The University of Cincinnati Intellectual Property and Computer Law Journal

Volume 6 | Issue 2 Article 3

April 2022

Losing Dignity: Eroding Privacy Rights of Immigrants in Technology-based Immigration Enforcement

Inma Sumaita
University of Cincinnati College of Law

Losing Dignity: Eroding Privacy Rights of Immigrants in Technology-based Immigration Enforcement

By: Inma Sumaita

Introduction:

Immigrants and their families across the United States live in constant fear of U.S. Immigration and Customs Enforcement ("ICE") agents, who target millions of undocumented persons, raiding their homes, worksites, and community spaces.[1] During an immigration raid, agents physically invade a workplace, arriving unannounced with militaristic force, to target workers for arrest and deportation.[2] Immigration agents seal off the workplace's exits and detain workers, then send them to remote detention centers without warning or chance of preparation.[3] These worksite raids have resulted in more than 1,800 arrests since 2017.[4]

In October of 2021, the Biden administration directed enforcement agencies to stop all workplace raids and instead focus on employers who willfully hire undocumented workers.[5] In the past few years, during which raids have intensified, ICE has rounded up tens of thousands of persons, charged hundreds with immigration law violations, and deported a massive portion of them.[6] Since these raids seek to enforce U.S. immigration laws against persons who broke the law by entering the U.S. without authorization or by overstaying their authorization, the morality and legality of these raids are not often questioned. However, in this ongoing hardline enforcement policy of immigration laws coupled with exponential leaps made in technology used for such purposes, the amount of basic dignity afford to immigrants are reaching an all time low.

---

[1] *Worksite immigration raids*, NATIONAL IMMIGRATION LAW CENTER (2020), https://www.nilc.org/issues/workersrights/worksite-raids/ (last visited Mar 14, 2022).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] Jasmine Aguilera, *Biden's ice raids shift is too late for immigrant families*, TIME (Oct. 20, 2021), https://time.com/6107024/joe-biden-ice-raids-immigrant-families/ (last visited Mar 14, 2022).
[6] Ice statistics, ICE, https://www.ice.gov/remove/statistics (last visited Mar 14, 2022).

Undocumented immigrants, especially, consistently face risks of discrimination, surveillance, and deportation. As it becomes easier to track and maintain records of people's lives through technology and innovation, the disparity in privacy rights seems to be further perpetuated. This article will explore how the law's designation of immigrants' illegality interplays with the Fourth Amendment doctrines of consent, administrative searches, reasonable expectation of privacy, and pretextual stops to exclude privacy protection for immigrants. In addition, this article also examines the legal quandries of using technology to invade privacy through the spread of immigration databases and the proliferation of federal and local surveillance of spaces occupied by immigrants within the border.

Scope:

This paper looks at the tension between immigration enforcement policies and the basic privacy rights as afforded by the U.S. Constitution. This paper examines the complex and opaque web of databases, related systems, and information-sharing mechanisms that facilitate federal immigration and local criminal enforcement. This paper will further discuss the constitutional issues raised by these immigration enforcement policies. The databases, systems, and mechanisms in place depend on the participation of private companies as well as the cooperation of state and local law enforcement with federal law enforcement and immigration and agencies. This paper will also evaluate the participation of both government and private actors in the increased surveillance of immigrants.

Background:

The Fourth Amendment to the United States Constitution was ratified in 1791 and is intended to protect the privacy of individuals in the United States. It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon

probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. U.S. Const. amend.IV.

In *Katz,*[7] Justice Harlan famously stated that the Fourth Amendment protects one's reasonable expectation of privacy.[8] Although most Americans enjoy these rights and protections, not everyone in America does. A population exists within the borders of the United States that is not afforded the right of privacy or to be left alone, stripped of the basic privacy protections of the Fourth Amendment. Since undocumented immigrants have limited Constitutional and privacy rights, their personal data is subject to a high probability of use and abuse. The Department of Homeland Security ("DHS") and ICE are using facial recognition software to identify, target, and locate undocumented immigrants. Although this is seemingly in violation of the rights to due process and to be free from unreasonable searches, and often uses race as a primary means of discrimination, these rights are not enforced or protected by the courts.

In the 1970s, the U.S. Supreme Court found that the Fourth Amendment applied to immigration enforcement, although with an increased tolerance for racial profiling.[9] In *United States v. Brignoni-Ponce,*[10] the Court recognized that traffic-checking practices at the border involve a different balance of public and private interests, and thus are subject to less stringent constitutional safeguards. Determination was required as to the circumstances in which a roving patrol could stop motorists in the general area of the border for an inquiry into their residence status. The Court found that such an interference with Fourth Amendment interests involved in the stop was "modest,"[11] while the inquiry served significant law enforcement needs. The Court therefore held that a roving-patrol stop did not require probable cause and may be undertaken if the stopping officer is "aware of specific articulable facts, together with rational

[7] *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967)
[8] *Id* at 361.
[9] *See United States v. Martinez-Fuerte*, 428 U.S. 543, 545 (1976); United States v. Brignoni-Ponce, 422 U.S. 873, 884 (1975).
[10] *United States v. Brignoni-Ponce*, *supra* note 9.
[11] *Id*. at 880.

inferences from those facts, that reasonably warrant suspicion" that a vehicle contains undocumented immigrants.[12]

Through a subsequent series of decisions, the Fourth Amendment of the U.S. Constitution (the "Fourth Amendment") has become abraded, granting little to no privacy protections to noncitizens, particularly in the realm of immigration enforcement.

De-evolution of the Fourth Amendment's Applicability for Immigrants:

Immigration & Naturalization Serv. v. Lopez-Mendoza,[13] completely changed how the Fourth Amendment was applied to deportation hearings. The Ninth Circuit found that agents of the U.S. Immigration and Naturalization Service ("INS"), the precursor agency to ICE, violated the Fourth Amendment rights of Adan Lopez-Mendoza and another similarly situated plaintiff, Elias Sandoval-Sanchez, at the time of their immigration arrests. The court found that any evidence that the agents had acquired through those unconstitutional arrests must therefore be excluded from proceedings in accordance with the exclusionary rule of the Fourth Amendment.[14] The exclusionary rule prevents the use of most evidence gained in violation of any part of the United States Constitution. A decision called *Mapp v. Ohio*[15] established that the exclusionary rule applies to evidence obtained from an unreasonable search or seizure in violation of the Fourth Amendment.

However, the Supreme Court granted certiorari and, in a plurality opinion written by Justice O'Connor, the Court held that the exclusionary rule "need not apply" in deportation hearings because deportation hearings are purely civil in nature and are not criminal hearings.[16] Justice O' Connor emphasized that "[t]he 'body' or identity of a defendant or respondent in a criminal or civil proceeding is

[12] *Id.*, at 884.
[13] *Immigration & Naturalization Serv. v. Lopez-Mendoza,* 468 U.S. 1032, 104 S. Ct. 3479 (1984)
[14] *Mapp v. Ohio,* 367 U.S. 643, 81 S. Ct. 1684 (1961)
[15] *Id.*
[16] *Immigration & Naturalization Serv.* at 1034.

never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred."[17]

Justice O' Connor arrived at her holding in trying to balance the Fourth Amendment's deterrent effect on future law enforcement misconduct against the loss of probative evidence as discussed in a prior case, *United States v. Janis*, 428 U.S. 433, 96 S. Ct. 3021 (1976). Ultimately, the Court found that the exclusionary rule is not needed to deter future misconduct because there are other safeguards in place.[18]

> In these circumstances we are persuaded that the *Janis* balance between costs and benefits comes out against applying the exclusionary rule in civil deportation hearings held by the INS. By all appearances the INS has already taken sensible and reasonable steps to deter Fourth Amendment violations by its officers, and this makes the likely additional deterrent value of the exclusionary rule small. The costs of applying the exclusionary rule in the context of civil deportation hearings are high. In particular, application of the exclusionary rule in cases such as Sandoval-Sanchez', would compel the courts to release from custody persons who would then immediately resume their commission of a crime through their continuing, unlawful presence in this country. "There comes a point at which courts, consistent with their duty to administer the law, cannot continue to create barriers to law enforcement in the pursuit of a supervisory role that is properly the duty of the Executive and Legislative Branches."That point has been reached here.[19]

However, in light of recent raids, immigrants are increasingly looked at through the lens of criminality, and undocumented immigrants are being investigated and tried as criminals.[20] Still there has been slow progress in regard to safeguards needed to ensure the Fourth Amendment rights of immigrants.

The Fourth Amendment became somewhat more pliable in criminal cases involving immigrants in *United States v. Verdugo-Urquidez,*[21] where the United States Supreme Court reversed the order granting defendant's motion to suppress evidence seized during a search of their residence in Mexico. The defendant argued that a search of his residence in Mexico violated his rights under the Fourth Amendment against

[17] *Id.*
[18] *Id.*
[19] *Id.*, at 1050 (internal citations deleted).
[20]The Immigration Reform and Control Act (IRCA) was passed in 1986 and made it illegal for employers to knowingly employ undocumented immigrants. This was the first time that a US law to made the undocumented status of an individual a designated crime.
[21] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 261, 110 S. Ct. 1056, 1059 (1990)

unreasonable search and seizure. The district court held that drug enforcement agents failed to justify the search of respondent's Mexico residence without a warrant. Justice Rehnquist delivered the opinion that found that the Fourth Amendment protection against unreasonable searches and seizures extended its reach only to "a class of persons who were part of a national community or who had otherwise developed sufficient connection with the United States to be considered a part of its community."[22] The Court distinguished the matter from cases where U.S. residents stationed abroad were still afforded rights under the Constitution, but because the defendant was a Mexican citizen with no voluntary attachment to the United States, and because the residence which was searched was located in Mexico, the protections against unreasonable search and seizure did not apply.

Given the vague language of the Verdugo opinion, one interpretation of Verdugo rejects a case-by-case evaluation of individuals' connections to the United States in favor of a categorical exclusion of certain classes of undocumented immigrants from Fourth Amendment protection. There is no clear consensus on which classes of undocumented immigrants are outside the Fourth Amendment's scope. The District of Utah's opinion in *United States v. Esparza-Mendoza*[23] provided that as a previously deported felon, the defendant in the case, lacked "sufficient connection" to the country to assert a Fourth Amendment suppression claim.

To determine whether Esparza had "substantial connections" to the United States, the court started the discussion with, "first, the historical background regarding the attachment of alien felons to the political community, and, second, the specific facts surrounding (the defendant)."[24] With respect to the history of immigrants with felony charges, the court noted that the Framers "would have had grave concerns about criminal aliens in particular,"[25] and brought attention to Britain's practice of sending convicted felons to its

[22] *Id.* at 265
[23] *United States v. Esparza-Mendoza*, 265 F. Supp. 2d 1254 (D. Utah 2003), aff'd, 386 F.3d 953 (10th Cir. 2004)
[24] *Id.* at 1267.
[25] *Id.*

colonies as indentured servants. The court further noted that even after Britain could no longer send felons to the U.S., many of the states passed legislation to prohibit the transportation of convicts across their state borders. According to the court, this historical exclusion of foreign criminals, in combination with the exclusion of foreigners from voting, weighed against a finding that a foreign felon could be "part of or connected to the nation's political community. To the contrary, the historical materials suggest that the Framers were doing everything possible to exclude such persons from the national community."[26]

Databases and Immigration Enforcement:

In *Gonzalez v. United States Immigr. & Customs Enf't*, 975 F.3d 788 (9th Cir. 2020) the detainee was a United States citizen who was held in county jail on immigration detainer after he was arrested on state charges. He brought a class action on behalf of current and former immigration detainees challenging the legality of the practice by the sheriff's department of detaining individuals solely on the basis of immigration detainers placed by ICE. The plaintiffs challenged the Government's issuance of immigration detainers which were based solely on searches of electronic databases to make probable cause determinations of removability. The district court concluded that the databases were unreliable for determining probable cause of removability and found that the government thus violated the Fourth Amendment by issuing detainers based solely on searches of the databases.[27]

The court of appeals affirmed that to issue a valid immigration detainer, probable cause must be established to believe that the person being detained "is, in fact, an alien."[28] Further, the case found that the establishment of probable cause in the immigration context is the same as it is in a criminal context. This

[26] *Id.* at 1269.
[27] *See Gonzalez*, 416 F. Supp. 3d at 1016–21
[28] *Id*. at 817, quoting *Alcocer v. Mills*, 906 F.3d 944, 953 (11th Cir. 2018)

means that the government must rely on a "reasonably trustworthy information sufficient to warrant a prudent person in believing that an individual has committed an offense."[29]

The decision in *Gonzalez v. ICE* challenges various U.S. Immigration and Customs Enforcement detainer practices, including the agency's reliance on unreliable databases to generate detainers for local law enforcement to hold individuals for transfer into immigration custody. The detainers generated by these databases were the foundation of an immigration enforcement program called Secure Communities.

Secure Communities was a deportation program designed by DHS that relied on extensive collaboration among federal, state, and local law enforcement agencies. According to ICE, 363,400 people were removed under this program before being discontinued by President Biden in 2021.[30] It relied significantly on detainers issued solely on the basis of such unreliable electronic databases. ICE officers and contractors reviewed the results of automated database searches on every person that was put into police custody anywhere in the country. ICE subjected over 2 million people to these unconstitutional arrests since the inception of the program in 2008 based on nothing but these database results.[31]

Another tool of federal and state cooperation favored by ICE is the 278(g) program. The 278(g) program, named after Section 287(g) of the Immigration and Nationality Act, became law as a part of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRAIRA").[32] This program establishes a formal Memoranda of Agreement which deputizes local law enforcement officers to perform central functions of federal immigration officers.[33]

---

[29] *Id*. at 819
[30] *Secure communities*, ICE, https://www.ice.gov/secure-communities (last visited Mar 14, 2022).
[31] *Press Release:Gonzalez v. ICE*, NATIONAL IMMIGRANT JUSTICE CENTER (Sep. 30, 2021), https://immigrantjustice.org/court_cases/gonzalez-v-ice (last visited Mar 14, 2022).
[32] *The 287(g) Program: An Overview*, AMERICAN IMMIGRATION COUNCIL (2021), https://www.americanimmigrationcouncil.org/research/287g-program-immigration (last visited Mar 14, 2022).
[33] *Id*.

Once deputized under 287(g), "law enforcement officers may issue immigration detainers, interview individuals to ascertain immigration status, check DHS databases for information about individuals they believe are not citizens, transfer immigrants directly to ICE custody, and even issue a Notice to Appear (NTA), the charging document that begins the federal deportation process."[34] There are currently only two types of 287(g) agreements that are employed in the field: the "jail enforcement" model and the "warrant service officer" model. The jail enforcement model allows deputized officers to interrogate suspected noncitizens who have been arrested on local charges regarding their immigration status and they may place immigration detainers on those that they suspect to be subject to removal.

Under the model of warrant service officer (WSO), ICE trains, certifies, and authorizes selected state and local law enforcement officers to execute ICE administrative warrants.[35] These officers are then permitted to perform the arrest functions of an immigration officer within their jails and/or correctional facilities.[36] This model differs from the jail enforcement model in that the local law enforcement officers are not authorized to interrogate alleged noncitizens about their immigration status.[37]

Federal, state, and local governments also have Inter-Governmental Service Agreements (IGSAs), which are contracts where local agencies agree to provide space in their county jails or state prisons to detain people during their immigration removal proceedings.[38] The federal government typically pays these facilities for each person that the jail or prison detains for ICE, so it provides a financial incentive to incarcerate more immigrants.[39] The existence of IGSAs disproportionally increases ICE's surveillance and

[34] Nayna Gupta & Heidi Altman, *Policy Brief: Disentangling Local Law Enforcement from Federal Immigration Enforcement* , NATIONAL IMMIGRATION JUSTICE CENTER (Jan 13, 2021), https://immigrantjustice.org/research-items/policy-brief-disentangling-local-law-enforcement-federal-immigration-enforcement (last visited Mar 14, 2022).
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Joshua Breisblatt & Alyson Sincavage, *Assumption of Risk: Legal Liabilities for Local Governments That Choose to Enforce Federal Immigration Laws*, NATIONAL IMMIGRANT JUSTICE CENTER (Mar 7, 2018), https://immigrantjustice.org/research-items/report-assumption-risk-legal-liabilities-local-governments-choose-enforce-federal (last visited Mar 14, 2022).

detention capacity.[40] Some jurisdictions participate in both a 287(g) program and an IGSA, creating perverse financial incentives for local police officers to execute detainers under their 287(g) authority in order to fill up their jails, which increases the likelihood of racial profiling in local arrest practices.[41]

Relying on local law enforcement officers to interpret complex federal immigration laws to make decisions, such as whether to issue an immigration detainer, exposes local law enforcement officers to significant liability.

Gang Databases and their Disprortionate Impact on Immigrants:

Local, state, and federal gang databases identify certain people as gang members, often without much reason, and may include photos and other information.[42] Anyone identified as a gang member or an "associate" may experience dramatic consequences to their immigration status.[43] Some gang-related databases that are used by immigration agencies and other law enforcement agencies in the U.S. include GangNET, ICEGangs, and the NCIC Gang File, as well as gang databases maintained independently by different state and local agencies.[44]

GangNET is a commercial intranet-linked software that appears to be critical for the collection and storage of gang related information by state and federal governments.[45] The program offers a database filled with information on individuals and gangs along with photo, data analysis, mapping, facial recognition software, a watch list, and a field interview form.[46] Agencies can use a single command to simultaneously search their own GangNET system as well as a network of GangNET systems in other states and federal

[40] *Id.*
[41] *Id.*
[42] SEAN GRACIA-LEYS ET AL., MISLABED: ALLEGATIONS OF GANG MEMBERSHIP AND THEIR IMMIGRATION CONSEQUENCES (2016), https://www.law.uci.edu/academics/real-life-learning/clinics/ucilaw-irc-MislabeledReport.pdf.
[43] *Id*.
[44] *Id*.
[45] *Privacy Impact Assessment for the GangNet,* DEPARTMENT OF JUSTICE (May 31, 2006), https://www.justice.gov/opcl/page/file/912976/download (last visited Mar 14, 2022).
[46] *Id*.

agencies.[47] The GangNET software is operational in many states such as Arizona, California, District of Columbia, and ten other states, as well as Canada.[48] Of those, some were sharing information in real time.[49] The system allows data collection from various law enforcement personnel, such as officers in the field, patrol officers, gang units, corrections officers, and other law enforcement entities.[50]

In 2010, ICE created its own gang database called ICEGangs, to function as a repository of personal information on suspected or confirmed gang members and their "associates," as well as for information on gang activities.[51] The ICEGangs system was based on GangNET's software and "tailored to include immigration status–related information."[52] Agents of ICE could use ICEGangs to gain access to other databases that use GangNET.[53] The Immigrant Legal Resource Center reported on April of 2017 that ICE has stopped using ICEGangs in 2016 because ICE agents were instead relying on other case management databases.[54] ICE has not confirmed that it no longer uses ICEGangs and has not issued any insight into how and when it collects and uses information pertaining to suspected gang membership.[55]

The Gang File in the FBI's National Crime Information Center ("NCIC") database provides information to both state and local law enforcement, but also to ICE as well.[56] The criteria under which information about a person would be inserted into the Gang File (formerly the Violent Gang and Terrorist Organizations File, or VGTOF) include that the person in question has admitted to being a gang member,

---

[47] *Id*.
[48] *Id*.
[49] *See: White Paper: GangNet® Software,* SRA International, https://s3.documentcloud.org/documents/1683801/gangnet8-whitepaper2013.pdf (last visited Mar 14, 2020).
[50] *Id*., p.2
[51] *Privacy Impact Assessment for the ICEGangs Database*, U.S. DEPT. OF HOMELAND SECURITY (Jan 15, 2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_16_ice_icegangs.pdf.
[52] *Id.*
[53] Sean Garcia-Leys, et. al., *supra* note 42, p. 8.
[54]*Practice Advisory: Understanding Allegations Of Gang Membership/Affiliation In Immigration Cases*, the IMMIGRANT LEGAL RESOURCE CENTER (Apr 2017), https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170509.pdf (last visited Mar 14, 2020).
[55] *Privacy Impact Assessment for the ICEGangs Database*, *supra* note 51.
[56] *National Crime Information Center (NCIC)* (Federal Bureau of Investigation), https://www.fbi.gov/services/cjis/ncic. (last visited Mar 14, 2020).

that informants have identified this person as a gang member, or that this person has spent time in a proximity of a gang, or in their "area."[57] State and local law enforcement officers can enter names into the Gang File, and often their submissions are not subject to any restrictions or checks for accuracy.[58]

The existence and use of the databases described above can be difficult to challenge because they were created, ostensibly, to combat crime and gang violence. However, as noted above, these databases are subject to few rules and little accountability. Historically, people who are listed in gang databases have had little control over their accuracy and few options to contest their inclusion in them.[59] Moreover, according to a report conducted by the National Immigration Law Center, gang databases have been shown to contain listings for people who quite clearly and unequivocally should not have been listed, citing cases for infants as an example.[60]

Whether someone is included in a gang database system is often left at the discretion of local law enforcement, and the police's reliance on racial stereotypes can lead to a disproportionate amount of people of color being included in the databases.[61] As the databases are so inextricably linked, when an erroneous information is entered into one database, it can easily infect others with inaccuracies because of their information-sharing practices.

[57] "Privacy Act of 1974; Notice of Modified Systems of Records," 64 Fed. Reg. 52343–52349 (Sep. 28, 1999), https://www.gpo.gov/fdsys/pkg/FR-1999-09-28/pdf/99-24989.pdf.

[58] James Jacobs and Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, N.Y.U. JOURNAL OF LEGISLATION AND PUBLIC POLICY, (Winter 2008) p. 193.

[59] *Untangling The Immigration Enforcement Web*, THE NATIONAL IMMIGRATION LAW CENTER (Sep, 2017) https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf (last visited Mar 14, 2022)

[60] *Id*.

[61] Rebecca A. Hufstader, *Immigration Reliance on Gang Databases: Unchecked Discretion and Undesirable Consequences*, 90 NYU. L. REV. 671 (2015).

In August 2016, the California State Auditor prepared a report about CalGang, California's version of GangNET, and exposed serious problems.[62] The report explains that CalGang plays an important role in populating federal gang databases, and its data is shared with other states.[63] However, the report states that the system operates without any oversight, contains unsubstantiated and incorrect information, and does little to actually protect public safety.[64] In 2019, a review by Chicago's Office of Inspector General found similar systemic issues in their version.[65]

In *Diaz Ortiz v. Garland*, 23 F.4th 1 (1st Cir. 2022), a noncitizen teenager, native to El Salvador filed a petition to review a decision by the Board of Immigration Appeals ("BIA") affirming an immigration judge's denial of his claims for asylum, withholding of removal, and protection under the Convention Against Torture ("CAT"). The United States Court of Appeals for the First Circuit found that federal immigration officers should not have relied on the Boston Police Department's gang database to determine that the teenager was a member of the gang, MS-13, and therefore deemed deportable upon that. The court observed that the way the information was entered into the databases was arbitrary and may be somewhat racially motivated:

> There is a patent disconnect between Diaz Ortiz's conduct as described in the database and any threatening, "gang-like" activities. None of the reports support an inference that he had participated in criminal activity at all, let alone the kinds of violent crimes for which MS-13 is infamous. Indeed, absent the unsubstantiated statements that those with whom he associated were gang members, the FIOs show no more than a teenager engaged in quintessential teenage behavior -- hanging out with friends and classmates. These social encounters occurred in unremarkable neighborhood locations for this peer group: at a park, at school, in front of one teenager's home, on the benches in an empty stadium. The record lacks any evidence as to why assigning points for those interactions was a reliable means

[62] *The CalGang Criminal Intelligence System: As the Result of Its Weak Oversight Structure, It Contains Questionable Information That May Violate Individuals' Privacy Rights* (California State Auditor, Report 2015-130, Aug. 2016), https://www.auditor.ca.gov/pdfs/reports/2015- 130.pdf.

[63] *Id.*, at p. 2.

[64] *Id.*, at p. 3.

[65] *Review of The Chicago Police Department's "Gang Database"*, CITY OF CHICAGO OFFICE OF INSPECTOR GENERAL (Apr, 2019) https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf (last visited Mar 14, 2022)

> of determining gang membership. Certainly, the fact that the young men were all Hispanic does not permit an inference that any, or all, of them were gang members.[66]

The court ordered a reconsideration of his asylum petition, citing "[f]laws in that database, including its reliance on an erratic point system built on unsubstantiated inferences." The court's ruling basically states that law enforcement agencies violate federal regulations when they gather "criminal intelligence" information without reasonable suspicion that a person is actually involved in any criminal conduct.

Thomas Nolan, a professor at Emmanuel College and former Boston police officer, testified on behalf of Diaz Ortiz as an expert.[67] Nolan advocated that Diaz Ortiz "should not have been listed as a verified gang member" because the "intelligence" about Diaz Ortiz did not comply with federal regulations governing shared criminal intelligence databases in the Code of Federal Regulations.[68] Nolan explained that the regulations are implicated since the Gang Assessment Database "is an interjurisdictional shared database that [is] accessible to other agencies."[69] The part of the code to which Nolan referred was originally adopted in 1980 to ensure that the operation of criminal intelligence systems was not conducted "in violation of the privacy and constitutional rights of individuals."[70] The court in the instant case, commented that this purpose that has remained unchanged.[71]

Following this opinion, it would logically flow that some of the criteria that are used to induct someone into gang databases would violate federal regulations and also raise constitutional concerns. As emphasized by the court, "[T]he federal regulations cited above plainly prohibit entities like BRIC from collecting 'criminal intelligence information' about an individual unless 'there is reasonable suspicion that the individual is involved in criminal conduct or activity.' 28 C.F.R. § 23.20(a) (emphasis added). Simply

---

[66] *Diaz Ortiz v. Garland*, 23 F.4th 1, 11 (1st Cir. 2022).
[67] *Id.*
[68] *See generally* 28 C.F.R. Part 23.
[69] *Diaz Ortiz v. Garland, supra* note 66.
[70] Criminal Intelligence Systems Operating Policies, 45 Fed. Reg. 40,156, 40,156 (June 13, 1980).
[71] *Diaz Ortiz v. Garland, supra* note 66, citing 28 C.F.R. § 23.1.

associating with people who may be engaged in criminal activity is not enough."[72] Thomas Nolan subsequently commented to a reporter that "freedom of association is a constitutionally protected activity under the First Amendment, and that's lost" in the establishment of gang database procedures.[73]

The Boston Police Department amended its database policy, clarifying that Bostonians may not be deemed gang members solely on the basis of a police officer's casual observations at random interactions.[74] It's unclear how much error is eliminated by this update but, the recent decision from the First Circuit might open up an avenue for further examination on the use and validity of such databases.

The Extent of ICE's Authority:

In *Morales v. Chadbourne*, the Rhode Island state court ordered that a woman be released from a local jail on personal recognizance while her criminal case was on going.[75] The jail continued to hold her back on an ICE detainer for immigration purposes.[76] The ICE detainer lacked any proper justification for her immigration detention.[77] Upon suing ICE, the court held that ICE lacked probable cause since it failed to sufficiently investigate her immigration status before the issuance of the detainer.[78] It was later established that the woman was, in fact, a naturalized U.S. citizen.[79] This case cemented that it is established law that ICE agents first Frequire probable cause to issue an immigration detainer.[80] The court noted, "It remains undisputed that the State detained Ms. Morales based on an invalid detainer and that it did not

[72] *Id*.
[73] Hassan Kanu, *D.C.'s gang database highlights unconstitutional systems nationwide*, REUTERS (Jan 19, 2022) https://www.reuters.com/legal/government/dcs-gang-database-highlights-unconstitutional-systems-nationwide-2022-01-19/ (last visited Mar 15, 2022)
[74] Boston Polic Department, *Boston Police Department Police Reform Policy Update*, CITY OF BOSTON (Jun 10, 2021) https://www.boston.gov/news/boston-police-department-police-reform-policy-update (last visited Mar 15, 2022)
[75] 235 F. Supp. 3d 388 (D.R.I. 2017).
[76] *Id*. at 394.
[77] *Id*.
[78] *Id*. at 397.
[79] *Id*.
[80] *Id*. at 398.

afford her appropriate notice and an opportunity to be heard on her further detention,19 both in violation of Ms. Morales' constitutional rights."[81]

Detainers issued by ICE are not judicial warrants, and local agencies are not required to respond to them.[82] A detainer can be signed by any ICE officer based on ICE's discretionary interest in deporting a person.[83] Unlike in the case of police warrants, ICE officers do not have the practice of obtaining a prompt probable cause determination from from a jude, prior to making an arrest.[84]

In 2020, Los Angeles County settled for $14 million in a class-action lawsuit against the L.A. County Sheriff Department for its practice of routinely holding people in jail beyond their release dates due to detainer requests from ICE. This settlement underscores the significant liability local law enforcement agencies face in cooperating with federal immigration agencies.[85]

In 2019, a federal district court judge issued a permanent injunction in *Gonzalez v. ICE*, 416 F. Supp. 3d 995 (C.D. Cal. 2019), which blocked ICE from issuing detainers based solely on information acquired from database searches, because the court found that such searches are too unreliable. This decision "blocked all detainers generated by one ICE station in Laguna Niguel, California, from which ICE issues detainers 24 hours per day within California and afterhours for 47 other states."[86] Recently, the Ninth Circuit Court of Appeals reviewed and upheld part of the district court's decision, finding that ICE's current use of detainers still fails to meet the Fourth Amendment's requirements.[87]

[81] *Id*. at 406.
[82] Nayna Gupta, *supra* note 34.
[83] *Id*.
[84] *Id*.
[85] Alene Tchekmedyian, *LA county to payout $14 million over unlawful immigration holds*, LOS ANGELES TIMES (Oct 13, 2020) https://www.latimes.com/california/story/2020-10-13/sheriffs-department-immigration-holdssettlement (last visited Mar 14, 2022)
[86] *Press release*, *supra* note 28.
[87] *Id*.

Border Searches of Electronic Devices:

The Supreme Court has yet to address whether the Fourth Amendment's border search exception extends to warrantless searches of personal electronic devices, such as cell phones and computers. These devices typically contain more personal and sensitive information than is typically found in a backpack or inside an automobile. However, some lower courts have addressed the constitutionality of such searches in a few notable cases.

In the 2014 decision *Riley v. California,* the Supreme Court considered the constitutionality of warrantless electronic device searches within the borders of the United States.[88] The Court held that the police are not allowed to conduct a warrantless search of a cell phone seized during an arrest. The Court held this despite the fact that the Fourth Amendment's warrant requirement usually does not apply to searches incident to a lawful arrest.[89] The Court noted that this exception applies to brief physical searches of property that are within the immediate control of the arrestee in order to prevent potential harm to the police officers and the destruction of evidence. The Court determined that "[t]here are no comparable risks when the search is of digital data."[90]

The Riley Court also surmised that searching cell phone data raised greater issues of privacy than searching physical items that are typically found on a person, such as a wallet.[91] The Court observed that unlike most physical items that one might have on their person, cell phones carry "immense storage capacity" and a broader range of private information, including photographs, text messages, contact information, videos, financial records, and internet browsing history.[92] As such, "[c]ell phones differ in

[88] *Riley v. California*, 573 U.S. 373, 378, 385 (2014)
[89] *Id*. at 401 ("[A] warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").
[90] *Id*. at 386.
[91] *Id*. at 393.
[92] *Id*. at 393–94.

both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[93] The Court held that the police must first secure a warrant before they can search the contents of a cell phone seized during an arrest,[94] but also noted that "other case-specific exceptions may still justify a warrantless search of a particular phone."[95] The Court suggested that there remained a continued availability of exception warranted in exigent circumstances to pursue a fleeing suspect, prevent the imminent destruction of evidence, or to assist persons who are seriously injured or are threatened with imminent injury.[96] The Court, however, did not address whether the border search exception allows warrantless electronic device searches at the border as an exigent circumstance.

Lower courts have applied the border search exception to electronic device searches. For instance, in *United States v. Ickes*, the Fourth Circuit court held that manually inspecting the contents of a computer at the border was permissible provided "the Supreme Court's insistence that U.S. officials be given broad authority to conduct border searches."[97] The court concluded that "[t]his well-recognized exception to the safeguards of the Fourth Amendment comes with an equally well-established rationale."[98]

The Ninth Circuit court ruled that the search of a computer also fell within the border search exception in *United States v. Arnold*, because examining a computer's files is analogous to scanning the contents of luggage.[99] The court also highlighted the balance of national interest against individual rights, quoting: "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[100] Conversely, the Ninth Circuit also found that

[93] *Id*. at 393.
[94] *Id*. at 403.
[95] *Id*. at 401-402.
[96] *Id*. at 402.
[97] *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005).
[98] *Id.* at 506.
[99] *United States v. Arnold*, 533 F.3d 1003, 1008–10 (9th Cir. 2008).
[100] *Id*. citing *United States v. Flores-Montano*, 541 U.S. 149, 156 S. Ct. 1582 (2004)

while a "quick look" at files in a computer would not warrant a strong suspicion, a forensic examination[101] of the hard drive exceeded the scope of a routine border search given its "comprehensive and intrusive nature."[102] The court clarified that "[e]lectronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files,"[103] and that, "[s]uch a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity."[104] The court held that a "computer strip search" such as in the aforementioned circumstances required reasonable suspicion.[105]

In 2018, the Fourth Circuit ruled that forensic border analysis of a cellphone required "some form of individualized suspicion" provided the scope of exposure of "uniquely sensitive information" within the device.[106] Citing Riley, the court in *United States v. Kolsuz* reasoned that cell phones are "fundamentally different" from other personal objects traditionally subject to government searches, such as wallets and purses.[107] Conversely, the Eleventh Circuit held that the Fourth Amendment requires no suspicion of criminal activity to warrant a forensic border searches of electronic devices in *United States v. Touset*.[108] The court noted that the Supreme Court has previously upheld an unwarranted search of a fuel tank at the border without imposing any heightened requirements for other types of personal property.[109] The court reasoned that even though the Supreme Court has imposed requirements of reasonable suspicion for searches that can be qualified to be highly intrusive (i.e., of a person's body), the Court has yet to extend this requirement to border searches of personal property, "however nonroutine and intrusive."[110] The court

[101] A forensic examination of an electronic device includes using a software to copy the hard drive and analyze its contents, including deleted content.
[102] *United States v. Cotterman*, 709 F.3d 952, 960, 966 (9th Cir. 2013).
[103] *Id*. at 965.
[104] *Id*. at 968.
[105] *Id*. at 966.
[106] *United States v. Kolsuz*, 890 F.3d 133, 145–46 (4th Cir. 2018).
[107] *Id*.
[108] *United States. v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018).
[109] *Id.* citing *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004).
[110] *Id*.

further reasoned that the restrictions imposed on warrantless cell phone searches incident to an arrest in *Riley*[111] did not apply to searches at the border, where expectations of privacy are diminished.[112]

Courts have also disagreed about what the proper scope of an electronic device search is at the border. The Ninth Circuit has held that the search of an electronic device must be limited to a search for digital contraband within the device itself, and does not include searching the device for additional evidence that may lead to the discovery of a crime in saying, "border officials are limited to searching for contraband only; they may not search in a manner untethered to the search for contraband." [113] The court distinguished the searches concerning items that are actually being smuggled from searches of evidence that may eventually lead to the discovery of contraband.[114] The court therefore determined that border officials may conduct searches of a cellphone under reasonable suspicion that the cellphone physically contains contraband.[115]

In *United States v. Aigbekaen*, the Fourth Circuit court ruled that Customs and Border Patrol ("CBP") officials may conduct forensic border searches of electronic devices so long as there is a reasonable suspicion that the electronic device contains evidence of a crime that "bears some nexus" to the exigent justifications for the border search exception.[116] Similarly, the First Circuit has held that "advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE." [117]

In summation, lower courts have generally offered CBP officers the latitude to conduct relatively limited searches of electronic devices at the border without requiring a warrant or any particularized suspicion. However, courts have disagreed about whether more intrusive searches require at the very least

[111] *Riley v. United States, supra* note 83.
[112] *United States. v. Touset*, *supra* note 101 at 1234.
[113] *United States v. Cano*, 934 F.3d 1002, 1018–19 (9th Cir. 2019), *reh'g denied*, 973 F.3d 966 (9th Cir. 2020).
[114] *Id*. at 1018.
[115] *Id*. at 1020.
[116] *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019).
[117] *Alasaad v. Mayorkas*, 988 F.3d 8, 21 (1st Cir. 2021).

a reasonable suspicion of a crime, and whether such reasonable suspicion must be specifically tied to evidence of the contraband found within the device itself, or if the suspicious may be used to gather any evidence of potential criminal activity that may be taking place.

Biometric Data Collection at the Border:

Biometric data is often collected from international travelers.[118] The term biometric data refers to unique identifiers of a person—such as their DNA, fingerprints, voice recordings, iris or retinal scans, walking gait, and facial geometry.[119] There are several federal statutes that address the collection and use of biometric data by the government, most of which involve screening international travelers who are arriving or departing and other border security measures.[120] 8 U.S.C. § 1365b requires that DHS establish an integrated and automated biometric entry-exit system which can record the arrival and departure of foreign nationals, collect biometric data to verify their identity, and authenticate travel documents through the comparison of biometrics.[121]

6 U.S.C. § 1118, requires that the CBP and the Transportation Security Administration consult each other on the deployment of biometric technologies. It further requires that DHS assess the impacts of using biometric technology and submit an assessment report to Congress.[122] The Office of Biometric Identity Management ("OBIM") routinely maintains a database called the Automated Biometric Identification System ("IDENT"), which holds more than 260 million unique identifiers.[123] This information can be used for a variety of purposes, including "to detect and prevent illegal entry into the United States," facilitate travel, and verify visa applications.[124]

---

[118] Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 773–74 (2018)
[119] *Id*.
[120] *See*, *e.g.*, 8 U.S.C. § 1379
[121] *Id*. § 1365b.
[122] 6 U.S.C. § 1118(c).
[123] *Biometrics*, DHS, https://www.dhs.gov/biometrics (last visited Feb. 24, 2022)
[124] *Id*.

Of course, this practice of collecting biometric information raises privacy concerns.[125] The Supreme Court has repeatedly stressed that the border yields a lower expectation of privacy and that the "[t]he Fourth Amendment balance between the interests of the Government and the privacy right of the individual is struck much more favorably to the Government "[126] The Second Circuit has indicated that collecting fingerprints, a type of biometric identifier, at a land port of entry was part of a routine search and no reasonable suspicion was required for justification.[127] In *Davis v. Mississippi*, the Supreme Court held that the collection of fingerprints did not raise Fourth Amendment concerns when conducted within the United States.[128] The Court upheld the police's practice of collecting the fingerprints of lawfully arrested persons, describing it to be minimally intrusive as it "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[129]

Additionally, the Supreme Court has also indicated that persons generally do not have a Fourth Amendment interest in "physical characteristics ... constantly exposed to the public," such as their facial features or tone of voice.[130] The Supreme Court in *United States v. Dionisio* held that a directive given to a grand jury for a witness to give a voice exemplar was not an infringement of the witness's Fourth Amendment rights. The Court opined,

> In Katz . . . we said that the Fourth Amendment provides no protection for what a person knowingly exposes to the public, even in his own home or office. . . . The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world. [131]

[125] *See, e.g.*, Stephanie Beasley, *Big Brother on the U.S. Border?*, POLITICO (Oct. 9, 2019)
[126] *United States v. Montoya de Hernandez*, 473 U.S. 531, 539–40 n.4 (1985).
[127] *Tabbaa v. Chertoff*, 509 F.3d 89, 99 (2d Cir. 2007).
[128] *Davis v. Mississippi*, 394 U.S. 721, 728 (1969).
[129] *Id.* at 729.
[130] *United States v. Dionisio*, 410 U.S. 1 (1973)
[131] *Id*. at 14 (internal quotations marks omitted)

As such, the practice of collecting biometric information such as facial geometry or walking gait will likely not raise constitutional concerns. In conclusion, current jurisprudence suggests that the current practice of biometric data collection such as the collection and comparison of facial geometry may be considered to be only minimally intrusive at the border and therefore will not likely implicate the Fourth Amendment.

Facial Recognition Software and Privacy:

ICE uses facial recognition to obtain personal information from DMV databases.[132] This can be a home address, license plate number, or more intimate details, like place of birth or whether a foreign passport was used to prove identity.[133] ICE can use this information to decide whom to target for immigration enforcement and to locate the people it has targeted.[134] It can also use DMV databases, primarily the driver license database, to locate specific individuals.[135] 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.[136] The problem with the practice of using facial recognition software to mine the data in DMV databases is that it lacks a governing authority. ICE has admitted that no federal policy governs ICE's ability to access or use DMV data.[137]

Neither Congress nor state legislatures have authorized the development of such a system.[138] For the time being, no one has given ICE explicit authority to mine DMV databases for data, but no one is

[132] Bill Chappell, *Ice Uses Facial Recognition To Sift State Driver's License Records, Researchers Say*, NPR (2019), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers. (last visited Mar 4, 2022).
[133] Audrey Knutson, *Saving Face; The Unconstitutional Use of Facial Recognition on Undocumented Immigrants and Solutions in IP*, 10 IP THEORY 1 (2021).
[134] Bill Chappell *supra*, note 127.
[135] Audrey Knutson *supra*, note 128.
[136] *Id*.
[137] *How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information*, NATIONAL IMMIGRATION LAW CENTER (May 2016), https://www.nilc.org/issues/drivers-licenses/ice-dmvs-share-information/ (last visited Mar 14, 2022).
[138] *Id*.

prohibiting ICE from doing this either.[139] As facial recognition usage develops rapidly, there are very few guidelines in place relating to privacy protections.

Tech giant Amazon is now involved in helping to locate and track undocumented immigrants.[140] Amazon's Ring Doorbell is a video doorbell which allows users to see people who come to the door in real time while also recording visitors.[141] The data is subsequently stored on Amazon's cloud.[142] The Ring app is also currently partnered with more than 400 police departments across America.[143] Audrey Knutson profers concerns that may come up surrounding the rise of such facial recognition software especially for undocumented immigrants:

> These partnerships streamline how Ring video data can be accessed by police, even without warrants. Currently, Ring does not use facial recognition software, but it did file 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. If a match occurs, the person's face can be automatically sent to law enforcement, and the police are able to arrive in minutes. 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. Rekognition has the ability to identify people from afar, a type of technology that immigration officials have voiced interest in for its potential enforcement use on the southern border. Amazon developed Rekognition as a way to analyze images and detect faces on a massive scale.[144]

Facial Recognition and Pushback:

Clearview AI, a facial recognition company based in America, provides software to companies, law enforcement, universities, and individuals.[145] The company's algorithm can match faces to a database

[139] Bill Chappell *supra*, note 127.
[140] Ben Piven, *What Is Amazon's Role In The Us Immigration Crackdown?* MIGRATION | AL JAZEERA (2019), https://www.aljazeera.com/economy/2019/7/16/what-is-amazons-role-in-the-us-immigration-crackdown (last visited Mar 4, 2022).
[141] 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 (last visited, March 4, 2022).
[142] *Id*.
[143] *Id*.
[144] Audrey Knutson *supra*, note 128.
[145] CLEARVIEW AI HOMEPAGE, https://www.clearview.ai/ (last visited Mar 4, 2022).

of more than three billion images indexed from the internet, including social media sites.[146] Clearview has been sued by two immigrant rights groups in California for allegedly violating privacy laws.[147] One of the complaints filed in Alameda county states that, "Clearview has provided thousands of governments, government agencies and private entities access to its database, which they can use to identify people with dissident views, monitor their associations, and track their speech."[148]

The American Civil Liberties Union ("ACLU") has also launched a case against Clearview in Cook County Court in Chicago.[149] The court has denied Clearview's motion to dismiss on the grounds of First Amendment claims.[150] The court noted that:

> The central conflict in this case is the clash between privacy rights and First Amendment protections in an age of ever-more-powerful technology. Defendant Clearview AI, Inc. ("Clearview") used facial recognition technology to capture more than three billion faceprints from publicly available photos on the internet. A faceprint is a biometric identifier used to verify a person's identity. To create a faceprint, Clearview's system scans the photo, measures, and records data such as the shape of the cheekbones and the distance between eyes, nose, and ears, and assigns that data a numerical value. These faceprints are then collected into a database, with faceprints for similar-looking faces clustered together. Clearview sells access to its technology, database, and investigative tools-the "world's best facial-recognition technology combined with the world's largest database of headshots"-by subscription to public and private entities. When a user wants to identify someone, the user uploads a photo. The system then processes the request, finds matches, and returns links to publicly available images on the internet. Often, the linked websites will include additional information about the person identified. The facts recited here are derived from Plaintiffs' Complaint and its exhibits and are accepted as true for purposes of Defendant's motion to dismiss.[151]

The court further held that Clearview's practice of face printing is not entitled to "strict scrutiny" of the speech restraint, which is the highest level of First Amendment protection, but instead should be determined

[146] *Id*.
[147] Irina Ivanova, *Immigrant Rights Groups Sue Facial-Recognition Company Clearview Ai*, CBS NEWS (2021), https://www.cbsnews.com/news/clearview-ai-facial-recognition-sued-mijente-norcal-resist/ (last visited Mar 4, 2022).
[148] *Renderos et al v. Clearview AI, Inc.*, et al. 3:2021cv04572.
[149] *Aclu v. Clearview Ai*, 2021 Ill. Cir. LEXIS 292
[150] *Id*.
[151] *Id*. citing *Kedzie & 103rd Currency Exchange v. Hodge*, 156 Ill. 2d 112, 115 (1993).

under "intermediate scrutiny."[152] This is appropriate because Clearview's actions do not address a matter of public concern, but rather solely serve Clearview in commercial purposes.

In 2008, Illinois passed the Biometric Information Privacy Act ("BIPA"), a law protecting the "biometric identifiers and biometric information" of its residents.[153] Two other states, Texas and Washington, followed suit and passed their own biometric privacy laws.[154] The Illinois law strictly forbids private entities from collecting, capturing, purchasing or otherwise obtaining a person's biometrics, including a scan of their "face geometry," without that person's consent.[155] Violating the BIPA can essentially provide a cause of tort action, and individuals can then sue for damages when such violations occur.[156]

After applying intermediate scrutiny, the court upheld the application of BIPA's opt-in consent requirement to Clearview's face printing.[157] The court then emphasized Illinois' important interests in protecting the "privacy and security" of the public from biometric surveillance by third parties, including the "difficulty in providing meaningful recourse once a person's [biometrics] have been compromised."[158] The court further explained that the opt-in consent requirement is "no greater than necessary" to advance this interest because it "returns control over citizens' biometrics to the individual whose identity could be compromised."[159] In response to Clearview's argument that accommodating BIPA hurts its business model, the court said, "[t]hat is a function of having forged ahead and blindly created billions of faceprints without regard to the legality of that process in all states."[160]

---

[152] *Id*.
[153] Julia D. Alonzo & Brooke G. Gottlieb, *Litigation breeding ground: Illinois' biometric information privacy act*, THE NATIONAL LAW REVIEW, https://www.natlawreview.com/article/litigation-breeding-ground-illinois-biometric-information-privacy-act (last visited Mar 4, 2022).
[154] *Id*.
[155] *Id.*
[156] *Id*.
[157] *Aclu v. Clearview Ai*, *supra*, note 144
[158] *Id*.
[159] *Id*.
[160] *Id*.

The current litigation surrounding privacy rights of immigrants are raising the right questions when it comes to addressing immigrants' rights. Legislations like BIPA would require being substantially fleshed out to protect undocumented immigrants. One possible solution for facial recognition search for immigrants and citizens alike is to create automatic property-like rights to their likeness as offered by Audrey Knutsmen.[161] However, as the paper explains, this solution will face substantial difficulty in regards to its implementation:

> 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." 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 yield 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.[162]

Knutsmen further suggests that the U.S. look to European law for guidance on granting moral rights to a person's face template.[163] Though these suggestions are insightful, it is most likely that the expansion of rights of undocumented immigrants will come through litigation, being driven by advocates and interest groups.

Conclusion:

In the face of exponential advances in technology, American courts have yet to balance the privacy rights of undocumented immigrants with the interest of immigration enforcement. Constitutional violations continue to deprive immigrants of liberty and property, resulting in family separations, heartache, and racial stereotyping at and within the border. Congress has the ultimate Constitutional power to regulate immigration, but it also has a a Constitutional duty to protect the substantive rights of all individuals,

[161] *Audrey Knutson* supra, note 128.
[162] *Id*. (citations omitted)
[163] *Id*.

including those undergoing immigration proceedings. The privacy rights of immigrants have eroded and continue to erode. When the ACLU sued the FBI and the Department of Justice over their use of facial recognition software, Kade Crockford, the director of the Technology for Liberty Program at the ACLU of Massachusetts told CNN, "Technology has outpaced our civil rights."[164] The federal government is continuously expanding the limits with surveillance and privacy invasion, especially at the Mexican border.[165] The framers could have never known the kind of concerns that technology has put upon the rights of people in the United States.

[164] Monica Haider, *ACLU sues federal government over surveillance fromfacial recognition technology*, CNN (Nov. 1, 2019), https://www.cnn.com/2019/11/01/us/aclu-sues-federal-government-over-surveillance-from-facial-recognitiontechnology/index.html (last visited Mar. 4, 2020).
[165] 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/ (last visited, Mar. 4 2022) .