and limitation for use of facial recognition technology."[114]

107. *See, e.g.*, Singer, *supra* note 67.

108. *See, e.g.*, Hill, *supra* note 63.

109. *See* Garvie, *Garbage In*, *supra* note 72 (explaining the non-existence of limitations on the input of photographs to be compared in facial recognition software).

110. *See* FACE Protection Act of 2019, H.R. 4021, 116th Cong.

111. *Id.*

112. *See id.*

113. Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020).

114. *Id.*

Because of this technology's scope and the layers of authority involved, similar measures should be instituted at the state level. State legislatures should adopt legislation requiring court orders or subpoenas in order for other government agencies—including local police officers and federal agencies—to obtain driver's license data for facial recognition purposes. This safeguard should follow the model employed by the state of Washington in requiring a court order to access this information—effectively precluding its access for immigration purposes when no crime is involved.[115] An effort is underway to adopt similar legislation on a state level in Maryland, where lawmakers were considering a measure in February 2020 to require ICE to obtain a warrant before accessing the state database containing motor vehicle records and driver's license photographs.[116] Unfortunately, the potential for retaliatory action by DHS has hindered support for the bill.[117] The state of New York enacted the so-called "Green Light Law" in February 2020, which allows undocumented immigrants to obtain driver's licenses and requires ICE and Customs and Border Protection (CBP) to obtain a court order prior to accessing its motor vehicle database.[118] However, DHS responded by citing the law as reason for its temporary barring of New Yorkers from enrolling in Global Entry and other programs aimed at getting travelers through borders and airport lines more quickly.[119]

C. *Provide Notice: Knowledge Is Power*

An uninformed public cannot be expected to hold elected officials accountable and voice support or dissatisfaction for these evolving—largely unchecked—practices. Even as technology continues to develop rapidly, assumptions cannot be made about the public's approval and trust of various government agencies sharing databases and employing facial recognition technology.[120] The federal DPPA language authorizing the sharing of

115. *See* WASH. REV. CODE § 46.20.037 (2020); Kevin Rector, *ICE Has Access to Maryland Driver's License Records: State Lawmakers Want to Limit It*, BALT. SUN (Feb. 26, 2020), https://www.baltimoresun.com/politics/bs-md-pol-ice-mva-bill-20200227-rsgqqajmwne4hollsz4svgpa6m-story.html (noting that "[b]eing in the country without proper documentation is a civil offense, not a crime").

116. Rector, *supra* note 115.

117. *Id.*

118. *Id.*

119. *Id.*

120. *See* Harwell, *Gold Mine*, *supra* note 1. As Ohio Representative Jim Jordan, the House Oversight Committee's ranking Republican, commented during a hearing on the technology, "No individual signed off on that when they renewed their driver's license,

personal data for "any government function" should not be used as a shield to expect the public to trust agencies are engaged in appropriate functions.[121] Similar to the stringent regulations being adopted globally for commercial businesses to inform consumers of their collection, use, and sharing of private data,[122] U.S. law enforcement agencies should be responsible for sharing their practices with the public as well.[123] Watchdog groups should, likewise, not be forced to bring lawsuits to compel government agencies to comply with FOIA requests inquiring about facial recognition practices.[124] Hiding behind the cloak of "government functions" in the DPPA and claiming "law enforcement sensitivities" to avoid disclosing how this technology is employed should be unacceptable to the taxpaying public.[125]

One response states could take would be to compile an in-depth analysis of facial recognition technology and share it with the public. The state of Ohio took this step in response to the explosive reporting last summer about ICE access to driver's licenses and subsequently produced a

got their driver's licenses. They didn't sign any waiver saying, 'Oh, it's okay to turn my information, my photo, over to the FBI.' No elected officials voted for that to happen." *Id.*

121. *See* 18 U.S.C. § 2721.

122. *See California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST., https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf [https://perma.cc/J2H7-9NN5] (explaining the California-specific legislation effective January 1, 2020, which provides consumers with the rights to know, delete, opt out, and enjoy non-discrimination based on their personal data); Aarti Shahani, *3 Things You Should Know About Europe's Sweeping New Data Privacy Law*, NPR (May 14, 2018), https://www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law (explaining the expansion of consumer rights over personal data under the European Union's General Data Protection Regulation).

123. Garvie, et al., *The Perpetual Line-Up*, *supra* note 47, at Section VI *Recommendations* ("Face recognition is too powerful to be secret. Any law enforcement agency using face recognition should be required to annually and publicly disclose information directly comparable to that required by the Wiretap Act.").

124. *See* Telford, *supra* note 8; Harwell, *ACLU Sues*, *supra* note 8.

125. *See* Owen Daugherty, *FBI, ICE Using State Driver's License Photos Without Consent for Facial Recognition Searches: Report*, THE HILL (July 7, 2019), https://thehill.com/policy/technology/451913-fbi-ice-using-state-drivers-license-photos-without-consent-to-create-facial ("'Due to law-enforcement sensitivities, ICE will not comment on investigative techniques, tactics or tools,' ICE said in a statement to The Hill.").

report detailing the state's use of this technology.[126] All jurisdictions employing facial recognition technology should adopt a similar approach—not only to enable a more informed debate on the issue—but because consent of the governed does not bestow an invisible cloak upon government agencies.[127] Transparency is essential for "We the People" to hold government accountable.[128]

VII. CONCLUSION

While U.S. law enforcement's use of facial recognition technology may not be as problematic as China's use of this technology to track Uighur Muslims, not having yet reached the outer bounds of the extreme does not justify continued unchecked use.[129] Careful consideration should be given to what safeguards are necessary to protect civil rights. For this reason, United Nations Special Rapporteur on freedom of opinion and expression, David Kaye, has called for "an immediate moratorium on the sale, transfer and use of surveillance technology [including facial recognition technology] until human rights-compliant regulatory frameworks are in place."[130] According to former House Oversight Committee Chairman Elijah E. Cummings' statement to *The Washington Post*, "'Law enforcement's access of state databases,' particularly DMV databases, is 'often done in the shadows with no consent.'"[131] It is imperative that the United States take a stance to bring

126. *Facial Recognition Inquires: A Special Report*, ATT'Y GEN. OHIO, https://www.ohioattorneygeneral.gov/FacialRecognitionInquiriesReport [https://perma.cc/8XR2-ZPMB].

127. *See* Robert Moore, *The Consent of the Governed Requires Transparency*, DENVER POST (July 18, 2008), https://www.denverpost.com/2008/07/18/the-consent-of-the-governed-requires-transparency/.

128. *See id.*

129. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html?auth=forgot-password&referring_pv_id=GQY2bxZyp76-3g4YQqsadSJT (detailing what is believed to be the first example of a government using facial recognition for racial profiling).

130. *UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools*, OFF. U.N. HIGH COMM'R HUM. RTS. (June 25, 2019), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736 [https://perma.cc/D8J6-VGNV].

131. Harwell, *Gold Mine*, *supra* note 1.

this practice out of the shadows in order for the public to be informed and decide if they want to voice concerns to their lawmakers or vote people out of office for disagreements with this practice.

*Mariah M. Kauder**

* Mariah M. Kauder is a 2021 J.D. Candidate at Drake University Law School. She received her Bachelor of Arts degree in Rhetoric, Media & Social Change from Drake University in 2016.