Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

IP Theory

Volume 10 | Issue 1 Article 2

Winter 2021

Saving Face; The Unconstitutional Use of Facial Recognition on Undocumented Immigrants and Solutions in IP

Audrey Knutson
audknuts@indiana.edu

Saving Face; The Unconstitutional Use of Facial Recognition on Undocumented Immigrants and Solutions in IP

Audrey Knutson

"As a general rule, it is not a crime for a removable alien to remain in the United States."
J. Kennedy, majority opinion in a 5-3 Decision

Arizona v. United States[1]

INTRODUCTION

Personal data is usually protected by privacy laws. The well-known Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA), and California Consumer Privacy Act (CCPA) are all founded on the presumption that an individual has the right to be left alone. Also, Justice Harlan famously asserted in *Katz v. United States* that the Fourth Amendment protects one's expectation of privacy.[2] Most Americans have these rights and protections, but not everyone in America does. There is a population within the United States that does not have the right of privacy—who does not have the right to be left alone, and who is not even afforded the basic privacy protections of the Fourth Amendment. Is there a way to protect these vulnerable individuals when the right to privacy is stripped away and the Fourth Amendment is inapplicable?

Undocumented immigrants have limited Constitutional and privacy rights, so their personal data has a high probability of use and abuse. The Department of Homeland Security ("DHS") and Immigration and Customs Enforcement ("ICE") are using facial recognition software to identify, target, track, and locate undocumented immigrants. This violates the right to be free from unreasonable searches, due process, and uses race as a primary means of discrimination. Yet these rights are not enforced or protected through the courts. Because of the dangers of using facial recognition and because facial image data cannot be protected through privacy avenues, one solution is to protect it with intellectual property law. The harms suffered by undocumented immigrants mandate protections and remedies that exist outside of courts. Although not a perfect fit, intellectual property law can be adjusted and revised to grant an individual property rights in his or her own facial templates to provide undocumented immigrants greater protection over their civil liberties than is currently afforded them by the Constitution, Supreme Court, and other federal legislation.

Part I states modern immigration policies and provides context for the reasoning and concerns surrounding facial recognition software and undocumented immigrants. Part II details the judicial problems in place for excluding the fruits of facial recognition in immigration deportation hearings and why undocumented immigrants are especially vulnerable because they are without Constitutional protections. It also analyzes how immigration has evolved and now requires new civil rights protections beyond the exclusionary rule. Finally, Part IV explores civil rights laws for undocumented immigrants within an intellectual property law framework and analyzes the feasibility, strengths, and weaknesses.

I. HOW FACIAL RECOGNITION WORKS

Facial recognition requires a camera to capture an image, an algorithm to create a "faceprint" or "facial template," a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database.[3] Facial recognition is non-intrusive, like

[1] 567 U.S. 387, 407 (2012).

[2] 389 U.S. 347, 360 (1967).

[3] Rosie Brinckerhoff, *Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray into Facial Recognition Technology from Haunting Consumer Privacy Rights Forever*, 70 Fed. Comm. L.J. 105, 112 (2018).

voice recognition, and unlike DNA testing. Of course, inaccuracies occur when images are incorrectly matched—the wrong person is identified. This can be caused by variations in external conditions such as lighting and the user's position and distance from the camera, as well as variations caused by facial expressions, aging and make-up[4] or more dubious problems with the software and its application, which will be explored in Part III.

II. HOW THE POLICE AND ICE ARE USING FACIAL RECOGNITION DATA

President Trump was elected under a strong anti-immigration policy. He has strived to regulate undocumented immigration, both through controlling future immigration through Mexico with a boarder wall as well as decrease the current amount of 11 million undocumented immigrants through deportation.[5] Removing these undocumented immigrants from the United States was a cornerstone of Trump's initial appeal to conservatives in the Republican Party, and also one of his most ambitious and potentially expensive policies.[6] He cited national safety as the reason behind these changes and even went so far as to say "Within ICE I am going to create a new special deportation task force focused on identifying and quickly removing the most dangerous criminal illegal immigrants in America who have evaded justice."[7]

Immigration falls under the executive branch of the DHS and its law enforcement agency, ICE. During the Trump administration's first fourteen months, there were 58,010 arrests by ICE of people without criminal convictions, which was three times as many as during the preceding fourteen months.[8] The administration has expanded the reach of interior enforcement, reduced refugee admissions dramatically, and slowed visa processing times, with a modest but noticeable effect on the number of people admitted in some visa categories.[9] On July 23, 2019, expedited removal proceedings were expanded to be applied to all undocumented immigrants who have been in the country for less than 2 years.[10] The change dramatically expands the ability of DHS to quickly deport certain immigrants without any of the due-process protections granted to most other people, including the right to an attorney and to a hearing before a judge.[11] No administration in modern U.S. history has placed such a high priority on immigration policy or had an almost exclusive focus on restricting immigration flows, legal and unauthorized alike.[12] ICE's emphasis on removal, expansion of power, and change in expedited removal proceedings demonstrate how today ICE is under increasing pressure and specific directives to locate and expel as many undocumented immigrants as possible.[13]

There are 10.5-11 million undocumented immigrants living in the United States, according to the Pew Research Center, but there are only about 6,100 officers in ICE's Enforcement and Removal

[4] Michael Yang & Francis J. Gorman, *What's Yours Is Mine Protection and Security in A Digital World*, Md. B.J. 24, 27 (2003).

[5] *See* Nick Corasaniti, *A Look at Trump's Immigration Plan, Then and Now,* N.Y. TIMES (Aug. 31, 2016), https://www.nytimes.com/interactive/2016/08/31/us/politics/donald-trump-immigration-changes.html [https://perma.cc/U8Q2-FRVZ].

[6] SARAH PIERCE, JESSICA BOLTER, & ANDREW SELEE, MIGRATION POLICY INST., *U.S. IMMIGRATION POLICY UNDER TRUMP: DEEP CHANGES AND LASTING IMPACTS* 15 (2018), https://www.migrationpolicy.org/research/us-immigration-policy-trump-deep-changes-impacts [https://perma.cc/H2TU-YKLB].

[7] *Transcript of Donald Trump's Immigration Speech,* N.Y. TIMES (Sept. 1, 2016), https://www.nytimes.com/2016/09/02/us/politics/transcript-trump-immigration-speech.html [https://perma.cc/U62N-5VFY].

[8] McKenzie Funk, *How ICE Picks Its Target in the Surveillance Age,* N.Y. TIMES (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/3CQJ-6HF2].

[9] *See* Yang & Gorman, *supra* note 4, at 15.

[10] Vanessa Romo, *Trump Administration Moves to Speed Up Deportations with Expedited Removal Expansion,* NPR (July 22, 2019, 5:20 PM), https://www.npr.org/2019/07/22/744177726/trump-administration-moves-to-speed-up-deportations-with-expedited-removal-expan [https://perma.cc/B428-C8DJ]. Prior to July 23, 2019, undocumented immigrants who cross into the U.S. by land can be deported without an immigration hearing if they are arrested within 100 miles of the border during the first 14 days after their arrival. Those who arrive by sea can be deported without legal proceedings if they are unable to prove they have been living in the U.S. for two years or more. *Id.*

[11] *Id.*

[12] *See* PIERCE ET AL., *supra* note 6, at 15.

[13] *See* Funk, *supra* note 8.

Operations (E.R.O.) division.[14] There are 50 states for ICE to cover, as well as Washington and territories like Puerto Rico, which all amount to more than 3.8 million square miles.[15] There are continuing staffing shortages.[16] To make up for its deficiencies in manpower, ICE looks to efficiencies in technology. Big data, AI, and algorithms allow ICE to do more with less.[17]

DHS and ICE are using social media, real-time cell location data, and artificial intelligence to target and locate undocumented immigrants.[18] However, this paper will examine only facial recognition software. Facial recognition software has huge current and future implications for use in the identification, targeting, tracking, and locating of undocumented immigrants and has been debated every few weeks in 2019 alone. Fourteen states and Washington D.C. and Puerto Rico issue drivers licenses to undocumented immigrants.[19] At least three of those states—Utah, Washington, and Vermont—are verified as having their DMVs actively working with ICE to run facial recognition software through their database of driver's license photos.[20] Over two dozen states allow law enforcement officials to request such searches against their databases of driver's licenses.[21] In addition to the voluntary offer of photo databases, ICE issued subpoenas, without probable cause, to gain access to these databases,[22] though many requests for searches involved nothing more than an email to a DMV official with the target's "probe photo" attached.[23] Warrants are not even required. ICE officials have mined state driver's license databases using facial recognition technology, analyzing millions of motorists' photos without their knowledge.[24]

Using facial recognition, ICE obtains personal information from DMV databases. This can be a home address, license plate number, or also more intimate details like place of birth or whether a foreign passport was used to prove identity.[25] ICE can use this information to decide whom to target for immigration enforcement and to locate the people it's targeted.[26] They can also use the DMV databases to locate specific individuals and the primary government database ICE relies upon is the driver license database.[27] According to the U.S. Government Accountability Office, ICE agents consider the data in DMV records, among others, to be more current and reliable than the DHS address database.[28]

The problem with using facial recognition software to mine the data in DMVs is the lack of governing authority. ICE admits that no federal policy governs ICE access to or use of DMV data.[29] Neither Congress nor state legislatures have authorized the development of such a system.[30] For the time being, no

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *See id.*
[18] *See id.*
[19] *State Laws Providing Access to Driver's Licenses or Cards, Regardless of Immigration Status*, NAT'L IMMIGRATION LAW CTR. (April 2020), https://www.nilc.org/wp-content/uploads/2015/11/drivers-license-access-table.pdf [https://perma.cc/D8AK-S29Y].
[20] *See* Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Database*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/5DWV-7SQU].
[21] *See id.*
[22] *Id.*
[23] 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/ [https://perma.cc/VF6S-FB5L].
[24] *See* Edmondson, *supra* note 20.
[25] *See* Funk, *supra* note 8.
[26] Joan Friedland, *How ICE Uses Databases and Information-Sharing to Deport Immigrants*, NAT'L IMMIGR. L. CTR. (Jan. 25, 2018), https://www.nilc.org/2018/01/25/how-ice-uses-databases-and-information-sharing-to-deport-immigrants/ [https://perma.cc/PAY5-BPG8].
[27] *DOCUMENTS OBTAINED UNDER FREEDOM OF INFORMATION ACT*
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/8LKG-QME7].
[28] *Id.* (citing *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/products/GAO-05-204 [https://perma.cc/BW3N-3ZWU]).
[29] *Id.*
[30] *See* Harwell, *supra* note 23.

one is telling ICE they can access DMV databases but also, no one is telling them they cannot. Facial recognition is rapidly advancing technology with very few guidelines and protections in place.[31]

Tech giant Amazon has also jumped in to help locate and track undocumented immigrants. Their Ring Doorbell is a video doorbell, which allows uses to see and talk to people who come to the door. It also records these visitors and the data is stored on Amazon's cloud. Ring is currently partnered with more than 400 police departments across America.[32] These partnerships streamline how Ring video data can be accessed by police, even without warrants.[33] Currently, Ring does not use facial recognition software but has filed a patent in December 2018 to pair the two technologies. The application describes a system that the police can use to match the faces of people walking by a doorbell camera with a photo database.[34] If a match occurs, the person's face can be automatically sent to law enforcement, and the police could arrive in minutes.[35] It is not a far leap to assume ICE can also access Ring video data with Ring facial recognition software or their own.

Furthermore, Amazon has pitched another facial recognition tool, Rekognition, to law enforcement agencies, including ICE, to target and identify undocumented immigrants.[36] Rekognition has the ability to identify people from afar, a type of technology immigration officials have voiced interest in for its potential enforcement use on the southern border.[37] Amazon unveiled Rekognition as a way to analyze images and detect faces on a massive scale.[38]

III. RELEVANT CASE LAW

The Fourth Amendment protects Americans from unreasonable searches and seizures and requires federal law enforcement to procure warrants with underlying probably cause to be able to obtain information for investigations. In order for a Fourth Amendment violation to occur, a "search" or a "seizure" must transpire.[39] In *Katz v. United States*, the Supreme Court defined a search as any government action that violates an individual's reasonable expectation of privacy.[40] The Fourth Amendment protects people's privacy and law enforcement must respect it.

If the Fourth Amendment is violated, the evidence obtained through that unconstitutional search and seizure is inadmissible in court.[41] A motion to suppress is used to prohibit evidence that has been unlawfully obtained by the government.[42] "[A] successful motion to suppress . . . lead[s] to the exclusion of various forms of evidence."[43] This is called the "exclusionary rule" and it is a judicially instituted remedy that penalizes past law enforcement misconduct and deters the same conduct in the future.[44] It "weighs the

[31] *Id.*
[32] Rani Molla, *How Amazon's Ring is creating a surveillance network with video doorbells*, VOX (Sept. 24, 2019), https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell [https://perma.cc/3RKA-ZKET].
[33] Colin Lecher, *Amazon's Ring reportedly partners with more than 200 US Police Departments*, THE VERGE (July 29, 2019), https://www.theverge.com/2019/7/29/20746156/amazons-ring-law-enforcement-partnerships [https://perma.cc/5SAT-93TV].
[34] Jacob Snow, *Amazon's Disturbing Plan to Add Face Surveillance to your Front Door*, ACLU (Dec. 12, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-yo-0 [https://perma.cc/5LZE-DT89].
[35] *Id.*
[36] Drew Harwell, *Amazon met with ICE officials over facial recognition system that could identify immigrants*, WASH. POST (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/ [https://perma.cc/Q984-GWJC].
[37] *Id.*
[38] *Id.*
[39] Stephanie Groff, *Where to Draw the Line: The Egregiousness Standard in the Application of the Fourth Amendment in Immigration Proceedings and the Racial Profiling Exception*, 26 GEO. MASON U. CIV. RTS. L.J. 87, 92 (2015).
[40] *Id. See also Katz*, 389 U.S. at 361.
[41] *See* Weeks v. United States, 232 U.S. 383, 394 (1914) (applying the rule only to Federal officials); Mapp v. Ohio, 367 U.S. 643, 655 (1961) (applying the rule to state officials as well).
[42] *See* Groff, *supra* note 39, at 91.
[43] *Id.* at 91–92.
[44] Mapp v. Ohio, 367 U.S. 643, 680 (1961).

cost of excluding evidence against the benefit of deterring future governmental misconduct."[45] The Fourth Amendment is based on the principle of an individual's right to being secure in an investigation and that they investigation is fair. The exclusionary rule is an "essential ingredient" of the Fourth Amendment as the right it embodies is vouchsafed by the Due Process Clause of the Fifth and Fourteenth Amendment.[46]

Immigration removal proceedings are an administrative process governed by guidelines and rules under both the Immigration and Nationality Act (INA) and Title 8 of the Code of Federal Regulations: Aliens and Nationality.[47] As civil actions, removal proceedings differ from criminal proceedings, but certain constitutional due process protections are nevertheless afforded to aliens,[48] such as the right to have a hearing presided by a judge, the right to present testimony and evidence, the right to be represented by counsel, and can seek appeals through the Board of Immigration Appeals ("BIA").[49] After the BIA, a further appeal may also be sought in a federal court of appeals. An Immigration Judge may remove an alien for any of the reasons in 8 U.S.C.A. § 1227(a), including illegal presence, disregarding a condition of entry, committing a crime of moral turpitude, failing to register under the Alien Registration Act, or falsifying documents.[50] Before the *Lopez-Mendoza* case was brought to court, most practitioners and courts agreed that the exclusionary rule applied to deportation proceedings.[51]

In 1984, *INS v. Lopez-Mendoza* completely changed the way the Fourth Amendment was applied to deportation hearings. The Ninth Circuit held that Immigration and Naturalization Service ("INS") agents ,the precursor to ICE, violated Adan Lopez-Mendoza's Fourth Amendment rights, and the rights of another similarly situated plaintiff, Elias Sandoval-Sanchez, in the course of their immigration arrests, and therefore any evidence that the agents had gathered as a result of those unconstitutional arrests should be excluded from proceedings in accordance with the exclusionary rule.[52] The Supreme Court granted *certiorari*.

In a plurality opinion written by Justice O'Connor, the Court held that the exclusionary rule "need not apply" in a deportation hearing[53] because there are purely civil and not criminal hearings.[54] Furthermore, she emphasizes that "[t]he 'body' or identity of a defendant or respondent in a criminal or civil proceeding is never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred."[55] To arrive at her holding, she balances the Fourth's deterrent effect on future law enforcement misconduct against the loss of probative evidence.[56] Ultimately, she decides the exclusionary rule is not needed to deter future misconduct because there are other safeguards in place.

First, deportation is possible even without evidence from an investigation because the sole, material issue in deportation proceedings is the respondent's identity and alienage.[57] Other evidence can be gathered to support the government's position on alienage. Also, O'Connor again makes it clear that the person and identity of the respondent is *not* suppressible.[58] Second, she cites that INS makes few arrests during a year (only 500 in 1983!) and very few "challenge the circumstances of their arrests."[59] Third, and in her eyes the most important, are the INS' own internal standard operating procedures to ensure its own officers are

[45] Groff, *supra* note 39, at 92.
[46] Mapp, 367 U.S. at 651.
[47] Groff, *supra* note 39, at 91.
[48] *Id.*
[49] *See* Katie Benner & Charlie Savage, *Due Process for Undocumented Immigrants, Explained*, N.Y. TIMES (June 25, 2018), https://www.nytimes.com/2018/06/25/us/politics/due-process-undocumented-immigrants.html [https://perma.cc/M48T-B45N].
[50] Matthew S. Mulqueen, *Rethinking the Role of the Exclusionary Rule in Removal Proceedings*, 82 ST. JOHN'S L. REV. 1157, 1164 (2008).
[51] *Id.* at 1165.
[52] Stella Burch Elias, *"Good Reason to Believe": Widespread Constitutional Violations in the Course of Immigration Enforcement and the Case for Revisiting Lopez-Mendoza*, 2008 WIS. L. REV. 1109, 1110 (2008).
[53] I.N.S. v. Lopez-Mendoza, 468 U.S. 1032, 1034 (1984).
[54] *Id.* at 1038.
[55] *Id.* at 1039.
[56] *See id.* at 1042.
[57] *Id.* at 1043.
[58] *Id.*
[59] *Id.* at 1044.

following the Fourth Amendment during investigations and arrests.[60] Finally, O'Connor cites other remedies available to respondents such as declaratory relief[61] and declares that the Court would not deal "with egregious violations of the Fourth Amendment or other liberties that might transgress notions of fundamental fairness and undermine the probative value of the evidence obtained."[62]

In the three and a half decades since *Lopez-Mendoza*, the policies and practices of immigration enforcement agencies have changed radically.[63] Pretextual traffic stops, warrantless home invasions, illegal workplace seizures, unnecessary force, US citizen children detained by armed officers, individuals stopped and questioned without any reasonable suspicion and detained without probable cause, have all become increasingly frequent and commonplace.[64] As mentioned above, INS made only 500 immigration arrests in 1983.[65] That number has increased dramatically and according to the U.S. Department of Justice Executive Office for Immigration Review (EOIR), since 2000, immigration-related cases account for the largest single category of federal prosecutions, and account for about half of all federal hearings.[66] EOIR records show that between 1952 and 1979 (the year that the Lopez-Mendoza respondents Adan Lopez-Mendoza and Elias Sandoval-Sanchez first appeared in immigration court) fewer than fifty motions to suppress evidence or terminate proceedings had ever been filed in immigration court.[67] In 2018 alone, 22,189 motions to terminate were granted.[68] O'Connor's "statistical safeguard"—the low numbers of immigrations arrests and challenges has dramatically increased and safeguards must also increase in 2019.

Lopez- Mendoza hinged mainly on the argument that deportations are civil proceedings and not criminal and therefore the balance tips in favor of procuring probative evidence rather than the protection of individual liberties. However, now the boundary line between civil and criminal immigration proceedings has been blurred. "Crimmigration" is a term. INS has been replaced by ICE, which combines the investigative and intelligence arms of INS as well as the "resources, responsibilities and authorities" of the Federal Protective Service, is DHS's largest investigatory unit.[69] There are new immigration-related crimes, increases in the minimum and maximum sentences for existing immigration crimes, increases in the fines imposed on immigrant defendants, and far greater numbers of prosecutions being brought for the commission of all immigration-related crimes.[70] Professor Stella Birch Elias notes,

> [W]hile the immigration-law system has adopted many of the punitive attributes of the criminal-law system, such as harsher sentences, higher fines, and greater numbers of federal prosecutions, it has failed to adopt the procedural checks and balances that protect criminal defendants from arbitrary or unconstitutional applications of the law.[71]

Facial recognition software is already heavily employed by the FBI, NSA, TSA, CIA, state police, and other federal and state agencies for law enforcement purposes. Most of the time, an undocumented immigrants only crime is being present in the United States[72], yet the same technology and investigative tools are being used on them as violent criminals and terrorists. Undocumented immigrants are subject to detention and deportation—deprivations of both liberty and property--without due process safeguards

[60] *Id.*
[61] *Id.* at 1045.
[62] *Id.* at 1050–51.
[63] Elias, *supra* note 52, at 1124.
[64] *Id.* at 1131-33.
[65] *Lopez-Mendoza*, 468 U.S. at 1044.
[66] *See* EXECUTIVE OFFICE FOR IMMIGRATION REVIEW, U.S. DEP'T OF JUSTICE, *STATISTICS YEARBOOK FISCAL YEAR 2018* (2018), https://www.justice.gov/eoir/file/1198896/download [https://perma.cc/D4BT-D4JG].
[67] *See* Mulqueen, *supra* note 50, at 1126–27.
[68] *See* U.S. DEP'T OF JUSTICE, *supra* note 66 fig.7.
[69] *See* Mulqueen, *supra* note 50, at 1174.
[70] *See* Elias, *supra* note 52, at 1142.
[71] *Id.* at 1143.
[72] Immigration and Nationality Act § 275, 8 U.S.C. § 1325 (2018), which criminalizes unlawful entry into the United States and became a federal crime in 1929. Unlawful entry includes any non-citizen who enters or who attempts to enter the United States.

afforded said violent criminals and terrorists. *Lopez-Mendoza* emphasizes the civil nature of deportation hearings, yet undocumented immigrants are increasingly being investigated and tried as criminals. Yet there are no safeguards in place to ensure their Fourth Amendment rights are protected.

DHS and ICE internal standard operating procedures are no longer a safeguard to law enforcement misconduct. Regulations prohibit DHS and ICE agents from using unreasonable and disproportionate force during the interrogation, arrest, and detention of a suspect.[73] Yet a number of complaints have been filed alleging ICE agents and law-enforcement officers used unreasonable and disproportionate force during the interrogation, arrest, and detention of civil immigration suspects.[74] Regulations state that individuals may not be detained and subjected to custodial interrogation in the absence of reasonable suspicion that they have committed an immigration violation.[75] Yet there have been complaints filed that allege they were detained by immigration officers who could not have had any reasonable suspicion to believe that they had committed immigration infractions.[76] Regulations specify that ICE officers may not enter residential premises without either a judicially approved search warrant or consent by the occupants of the premises.[77] Yet, in many recent cases, immigration respondents have filed motions to suppress evidence obtained during illegal, warrantless, and nonconsensual searches of their homes.[78]

Specifically with facial recognition, there is no internal (or external for the matter) procedure to govern its use by ICE in DMVs or elsewhere.[79] ICE can theoretically expand its facial recognition software to other state and federal agency databases such as security camera footage or perhaps they could release squadrons of drones into US airspace that are equipped with real-time facial recognition technology or could install cameras in hospitals, street corners, and schools. Those are not ridiculous leaps and conclusions if law enforcement is already using doorbells to locate undocumented immigrants. Where is the line? There are no regulations, no standards of reasonable suspicion, probable causes, or "hunches." Facial recognition is founded on being able to conduct suspicionless searches. There are no detectable safeguards in place to ensure that DHS and ICE agents are adhering to the Constitutional standards and case law associated with the Fourth Amendment. This is akin to the wild west where anything goes and until other safeguards are developed, martial law rules supreme.

Without the Fourth Amendment protection from government misconduct, there are few forms of relief available for undocumented immigrants. O'Connor cited another safeguard in *Lopez*-Mendoza, remedies available to respondents such as declaratory relief.[80] However, Justice White wrote in his dissent, "[t]he suggestion that alternative remedies, such as civil suits, provide adequate protection is unrealistic."[81] Few challenge the constitutionality of these searches and due process violations because they are no longer in the country and/or are scared and mistrustful of US law enforcement and the justice system. Many times, respondents return to situations of extreme poverty and violence and taking the time and effort to pursue civil suits are unreasonable. The victims of these violations are powerless.

Moreover, since 1984, statutory provisions and case law have eroded almost all of the options for meaningful judicial review that were once available to immigration respondents whose constitutional rights have been violated.[82] The 1996 amendments to the Immigration and Naturalization Act limited judicial review of removal proceedings, leaving the petition-for-review process as the primary opportunity for recourse.[83] Another safeguard against law enforcement misconduct is a *Bivens* Action,[84] which allows

[73] 8 C.F.R. § 287.8(a)(iii) (2020).
[74] *See* Elias, *supra* note 52, at 1147.
[75] 8 C.F.R. § 287.8(b)(1) (2020).
[76] *See* Elias, *supra* note 52, at 1147.
[77] 8 C.F.R. § 287.8(f)(2) (2020).
[78] *See* Lindsay Kee, *"We Don't Need a Warrant, We're ICE"*, ACLU (Oct. 21, 2011, 5:46 PM), https://www.aclu.org/blog/we-dont-need-warrant-were-ice [https://perma.cc/U9RP-V5DN].
[79] *See* National Immigration Law Center, *supra* note 27.
[80] *See* Elias, *supra* note 52.
[81] INS v. Lopez-Mendoza, 468 U.S. 1032, 1055 (1984) (White, J., dissenting).
[82] *See* Elias, *supra* note 52, at 1153.
[83] *Id.*
[84] *See* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971).

victims of Fourth Amendment violations by federal officers acting in the color of federal authority to bring a sit for damages. In 2008, the Bush administration decided that I.N.A. § 242 prevents immigration respondents from bringing *Bivens* claims for damages.[85] Respondents only had limited opportunities for relief in 1984 and those options have since dwindled.

Most importantly, reliance on remedies is insufficient because both the DHS, who need deterrence, and the political forces that dictate policy can prevent the plans from being put into place or can turn safeguards into mere paper procedures.[86] This concern is particularly apparent in immigration enforcement because aliens are disconnected from the political process.[87] Those targeted by immigration agents or police officers enforcing immigration laws are vulnerable and socially marginalized, and therefore highly unlikely to turn to the legal system to seek recompense for any wrongs they have suffered.[88] As a result, constitutional violations by law-enforcement officers have spread throughout the nation, growing rapidly in the last two years and crossing geographical and institutional boundaries with increasing frequency.[89]

This really drives the point home that there are not many viable options to fix Fourth Amendment violations of unreasonable searches in facial recognition. Since there is no check on the Constitutionality of these searches, there is little pressure that they will need to be conducted with warrants with probable cause or even reasonable suspicion. Also, facial recognition can be easily and quickly run through databases, making them an effective "sweep" for evidence of suspected unlawful entry. *Chandler v. Miller* commands that to be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.[90] Without even an inkling of individualized suspicion the employment of facial recognition software becomes nothing more than big brother watching.

Immigration searches and seizures that are based solely or mostly on racial profiling should presumptively constitute "egregious" Fourth Amendment violations because they are unconstitutional under the equal protection clause of the Fourteenth Amendment. For an immigrant to successfully have evidence deemed inadmissible during his removal proceeding, she has to prove that the manner in which the evidence was seized was "so egregious" that, not only was there a Fourth Amendment violation, but there also was a violation of his right to fundamental fairness and due process of law under the Fifth Amendment.[91] Right now there is not uniformity in how the circuit courts are interpreting "egregious violations" but the Second, Third, and Ninth Circuit have held that an egregious violation may be found if the stop was based on race, nationality, or other grossly improper considerations.[92]

When the person in the photo is a white man, the software is right 99 percent of the time.[93] Researchers and numerous studies argue that's because the software is trained on vast sets of images that skew heavily toward white men, leaving women and minorities vulnerable to holes in mammoth databases.[94] In other words, there are far more white men in databases used to train the A.I. algorithms used in facial recognition so the software is inherently "smarter" and better at identifying white men yet struggles with women and minorities because it has not had as much "practice."

Many believe human error also contributes to facial recognition's inaccuracies. Critics worry that people are not being trained adequately in how to use the technology and interpret its results.[95] Researchers

[85] *See* Elias, *supra* note 52, at 1153.
[86] *See* Mulqueen, *supra* note 50, at 1194–95.
[87] *Id.*
[88] *See* Elias, *supra* note 52 at 1156.
[89] *Id.*
[90] Chandler v. Miller, 520 U.S. 305, 305 (1997).
[91] Chris Modlish, *Immigrant Rights in Jeopardy: A Denial of Constitutional Protection in* De La Paz v. Coy, 57 B.C.L REV. E-SUPPLEMENT 104, 117–18 (2016).
[92] *See* Groff, *supra* note 39, at 89. 117–18.
[93] Steve Lohr, *Facial Recognition is Accurate if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/G82A-3YX4].
[94] Rachel Siegel, *Rashida Tlaib isn't the Only One who Thinks Race Biases Facial Recognition Results,* WASH. POST (Oct 4, 2019), https://www.washingtonpost.com/technology/2019/10/04/rashida-tlaib-isnt-only-one-who-thinks-race-biases-facial-recognition-results/ [https://perma.cc/BKD3-R2QM].
[95] *Id.*

say that law enforcement agencies do not always disclose how its analysts are taught to use the systems, or who is conducting the training and they worry that even if a department claims a strong training protocol, people will inevitably let biases about gender and race creep into how they assess a match.[96] There is not a lot of transparency in both the software and how people are using it, which makes it sound like there is something to hide.

How inaccurate is facial recognition? In 2015, Google had to apologize after its image-recognition photo app initially labeled African Americans as "gorillas."[97] The ACLU used Amazon's Rekognition, the software it has been trying to sell to law enforcement and ICE, and incorrectly matched twenty-eight members of Congress, and identified them as other people who have been arrested for a crime.[98] M.I.T. researchers also reported that Rekognition also had trouble correctly identifying a person's gender.[99] The Congressional Black Caucus specifically expressed concern to Amazon about the "profound negative unintended consequences" face surveillance could have for Black people, undocumented immigrants, and protesters.[100]

Matching a face template with a face then opens the door to problematic issues.

> [O]nce someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the Government buildings you enter, and the photos your friends post online. In fact, a series of experiments conducted at Carnegie Mellon University objectively concluded that "[i]f an individual's face on the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her.[101]

Thus, for undocumented immigrants, a search for facial data is not merely a suspicionless search like it is for American citizens, but the first step in deportation. Facial data is being used to target and locate individuals.

Instead of pinpointing an individual, facial recognition creates a lineup of people. The technology is extremely inaccurate and exponentially more so when the individual is non-white, and non-male. Essentially, facial recognition is operating on racial/ethnic bias and is indistinguishable from discrimination based on race, ethnicity, and national origin. When applied by the federal government, all race-based classifications are subject to strict scrutiny,[102] and are constitutional only if they are narrowly tailored to further compelling governmental interests. Because the government has not been upfront and transparent with its use of facial recognition, it is hard to say whether or not these means really are narrowly tailored.

Caselaw supports not using the results of racial profiling in deportation hearings. In *Gonzalez-Rivera v. INS*, the officer arrested the alien based only on his Hispanic appearance, and the court concluded that this constituted egregious behavior that violated the respondent's Fourth Amendment rights.[103] The Ninth Circuit held, "we have long regarded racial oppression as one of the most serious threats to our notion of fundamental fairness and consider reliance on the use of race or ethnicity as shorthand for likely illegal conduct to be 'repugnant under any circumstances.'"[104] They emphasized:

[96] *Id.*
[97] *See* Lohr, *supra* note 93.
[98] *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots,* ACLU (Jul. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/KK7K-NXFA].
[99] *See* Siegel, *supra* note 94.
[100] *See* Snow, *supra* note 98.
[101] *See* Modlish, *supra* note 91, at 115.
[102] Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 200 (1995).
[103] *See* Groff, *supra* note 39.
[104] Gonzalez-Rivera v. INS, 22 F.3d 1441, 1449 (9th Cir. 1994).

> [F]ederal courts cannot encourage impermissible uses of race, reliance on ethnicity as the sole factor in the creation of a reasonable suspicion . . . [t]he court compared the immigration officers' action to a facial racial classification and concluded that in an equal protection context, it was presumptively invalid.[105]

Racial profiling has not only violated the Fourth Amendment's unreasonable search clause, but also the Fourteenth Amendment's equal protection clause—that requires the government to treat people equally. The history of discriminatory government surveillance makes clear that face surveillance will disproportionately harm people already targeted by the government and subjected to racial profiling and abuse — immigrants, people of color, and the formerly incarcerated.[106] Because facial recognition is less accurate for darker skinned faces and women, these systems threaten to further entangle people with law enforcement, ripping families apart and increasing the likelihood of racially biased police violence.[107] Facial recognition is unconstitutional.

Moreover, facial recognition has also violated the Fifth Amendment's due process clause through possible Brady violations. Suppression of evidence favorable to a defendant violates due process because the evidence is material either to guilt or punishment.[108] Because facial recognition software is inaccurate and either misidentifies individuals or picks multiple possible matches, the software creates information that could exculpate a defendant. Other matches indicate the possibility of other perpetrators. The fact that the analysts of the software are choosing one person from multiple possible people also indicates the possibility of other perpetrators and possible improper suggestiveness. Also, the fact that analysts may not even be properly trained compounds the possibility of error.

Thus, when a face template is run through a database looking for person A, it might choose person B instead. It chooses person B because B is also a person of color. Person B may also be undocumented. There could have been no probable cause, reasonable suspicion, or any suspicion at all. Facial recognition has turned into a fishing expedition that casts a wide net and instead of exonerating some defendants it implicates others. These are severe Constitutional violations violating serious individual rights.

Lopez' reasoning as to why the Fourth Amendment and why undocumented immigrants have no expectation of privacy are not applicable in 2019. There is increasing debate on whether or not to relitigate *Lopez-Mendoza* to reconsider applying the exclusionary rule to deportation hearings. Many critics believe this is the solution. However, as the above analysis shows, an increase in investigative technology and pervasive and diverse constitutional violations have dictated a need for other protections. Also, as emphasized by O'Connor, the body or identity of an immigrant is never suppressible in court. Reinstating the exclusionary rule is not an option.

O'Connor's *Lopez-Mendoza* reasoning does not hold up in 2019 with evidence obtained from facial recognition software because the increasingly criminal nature of immigration and its enforcement, the lack of relief available when constitutional violations occur, and the severe racism and disregard for exculpatory procedures. Much has changed since 1984, but *Lopez-Mendoza* is still the principal case controlling the inclusion or exclusion of evidence in immigration proceedings.[109] It effectively disqualified undocumented immigrants from having the same level of privacy as American citizens.[110] With privacy chipped away and a serious need to fix the civil liberties violations of undocumented immigrants, there is a serious hole needed for protective legislation.

[105] *Id.* at 1449-50.

[106] *See* Snow, *supra* note 34.

[107] *Id.*

[108] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

[109] *See* Mulqueen, *supra* note 50, at 1181-83.

[110] The 2-pronged *Katz* tests extends Fourth Amendment protection to (1) where people have an expectation of privacy (subjective) and (2) society is prepared to accept that expectation (objective). *See supra* note 2. *Lopez-Mendoza* essentially fails undocumented immigrants at both prongs.

IV. POSSIBLE SOLUTIONS

In 2008, Illinois passed the Biometric Information Privacy Act, ("BIPA"), a law protecting the "biometric identifiers and biometric information" of its residents.[111] Two other states, Texas and Washington, also followed and passed their own biometric privacy laws, although not as robust as the one in Illinois, which strictly forbids private entities to collect, capture, purchase or otherwise obtain a person's biometrics — including a scan of their "face geometry" — without that person's consent.[112] Face templates are biometric data, data used to identify specific individuals, and thus using an individual's face and face templates in algorithms is a violation of Illinois law. Violations of BIPA are essentially tort causes of action and individuals can then sue for damages when violations occur.

Of course, legislation like BIPA would need to be strengthened to protect undocumented immigrants. As demonstrated in Parts II and III, they are more vulnerable in regard to their privacy than American citizens and there is more risk for unconstitutional abuses. Furthermore, just like declaratory relief, most undocumented immigrants would not seek damages through civil suits for privacy violations like Illinois citizens can. However, BIPA demonstrates that American is prepared to recognize the rights of self like in face templates and restrictions in using them in identifying algorithms. The principles behind BIPA lay a solid foundation for additional, more robust rights to be created for undocumented immigrants.

Interestingly enough, the Civil Rights Act of 1964, prohibiting discrimination based on race, color, religion, sex, or national origin, was passed under the commerce clause—Congress' power to pass legislation over commercial activity. Among the other plenary powers of Congress is the right to enact legislation concerning intellectual property. Art. I, § 8, cl. 8 grants Congress the enumerated power "[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." A possible solution to protect undocumented immigrants from facial recognition searches is to protect their face templates under the IP power of Congress.

The problem with creating property-like rights for face templates is American law does not recognize these "rights of self." Americans do not actually own their names, social security numbers, or identities and courts have struggled giving property rights to body parts like sperm cells, spleen cells, corneas, etc.[113] Similarly, no one actually owns their fingerprints. However, a face template is not as tangible as body parts and can exist entirely within the digital realm. And unlike fingerprints or body parts, there is a higher probability of abuse of face templates—as evidenced above, racial discrimination in investigations can occur from face template evidence alone. When an investigation yields fingerprints or even DNA, it is not proceeding through discriminatory avenues but rather reliable scientific paths. Facial recognition is too inaccurate to be relied upon and the threat of discrimination is too high. Add in the constitutional concerns of undocumented immigrants, and the necessity to create present possessory interests in face templates becomes of great importance.

Applying a framework of protection under current intellectual property law is also problematic. Companies who create facial recognition software may have it protected under patents or trade secrets, but this protection does not extend to the face templates themselves. Data is not patentable subject matter under 35 U.S.C. § 101,[114] and trade secrecy is not applicable because data should not be surrounded by a cloak of secrecy but rather should be more transparent. A big issue behind ICE using data to target and find undocumented immigrants is the mystery behind their methods and sources and to give individuals more

[111] Kashmir Hill & Aaron Krolik, *How Photos of Your Kids are Powering Surveillance Technology,* N.Y. TIMES(Oct. 11, 2019), https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html [https://perma.cc/9RYR-TJ94].

[112] *Id.*

[113] *See* Moore v. Regents of Univ. of Cal., 51 Cal. 3d 120 (1990); Brotherton v. Cleveland, 923 F.2d 477 (6th Cir. 1991); Hecht v. Superior Ct., 16 Cal. App. 4th 836 (Ca. App. 1993).

[114] *See* Alice Corp. Pty. v. CLS Bank Int'l, 573 U.S. 208, 214 (2014).

rights in their data, we need to seek out ways to make their means more out in the open. Also, granting companies who cooperate with law enforcement property rights in the face template data further makes undocumented immigrants more vulnerable and helpless.

Copyright protection is another possibility but not without its issues. In order to be eligible for US copyright, data needs to be original and have an element of creativity added.[115] Programs, like facial recognition, are generally copyrightable under 17 U.S.C. § 101 (because the codes creating the programs are "written"). But US copyright only protects against copying and distributing of any eligible compilation of data. The exclusive reproduction and derivative work rights, as construed by the Supreme Court, will not normally prevent unauthorized extractions of disparate data.[116] Thus, this protection is more for the databases and not the data contained within the databases. Again, copyright protection is not adequate for protection of face template data within these third-party databases.

One of the largest problems with creating IP protections in face templates is the ease at which digital data is alienable. DMV photos, stock photos, or video stills from Ring or other available sources can easily be exchanged between parties. Likewise, so can face templates. This argument is also at the heart of privacy arguments against property rights in personal information.[117] Alienability is among the "bundle of sticks" in property rights and it would seem that creating intellectual property rights would create more problems than solutions.

However, it could be useful to look outside of the United States for a better solution for rights in face templates. The UK specifically has been more favorable to protecting compilations of factual information than many other countries in Europe and also the USA.[118] But more importantly, the European continental copyright principle of moral rights provides a more workable framework. Morals rights are among the bundle of rights given by European copyright,[119] and emphasize the strong link between the work and its author.[120] Among the commonly recognized moral rights are the paternity right (i.e., the right to be identified as the author of the work) and of integrity (i.e., the right to protect the work from alterations that would be harmful to the author's reputation).[121] Also in France, authors also have moral rights of "divulgation" (i.e., the right to decide when and under what circumstances to divulge the work) and sometimes even of withdrawal (i.e., the right to withdraw all published copies of the work if the work no longer represents the author's views or otherwise would be detrimental to the author's reputation).[122] The integrity and divulgation interests may be the closest analogous moral rights that might be adaptable to protect personal data.[123]

These concepts are codified in the 1996 Database Directive, which harmonized database law in Europe. It created a *sui generis* intellectual property right to protect against the extraction or re-utilization of all or the substantial part of the contents of a database.[124] The database contents do not even have to necessarily be protected by copyright in the first place. Even though it protects database owners/creators, it still uses the right to exclude others and places limits on how the data can be used.

Moral rights could be granted to face templates to protect them from unauthorized use from the government. Paternity rights can be given to give individuals some claim to their faces. An integrity right can also be given to place limits on what their faces and face templates may not be used for and the right of divulgation limits what they may be used for. Thus, facial recognition software would not be able to be run on databases containing a person's face or face template because they have an intellectual property right

[115] *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991).

[116] J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?,* 50 VAND. L. REV. 51, 63 (1997).

[117] *See* Pamela Samuelson, *Privacy as Intellectual Property?,* 52 STAN L. REV. 1125, 1137-38 (2000).

[118] SIMON STOKES, DIGITAL COPYRIGHT: LAW AND PRACTICE 80 (5th ed. 2019). *Feist* would probably have come out differently in the UK and a telephone directory made with "sweat of the brow" of the creator would have been enough to overcome originality. *Id.*

[119] PAUL TORREMANS, HOLYOAK AND TORREMANS INTELLECTUAL PROPERTY LAW 219 (5th ed. 2008).

[120] *Id.* at 229.

[121] *See* Reichman & Samuelson, *supra* note 116, at 1147.

[122] *Id.*

[123] *Id.* at 1148.

[124] *See* STOKES, *supra* note 118, at 81.

in this data, the paternity right. And by a statuary limitation, the integrity and divulgation rights would prohibit the searches from taking place. Another possible solution is granting contracts akin to licenses for a face or face template. However, this would create a myriad of contracts to be decided upon and considered and is not as workable as moral rights.

Of course, the United States has yet to adopt anything similar to moral rights in the realm of copyright and creating a new body of law to protect biometric data is perhaps too large a step. Conceptually, even though purely theoretical, it seems as though European moral rights can provide a basic template.

CONCLUSION

Despite the drastic changes to the world of immigration since 1984, American courts have failed to increase the privacy rights of undocumented immigrants. Constitutional violations are continually being repeated in deprivations of liberty and property resulting in family separations, children without parents, and children in border prisons.

Ultimately, Congress has the Constitutional power to regulate Immigration, but how can they protect the substantive rights of individuals undergoing the process of immigration/deportation?

This was an academic legal exploration in how to give undocumented immigrants more rights in their facial data because of the injustices of facial recognition technology in both the immigration enforcement and justice systems. The privacy rights of undocumented immigrants have been eroded and are virtually (and digitally) non-existent. Realistically, the civil rights of undocumented immigrants cannot be entirely protected by European copyright law, adapted to these means, but Congress can possibly use IP to enable power to create these protections.

The dangers of facial recognition are currently being debated in legislatures and courts all over the country. The California legislature has already banned facial recognition software on police body cams.[125] The ACLU is suing the Department of Justice, FBI, and DEA over the use of facial recognition software, saying the "government's use of biometric identification and tracking technologies—tools that enable "undetectable, persistent and suspicionless surveillance on an unprecedented level."[126] The federal government continues to push the envelope with surveillance and facial recognition and drones at the Mexican border.[127] It appears as though the use of facial recognition is the biggest loop-hole in the Bill of Rights. James Madison did not even see it coming.

[125] Rachel Metz, *California Lawmakers Ban Facial Recognition Software from Police Body Cams,* CNN (Sept. 13, 2019), https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html [https://perma.cc/6PV7-7VBU].

[126] Monica Haider, *ACLU sues federal government over surveillance from facial recognition technology,* CNN (Nov. 1, 2019), https://www.cnn.com/2019/11/01/us/aclu-sues-federal-government-over-surveillance-from-facial-recognition-technology/index.html [https://perma.cc/4AB2-V6RB].

[127] Sidney Fussell, *The Endless Aerial Surveillance of the Border,* THE ATLANTIC (Oct. 11, 2019), https://www.theatlantic.com/technology/archive/2019/10/increase-drones-used-border-surveillance/599077/ [https://perma.cc/U4J7-3WNF].