# Untangling The Immigration Enforcement Web

## Basic Information for Advocates About Databases and Information-Sharing Among Federal, State, and Local Agencies

September 2017

National Immigration Law Center

THE NATIONAL IMMIGRATION LAW CENTER is exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. Our mission is grounded in the belief that every American—and aspiring American—should have the opportunity to fulfill their full potential regardless of where they were born or how much money they have. Using our deep expertise in a wide range of issues that affect low-income immigrants' lives, we work with communities, in courtrooms, and with legislatures to help advance policies that create a more just and equitable society for everyone.

# UNTANGLING THE IMMIGRATION ENFORCEMENT WEB

## Basic Information for Advocates about Databases and Information-Sharing Among Federal, State, and Local Agencies

**SEPTEMBER 2017**

Immigrants are caught in a complex and opaque web of databases, related systems, and information-sharing mechanisms that facilitate immigration enforcement and erect barriers to their full participation in economic and social life in the United States. These databases, systems, and mechanisms often depend on the entanglement of state and local law enforcement or licensing agencies with federal immigration and law enforcement agencies.

Advocates have raised many concerns about how these databases, related systems, and information-sharing mechanisms work. President Donald Trump's recent executive orders (EOs) and the U.S. Department of Homeland Security's (DHS's) implementation memorandums will expand immigration enforcement dramatically without due process protections, increase state and local involvement in immigration enforcement, and undermine federal Privacy Act guarantees.

This report doesn't describe all the numerous information-sharing networks and systems that exist, in part because publicly available information is so limited. Given the lack of transparency at

CONTENTS

every level of government and uncertainty about how the executive orders will be implemented, many important questions remain unanswered.

But we begin our inquiry by focusing on a few important issues: the mechanisms of federal entanglement with state and local law enforcement agencies (such as Secure Communities, 287(g), and the National Crime Information Center database); the use of gang databases; the use of mobile devices to capture biometrics, such as fingerprints and photographs, in the field; and driver's license and municipal identification card databases—all of which facilitate immigration enforcement. We also examine the ways in which DHS and the U.S. Department of Justice (DOJ) protect their databases from scrutiny and accountability. Finally, we offer general suggestions on how states and communities can protect their residents.

We hope that the following questions and answers will give immigrants and their advocates a better understanding of (1) how the exchange of data occurs currently, (2) how to evaluate the potential immigration-related risks and benefits of interacting with federal and state authorities, and (3) how to forge strategies and measures that will protect immigrants more effectively.

# How ICE Works with State and Local Officials to Enforce Immigration Law

## What are some mechanisms that facilitate U.S. Immigration and Customs Enforcement (ICE) entanglement with state and local law enforcement?

As described more fully below, the entanglement between ICE and state and local law enforcement occurs through:

**Technological access**

- The Federal Bureau of Investigation's (FBI's) Next Generation Identification (NGI) database and DHS's Automated Biometric Identification System (IDENT) databases are interoperable.[1] This means that, through the Secure Communities (S-Comm) program, fingerprints of an arrested person may be checked against both FBI and DHS databases.
- State and local law enforcement have access to federal databases such as the National Crime Information Center (NCIC) database that contains *civil* immigration information.
- ICE has access to state and regional criminal justice networks and databases that allow the agency to identify individuals who have been arrested and convicted.[2]

**Physical access.** Jail authorities give ICE agents access to jails and lists of arrestees, enabling the agency to target individuals for deportation.

**Transfer of authority to state and local law enforcement.** DHS can give state and local law enforcement agencies authority to enforce civil immigration law under section 287(g) of the Immigration and Nationality Act (INA).

**Collaborative operations among ICE, U.S. Customs and Border Protection (CBP), and state and local law enforcement**

- This may involve joint operations with state and local law enforcement,
- State and local law enforcement may also allow ICE or CBP access to their technology, such as facial recognition technology.

**Informal communications**

- State and local law enforcement officers communicate in an unregulated fashion with ICE agents. For example, police may contact ICE regarding a driver stopped for a traffic infraction if they suspect the driver is not authorized to be in the U.S.
- Law enforcement officers can also report activity they believe to be suspicious to DHS's Homeland Security Investigations (HSI) through a system called FALCON Tipline (FALCON-TL). That information may be shared with ICE agents.[3]

## How does Secure Communities work?

S-Comm is an immigration enforcement program that was administered by DHS from 2008 to 2014 and revived by the Trump administration in 2017.

### Checking arrestees against databases

Under S-Comm, FBI and DHS databases—respectively the Integrated Automated Fingerprint Identification System (IAFIS, which has been replaced by NGI[4]) and the Automated Biometric Identification System (IDENT)—are interoperable,[5] so that fingerprints of arrested people taken at booking on criminal charges are checked automatically against the FBI and DHS databases.

ICE is then notified of any "hit" against its databases and can lodge a detainer against the person who is the subject of the hit, requesting that the jail where the person has been booked hold them for up to 48 hours *after* they would otherwise have been released, so that ICE can pick them up.[6]

### Flaws in S-Comm and its replacement by Priority Enforcement Program

S-Comm has had a disparate impact on people of color, suggesting that many people identified through the system may have been arrested as a result of racial profiling.[7] Local police have frequently stopped Latinos for minor traffic offenses as a pretext for checking their immigration status.[8] And the program has facilitated the deportation of people arrested for minor crimes.[9]

S-Comm generated extensive criticism from law enforcement and community members, as well as a wave of costly lawsuits. Several courts found that keeping people jailed beyond the time that they would normally be released, simply because DHS has requested that they not be released, violates the Fourth Amendment or exceeds DHS's statutory authority.[10] In response, ICE announced in November 2014 that it would implement the Priority Enforcement Program (PEP) in S-Comm's place.[11] PEP purportedly focused on narrower enforcement priorities and, generally, asked that local law enforcement notify immigration enforcement authorities of jailed individuals' impending release dates rather than that their release be delayed (i.e., that their detention be prolonged).[12]

But like S-Comm, PEP relied on the same underlying mechanism whereby arrested individuals' fingerprints are checked against interoperable FBI and DHS databases. Many advocates therefore called the changes cosmetic.[13]

### S-Comm revived by Trump administration

President Trump's executive order of January 25, 2017, titled "Enhancing Public Safety in the Interior of the United States" and DHS's subsequent implementation memorandum had the effect of reviving Secure Communities and dismantling PEP.[14] This will likely revive the problems that caused the Obama administration to scrap S-Comm.

The executive order vastly expands immigration enforcement priorities,[15] increasing the number of people subject to S-Comm interoperability. This makes many more noncitizens vulnerable to being deported, regardless of whether they are formally charged with a crime, have been accused of only a minor infraction, or have charges against them dropped because they are innocent.[16]

### Interoperability between databases in the civil context

In addition to having FBI and DHS database interoperability through S-Comm, DHS has laid the groundwork for interoperability between FBI and DHS databases in the civil context, e.g., in situations where people are being screened for suitability for a job or a license. In 2013, DHS authorized that fingerprints from people who are subject to other FBI background checks be checked against DHS databases "to determine eligibility or suitability for employment, access, or other purposes."[17] Implementation of this authorization would mean that fingerprint checks done in a civil context could put people at risk of immigration enforcement.

## How do 287(g) programs work?

Under INA section 287(g), DHS can enter into memorandums of agreement (MOAs) with state and local law enforcement agencies that allow the latter to enforce federal immigration law either in jails or in the course of performing their regular work.

### "Task force" agreements

Prior to 2012, DHS entered into "task force" agreements with states and localities, which allowed police officers, sheriff's deputies, etc. to enforce immigration law in the field. Abuses abounded, including racial profiling and targeting of people who posed no threat to public safety or had no criminal record.[18]

In response to such abuses, the Obama administration ended the task force 287(g) agreements. DHS also reduced the number of 287(g) jail model agreements significantly, leaving only 38 jail agreements in 16 states.

### Trump administration mandates new 287(g) agreements

Despite the long track record of problems with 287(g), the executive orders that President Trump issued on January 25, 2017—"Enhancing Public Safety in the Interior of the United States"[19] and "Border Security and Immigration Enforcement Improvements"[20]—mandate that DHS enter into 287(g) agreements with state and local officials. The DHS memo implementing the president's executive orders makes clear that both ICE and CBP may enter into these agreements, in the form of jail enforcement, task force, or joint jail enforcement–task force agreements.[21]

As of August 2017, ICE had expanded the number of 287(g) jail model agreements to 61—an increase from 37 in March 2017. They involve law enforcement agencies in 18 states, and many of the new agreements are in Texas.[22] We also expect that new task force model agreements will be entered into soon. CBP has not announced whether it has entered into any 287(g) agreements.

### Expansion of expedited removal authorized

The "border security" executive order and DHS's implementing memorandum also authorize the expansion of "expedited removal." Under expedited removal, with limited exceptions, immigration officers may summarily order the deportation of a person whom they determine is "inadmissible" (to the U.S.) if the person cannot establish that they have been in the U.S. for more than two years. Under current administrative rules, however, "use of expedited removal is limited to undocumented immigrants who are encountered within 100 miles of the border and who cannot, to the satisfaction of an immigration officer, demonstrate that they have continuously

resided in the United States for the 14-day period immediately before apprehension."[23] Expedited removal deprives immigrants of having their case heard in immigration court. Expansion of expedited removal so it may be applied to people who can show they've resided in the U.S. longer than 14 days is not yet in effect; it may not be implemented until an implementation notice about it is published in the Federal Register.

It is unclear whether local jurisdictions that have signed 287(g) agreements will have authority to implement the expanded expedited removal process. That will be of special concern if local jurisdictions enter into 287(g) agreements with CBP.

### Local law enforcement access to DHS technology

Agreements under INA section 287(g) give law enforcement officers access to the DHS technology infrastructure.

- They "receive a DHS email account and access to the necessary DHS systems and associated applications."[24]
- The standard MOA states that use of the infrastructure and DHS/ICE information technology security are set forth in an Interconnection Security Agreement (ISA).[25] But the ISA that entities enter into with ICE is unavailable. A presumably comparable CBP ISA deals with technical issues such as interconnection requirements and system security but does not include any language that protects the rights of people affected by the agreement.[26]

## What other mechanisms give ICE officers access to local arrest records?

The following programs and mechanisms give ICE officers access to local arrest records:

### Criminal Alien Program (CAP)

Through the Criminal Alien Program (CAP), ICE officers are given access to local jails as well as permission to interview people held there. As a result, they are able to target people in jails and prisons, to put them into removal proceedings.[27] ICE is able to identify foreign-born people who are in jail because jail staff give ICE officers access to lists or records indicating who in their jail is foreign-born.[28]

Like S-Comm, CAP encourages racial profiling. A study of CAP shows that when police officers knew that they could check the immigration status of anyone they arrested, because ICE had a presence in the local jail, arrests of Latinos increased.[29]

### State and regional databases

ICE also has access to state, regional, and local criminal justice databases (including in jurisdictions that limit cooperation with ICE) that identify people who have been arrested, who have been involved in the criminal justice system, or whose names are entered in civil databases.[30] For example, in Connecticut, ICE can obtain access to "state DMV [Department of Motor Vehicles] data, court data, probation information, protective orders, boating certifications, hunting and fishing licenses, and other data" through the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) system.[31]

## How do state and local law enforcement officers use the National Crime Information Center (NCIC) database?

NCIC is an FBI database containing, according to the FBI, "an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year."[32] This FBI database is accessible to state and local law enforcement officers so they can check, for example, whether a person pulled over during a traffic stop is wanted by or has an outstanding criminal warrant from another jurisdiction.[33]

### NCIC contains civil records in addition to criminal ones

Despite the FBI's designation of NCIC as a *criminal* database, it also includes *civil* immigration records. These records are currently housed in the NCIC's Immigration Violator File, which, according to the FBI, contains civil immigration records "on criminal aliens whom immigration authorities have deported and aliens with outstanding administrative [i.e., civil] warrants of removal."[34] And it appears that information in the Immigration Violator File also is housed in the NCIC's Wanted Persons File.[35]

But Congress has never authorized inclusion in the NCIC of immigration arrest and deportation records, other than those pertaining to previously deported "criminal aliens."[36] In addition, the President's Task Force on 21st Century Policing recommended in a 2015 report that civil immigration information not be included in the NCIC.[37]

### Police stops based on pretexts and racial profiling a danger

As described below, police officers, via mobile devices, can use a service in the FBI's biometric database (the NGI) called the Repository for Individuals of Special Concern (RISC) to check the NCIC's Immigration Violator File and obtain an almost instantaneous response.

As discussed below, the NCIC also includes a Gang File. State and local law enforcement may use and enter information into the Gang File, as well as into other NCIC files, such as the Wanted Persons File. In addition, the Interstate Identification Index (III), "which contains automated criminal history record information, is accessible through the same network as NCIC."[38]

Access to immigration-related information in the NCIC gives police officers an opportunity to inform ICE that they have stopped a person about whom there is information in the NCIC database. As more local law enforcement agencies enter into new 287(g) task force agreements, more local police officers will be able to use NCIC information specifically for immigration enforcement. A predictable result will be that some officers will use pretexts and racial profiling to stop more people—especially people of color—specifically to check whether there is information about them in the NCIC.

### Shocking level of inaccuracies in NCIC data

The FBI has not evaluated the inclusion of civil immigration information in NCIC. Independent evaluations, in contrast, have revealed shocking levels of inaccuracies in NCIC data. Using data obtained through a Freedom of Information Act request, a 2005 Migration Policy Institute study found that "[f]orty-two percent

of all NCIC immigration hits in response to a police query were 'false positives,' where DHS was unable to confirm that the individual was an actual immigration violator."[39]

## Why does civil immigration information appear in responses to FBI criminal background checks received by state and local law enforcement and state and local agencies?

When someone is arrested on a criminal charge and fingerprinted, their fingerprints are sent to the FBI for a criminal background check.[40] In addition, many jobs and professional license applications require FBI criminal background checks to establish that applicants have not committed a crime that would disqualify them for the job or license.[41] These fingerprints are taken for noncriminal justice (i.e., civil) purposes.

In both the criminal and civil contexts, fingerprints are submitted to the FBI through a designated state criminal justice agency. A "rap sheet" is returned to that state criminal justice agency, and the results are transmitted to other relevant agencies.[42] That rap sheet often includes civil immigration information, even though, under federal law, an FBI check for criminal history should include information *only* about the person's past interactions with the criminal justice system.[43]

Nevertheless, advocates report that individuals' criminal history records, after the FBI has completed a background check on them, often include information on civil, administrative warrants, as well as civil immigration arrests and prior deportation orders.

## Does ICE conduct joint operations with state and local law enforcement and use their technology?

Yes—ICE conducts joint operations with state and local law enforcement and uses their technology. For example, ICE partnered with police in Escondido, Calif., to conduct driving-under-the-influence (DUI)/immigration checkpoints in a project called Operation Joint Effort.[44] And as described below, police and ICE have carried out joint operations as part of ICE's Criminal Alien Removal Initiative (CARI).

During recent joint operations with local police purportedly intended to result in criminal arrests of targeted people on gang and drug charges, ICE's Homeland Security Investigations division has arrested bystanders on immigration charges. ICE has made the immigration arrests during these operations despite the local cooperating police agencies' stated commitment not to participate in immigration enforcement.[45]

It is not clear if ICE has its own facial recognition technology at this time, though CBP has begun to use facial recognition exit technology in certain U.S. airports.[46] But state and local police use such technology, and ICE has access to it. For example, mobile facial recognition technology used by San Diego law enforcement is available to "[t]wenty-five local, state and federal law enforcement agencies—including U.S. Immigration and Customs Enforcement, the Border Patrol, the San Diego County Sheriff's Department and San Diego State University."[47]

As described below, ICE agents also have asked state DMVs to use their facial recognition technology to assist them in immigration enforcement. And the FBI has

agreements with at least 16 states that allow searches of their driver's license photos through the states' facial recognition systems.[48]

## What can you do to minimize ICE's entanglement with state and local law enforcement?

To minimize ICE's entanglement with state and local law enforcement, consider taking some or all of the following actions.

**Advocate for laws, resolutions, or policies that:**

- Limit ICE access to jails or to lists of people confined in local jails.
- Prohibit using state or local resources to enforce civil immigration law.
- Limit the collection and recording of information that might reveal a person's immigration status, and limit the disclosure of personal information for purposes that aren't directly related to administering a local program or service.
- Limit joint operations with ICE.
- Require notice where people's personal information, including their address or immigration status, is shared with federal agencies.
- Require information-sharing agreements with federal agencies to prohibit use of information for immigration enforcement purposes.
- Prohibit questioning of arrested people about their place of birth.

**Limit joint operations with ICE.** Advocate against your community or state entering into a 287(g) agreement with ICE or CBP.

**Monitor.** Track incidents of racial profiling.

**Complain.** File complaints about racial profiling with local, state and federal civil rights authorities.

**Sue.** File lawsuits challenging your city's actions if law enforcement authorities hold people in jail beyond when they otherwise would be released, since such policies could violate the Fourth Amendment to the Constitution or other civil rights laws.

**Communicate.** Seek media coverage of people whose experiences humanize this issue, to show the harmful consequences to real people (neighbors, fathers and mothers, friends) of data-sharing.

# How Local, State, and Federal Gang Databases Interact, and How They Harm Immigrants

## How are individuals identified as gang members?

The federal government, states, and localities have created databases, described below, that label, stigmatize, and punish many citizens and noncitizens as "gang members." Information in these databases, which are notoriously inaccurate, is shared among law enforcement agencies at all levels of government. One inevitable result of this sharing is that if one database contains erroneous data, the errors will transfer to other databases as well.

## What are the consequences for immigrants identified as gang members?

For an immigrant, being identified as a gang member has dramatic consequences. Gang members have long been considered a priority for immigration enforcement. Being a gang member can make the person ineligible for Deferred Action for Childhood Arrivals (DACA) or other discretionary immigration relief.[49] Merely being accused of gang membership, no matter how vague the accusation, can lead to the accused person being denied bond in an immigration case or being sentenced to enhanced punishment in a criminal case.[50]

## How do state and federal gang databases interact?

Gang-related databases used by immigration and other law enforcement agencies in the U.S. include GangNET, ICEGangs, and the NCIC Gang File, in addition to gang databases maintained by different state and local agencies.

### GangNET

Commercial intranet-linked software called GangNET appears to be critical for gang information collection, storage, and sharing by states and the federal government.[51] GangNET offers a database with information on and photos of individuals and gangs, data analysis, facial recognition software, mapping, a field interview form, and a watch list. Using a single command, agencies can simultaneously search their own GangNET system and a network of GangNET systems in other states and federal agencies.[52]

The GangNET software is operational in many states,[53] as well as in Canada. ICE, the FBI, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are also connected to it and able to share information in real time.[54] The GangNET system allows data collection from a variety of law enforcement personnel, such as officers in the field, gang units, patrol officers, corrections officers, and any other law enforcement entity.[55]

### ICEGangs

ICE created its own gang database called ICEGangs in 2010, to serve as a repository of personal information about suspected or confirmed gang members and

"associates," as well as for information on gang activities. ICEGangs was based on GangNET software and was "tailored to include immigration status–related information."[56] Agents were able use ICEGangs to gain access to other databases that use GangNET.[57]

In an April 2017 practice advisory, the Immigrant Legal Resource Center reports that ICE stopped using ICEGangs in 2016 because ICE agents were relying on other case management databases.[58] ICE issued a privacy impact assessment (PIA) on ICEGangs in 2010 that describes the database.[59] But ICE has not issued any public notice indicating that it no longer uses ICEGangs and has not issued any documents disclosing how and when it collects and shares information pertaining to suspected gang membership.

**NCIC Gang File**

The Gang File in the FBI's NCIC database provides information to state and local law enforcement, as well as to ICE.[60] The criteria for inserting information about a person in the Gang File (formerly the Violent Gang and Terrorist Organizations File, or VGTOF) include that the person has admitted to being a gang member, that informants have identified the person as a gang member, or that the person has spent time in a gang's "area."[61] State and local law enforcement officers may enter names into the Gang File, often without their submissions being subject to restrictions or checks for accuracy.[62]

## What's wrong with gang databases?

The existence and use of databases containing information about gangs and their members can be difficult to challenge, because they were created, ostensibly, to combat gang violence. But gang databases are subject to few rules and little accountability. And, historically, people who are listed in gang databases have had few options for contesting their inclusion in them. Moreover, as noted below, gang databases have been shown to contain listings for people who clearly and unequivocally should never have been listed—infants, for example.


Whether someone is listed in a gang database is often at the discretion of local law enforcement, and police reliance on racial stereotypes can lead to the disproportionate inclusion of people of color in the databases.[63] And, as noted above, when erroneous information is entered into one gang database, it can

easily infect other gang databases with inaccuracies, because of information-sharing practices.

An August 2016 report by the California State Auditor about CalGang, California's version of GangNET, exposes serious problems.[64] As the report explains, CalGang plays an important role in populating federal gang databases, and its data is shared with other states, but it operates without oversight, has unsubstantiated and incorrect information, and does little to protect public safety. Here are some of the report's findings:

- Some groups and individuals didn't meet the criteria for inclusion in CalGang.[65]
- In a shocking indication of the database's inaccuracy, the auditor found that it included listings for 42 babies less than a year old, 28 of whom supposedly admitted to being gang members.[66]
- Juveniles weren't notified of their inclusion in CalGangs—even though, under state law, juveniles and their parents must be notified before they are listed—and therefore couldn't contest having been listed.[67]
- Data wasn't properly purged as required by federal and state guidelines, and the database included "illogical" purge dates, sometimes more than 100 years in the future. As a result, people remained listed in the database erroneously when there was no evidence that they were part of a gang.[68]

## What can you do?

- Find out about the gang databases in your state and community, the rules for being listed in the databases, and how to challenge an individual's inclusion.
- Gather stories about the damaging collateral consequences for people whose names are included in a gang database.
- Ask for audits of state and local gang databases like the one conducted in California.
- Advocate for policies that provide access to information about inclusion in the databases and methods to challenge inclusion.
- Challenge wrongful inclusion through litigation and in immigration court.

# How DHS Agencies and State and Local Law Enforcement Use Mobile Biometrics Devices to Identify People for Immigration Enforcement Purposes

## Do ICE, CBP, and local law enforcement use mobile devices to collect biometric information, such as fingerprints, photographs and iris scans, in the field?

Yes. ICE, CBP, and local law enforcement have at their disposal technology that enables them to use mobile devices to fingerprint and photograph people in the field and to check their biometrics against federal databases, including NGI and IDENT.

As ICE explains in a 2012 privacy impact assessment, "ICE uses IDENT to enroll biometrics about individuals encountered and/or arrested for criminal or immigration violations through the course of an investigation, arrest, booking, detention, and/or removal from the United States."[69] The PIA made clear that IDENT includes biometrics and photographs collected with mobile devices.[70]

For example, in 2016 two companies, NEC and Government Acquisitions, announced that NEC had delivered NEC's NeoScan45 mobile fingerprint capture devices to ICE.[71] The device will "capture … up to 10 fingerprints, both rolls and flats, and its multi-operating system support[s] … both iOS and Android" devices.[72]

And ICE uses an app called Eagle Direct Identification Environment (EDDIE) to fingerprint and photograph people in the field.[73] It "gives all 12,000 ICE officers the ability to collect biometric data in the field using their agency-issued Apple iPhone and a pocket-size Bluetooth-connected fingerprint scanner."[74]

Likewise, CBP officers use mobile devices to collect fingerprints, photographs, and iris scans.[75]

The FBI has provided law enforcement with expanded access to civil immigration information in the NCIC via mobile devices used in the field:

- The Repository for Individuals of Special Concern (RISC) is an NGI service, launched in 2011, that allows law enforcement to take fingerprints in the field using mobile devices and to check them against the NGI databases.[76] The RISC offers "rapid search, with response times of less than 10 seconds."[77]
- In 2012, the FBI added the NCIC's Immigration Violator File to the files checked through the RISC.[78]

## Who gets fingerprinted and photographed in the field?

ICE agents fingerprint and photograph people "encountered" when they are conducting investigations, not only people whom they have targeted for arrest or who have been arrested.[79] This can result in "collateral" arrests, as well as in the retention of those biometrics in databases even for people who are not arrested.

## What happens to those fingerprints and photographs?

In general, fingerprints taken during ICE "encounters" are sent to both NGI and IDENT. The DHS Office of Inspector General explained that, "In 2008, according to officials we interviewed, ICE management directed its employees to send all fingerprints collected during immigration enforcement encounters to both IDENT and the FBI repository (at the time, the Integrated Automated Fingerprint Identification System or IAFIS, now NGI)."[80]

## Does ICE cooperate with state and local law enforcement in using mobile technology?

Yes. As mentioned previously, the mobile facial recognition technology used by San Diego law enforcement is available to ICE, the Border Patrol, as well as other local, state, and federal law enforcement agencies.

In 2014, *The Nation* magazine reported:

> The Criminal Alien Removal Initiative, which began in the spring of 2012, was one of the formal programs inside ICE designed to carry out this goal [of deporting noncitizens who had criminal convictions]. But in New Orleans, CARI morphed into an aggressive initiative characterized by coordination between ICE and local police, and the use of mobile fingerprinting devices wielded against seemingly random groups of Latino residents. Critics in Louisiana have dubbed ICE's practices "stop-and-frisk for Latinos." Immigrants report being detained at checkpoint-style operations at apartment complexes, grocery stores, soccer fields and laundromats.[81]

And the Congress of Day Laborers reported:

> Organizers heard an increasing number of reports about New Orleans cops pulling over Latino drivers for minor offenses like failing to use a turn signal and then calling ICE agents to the scene. Immigrants reported that agents were entering their homes without permission, in a few instances after unlocking doors with confiscated keys. Agents rounded up whole groups of people at Bible study groups, soccer fields and other public spaces in Latino neighborhoods—and used the fingerprinting machines to figure out who had a criminal record.[82]

## What's wrong with ICE's reliance on mobile devices in the field?

Mobile devices are used without any governing rules or accountability and result in searches of individuals without adherence to legal standards such as probable cause and in violation of the Fourth Amendment. For example, according to an article by the Center for Investigative Reporting, an ICE agent using the San Diego mobile facial recognition system wrote in a testimonial that

> his "'spidy [sic] senses' were tingling" about the immigration status of a neighbor of the person he was pursuing.
>
> He decided to run the man's picture through the facial recognition software. The agent discovered the man was in the country illegally and had a 2003 DUI conviction in San Diego.[83]

Reliance on "spidey senses" encourages racial profiling and is not a lawful substitute for probable or reasonable cause.

## What can you do?

- File complaints with federal civil rights agencies if ICE agents use mobile devices to take fingerprints or photographs of people in the field, especially if those people are not arrested on immigration charges.
- Challenge in immigration court the arrests of people stopped without probable cause, who were then identified with the use of mobile devices.
- Advise immigrants to object to, and not to consent to, their biometrics being taken in the field with mobile devices.
- Collect stories about ICE's use of mobile devices to take biometrics.
- Work with allies in the privacy rights community to challenge the use of mobile devices to take biometrics.

# How ICE Uses State Driver's License Databases for Immigration Enforcement Purposes

## Why are immigrants and states concerned about DHS's use of information in state department of motor vehicle (DMV) databases?

Currently, 12 states plus the District of Columbia and Puerto Rico issue licenses to drivers regardless of their immigration status.[84] Licenses that do not satisfy the federal REAL ID Act criteria are marked as not acceptable for federal purposes and are distinguishable from REAL ID–compliant licenses in appearance. Rules vary, but in some states lawfully present immigrants and/or citizens may also have licenses that are not REAL ID–compliant.

Drivers with marked licenses may fear that ICE will use information they provided in obtaining the licenses, or the fact that they have the licenses, in identifying undocumented immigrants or other noncitizens for deportation. And states may fear that ICE's use of their database for immigration enforcement purposes will deter immigrants from seeking the license, and will undermine their public safety interest in expanding access to driver's licenses.

## Can ICE obtain information from DMV databases?

Yes. Local, state, and federal law enforcement agencies, including ICE, routinely have relied upon DMV databases to obtain information, such as addresses, on citizens and immigrants alike.[85] The fact that ICE, like other law enforcement agencies, may obtain DMV information is not surprising or unusual.

But this does not mean that ICE has unfettered direct access to DMV databases or that it can collect information indiscriminately, such as obtaining the name of every driver who has a marked license.

## How does ICE obtain information from DMV databases, and what limits govern its access?

ICE has admitted that no federal policy governs how and when it obtains information from DMVs.[86] As revealed in a response to a Freedom of Information Act (FOIA) request to DHS and ICE submitted by the National Immigration Law Center and subsequent litigation, as well as a public records request in California, ICE gains access to DMV information through sophisticated technological means as well as informal communications.[87]

ICE can use an automated, state-owned network called Nlets to obtain certain information, such as a person's basic identity and physical characteristics, provided in driver's license applications as well as in subsequent driver history (e.g., records of accidents and traffic offenses).[88] If ICE is interested in particular individuals, it can use this information to locate them, but Nlets fields do not include a driver's immigration status or whether the driver obtained a marked license. Nlets has a

driver's license photo-sharing system to which ICE has access, but not all states choose to participate in it.[89]

ICE also has access to driver's license information through state criminal justice networks. For example, ICE has access to driver's license information through Connecticut's COLLECT system.[90] In addition, ICE Enforcement and Removal Operations (ERO) field offices are in regular email and other communication with state DMVs outside of the formal automated networks. In ways that are ad hoc and decentralized, ERO agents have informal relationships with state DMVs that allow them to request and obtain information and photos in driver's license and vehicle registration databases and to collaborate with DMVs in immigration enforcement.[91]

In addition, the FBI has agreements with at least 16 states to allow searches of their driver's license photographs through the states' facial recognition systems.[92] This may provide an additional avenue for DHS access to photos in some state systems.

## How has ICE used DMV records and collaborated with state DMVs in immigration enforcement?

ICE has used DMV records to locate individuals for immigration enforcement purposes and has used the DMVs' technological capacities, such as facial recognition software, to identify and locate targets. In some instances, DMV employees have collaborated with ICE in immigration enforcement by drawing individuals to a DMV office so that ICE can arrest them. DMV employees have sometimes reported people they merely suspect of being undocumented to ICE, often on the basis of racial profiling.[93]

ICE has also asked DMVs to "run" license plates at particular addresses in order to determine the identities of residents there.[94]

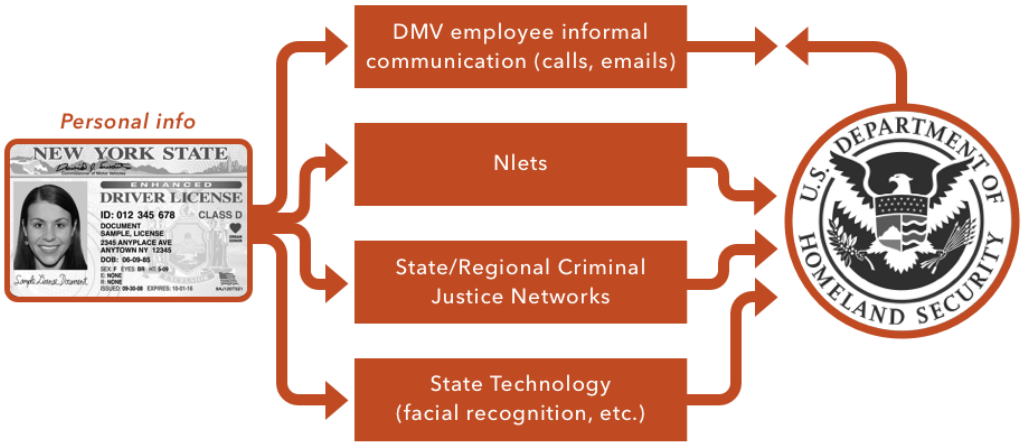
Through a public records request,[95] the ACLU of Vermont obtained documents that reveal an absence of standards regarding when the Vermont DMV makes a referral to ICE for a possible immigration violation;[96] ICE soliciting cases from the DMV or asking to do a drive-by;[97] the DMV asking ICE to check for deportation orders or warrants or for other information, including in cases where there is no driver's license violation;[98] the DMV and ICE collaborating in using a DMV appointment as a means to arrest a person for immigration violations;[99] and ICE urging that certain people be arrested and fingerprinted for state criminal charges so ICE will be notified about them (likely a reference to Secure Communities).[100]

## Can ICE obtain information about *everyone* who has a license that is not REAL ID–compliant?

ICE denies that it "trolls" DMV records to identify enforcement targets.[101] And automated systems such as Nlets do not allow bulk searches using a common field such as the type of license. But there are a few instances where ICE has sought bulk records. For example, DHS has asked state DMVs for information about people with temporary visas in order to identify people who could be deported.[102]

ICE's mechanisms of obtaining DMV records through informal means and the lack of any sort of agency-wide policy leave open the possibility that ICE will seek bulk records. This creates an opportunity for advocacy on the state level. States have

determined that issuing driver's licenses to their residents makes their communities and roads safer and reduces insurance costs over time; they have an interest in imposing limits on ICE's ability to obtain bulk information.




## What can you do to keep DMV records from being used for immigration enforcement?

### Know your state's laws

Many states' driver's license laws include privacy and antidiscrimination provisions, and other protections. You should review your state's existing laws or policies to identify any provisions that:

- protect confidentiality of information provided to obtain a driver's license;
- limit the disclosure of that information;
- prohibit discrimination against holders of those licenses or IDs;
- clarify that no assumptions about a person's immigration status should be made based on the fact that they hold a particular kind of license or ID.

You should also find out whether there are any exceptions to these state rules and policies and, if there are, what they are.

### Find out how your state provides drivers' information to ICE or other federal agencies

You should try to:

- Learn how and under what circumstances ICE and other law enforcement agencies use criminal justice networks to obtain driver's license information in your state. This may entail meeting with state officials or submitting a public records request.
- Research whether your state shares driver's license photographs with ICE and other law enforcement agencies or uses facial recognition technology on ICE's behalf.

- Advocate that your state decline to respond to requests from the FBI or DHS to run face-recognition searches against its DMV database for immigration enforcement purposes.

**Seek additional protections, if necessary**

If you need to seek additional protections from your state legislature, you can advocate to:

- Protect against licenses or state ID cards being used as evidence of immigration status. This protection will help ensure that law enforcement officers do not use a marked license as an excuse to take steps that may lead to its holder being detained or deported by immigration authorities.
- Make sure that application procedures do not require applicants to attest that their presence in the U.S. is unlawful.
- Include in state laws and regulations antidiscrimination provisions that prohibit disparate treatment of people based on the type of driver's license they have.
- Set limits on wholesale or bulk disclosure of information, such as instituting a requirement for particularized requests, probable cause, or judicially authorized criminal warrants before information may be disclosed.
- Advocate for policies that prohibit sharing of DMV information for immigration enforcement purposes.

# How Cities Can Protect Against ICE Using Municipal Identification Cards for Immigration Enforcement

## Why do cities issue municipal ID cards?

Many cities issue municipal IDs that are available to residents regardless of their citizenship or immigration status.[103] In some cities, nonprofit or faith organizations issue IDs. These ID cards help many residents who may lack current proof of identity. This includes not only immigrants, but survivors of domestic violence or disaster, homeless people, seniors, and transgender residents.

## Can ICE obtain information provided in municipal ID applications?

Municipal IDs are creatures of state and local laws. The rules about the documents that must be submitted to establish identity or residency, the retention of those documents, and which individuals or agencies may have access to them depend on state and local laws and policies.[104]

No federal law requires municipalities to collect or retain specific information or to grant ICE access to their ID databases. ICE does not have access to municipal ID records through Nlets or any other automated system. But we have seen attempts to challenge local laws and policies regarding municipal ID confidentiality protections:

- In New Haven, Conn., private citizens who attempted to obtain information provided in municipal ID applications were denied access as a matter of public safety.[105]
- In New York, after the presidential election, two Republican assembly members challenged New York City's plan to destroy documents used to obtain the IDs, and obtained a temporary order stopping the destruction.[106] But in April 2016, the state court ruled in favor of the city, granting it permission to not retain personal documents used in the application process, such as copies of foreign passports.[107] In addition, the city revised its protocol and stopped retaining for any period of time the underlying application documents, to protect the privacy and confidentiality of applicants.[108]

## What can you do to prevent municipal ID records from being used for immigration enforcement?

### Know your city and state laws

Review existing laws or policies to identify or begin to advocate for any provisions that:

- protect confidentiality of information provided to obtain a municipal ID;
- limit retention of documents used to obtain IDs;
- limit the disclosure of information provided to obtain IDs;

- prohibit discrimination against holders of municipal IDs; and
- provide that no assumptions about a person's immigration status should be made based on the fact that the person has a municipal ID.

**Advocate for confidentiality and antidisclosure protections with respect to municipal IDs**

Advocate for policies that protect privacy. For example:

- Unless required by law, don't ask for, record, or retain information that may be used to reveal a person's immigration status.
- Ensure that information provided to obtain a municipal ID may be used only to determine eligibility for the ID.
- Set limits on preventing wholesale or bulk disclosure of information, such as a requirement for particularized requests, probable cause, or judicially authorized criminal warrants before information may be disclosed.

**Make municipal IDs attractive and available both to immigrants and to U.S. citizens**

- Ensure that the municipal ID confers broad benefits—e.g., discounts at grocery stores and pharmacies, free membership at cultural institutions, or the ability to use it as a public library or debit card—that can attract diverse applicants.[109]
- Conduct outreach to populations that may not have ready access to existing forms of ID, such as homeless people or low-income seniors.
- Appeal to your community's values with respect to preventing government overreach and discrimination against immigrants or other residents.[110]

# How Federal Agencies Protect Their Databases from Scrutiny and Accountability

## What role does the Privacy Act play with respect to federal records systems?

According to the U.S. Department of Justice, the Privacy Act of 1974 "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[111]

## What is a system of records?

The DOJ describes a system of records as "a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual."[112] For example, DHS's biometric database, IDENT, is a system of records, as is the FBI's biometric database, NGI.

## How does the Privacy Act prevent information about specific people from being disclosed?

The Privacy Act provides that records about citizens and lawful permanent residents may not be disclosed without their written consent, subject to 12 statutory exceptions. The act also gives citizens and lawful permanent residents the right to obtain access to, and to amend, their records.[113]

## Are federal agencies required to disclose information about their databases?

Yes. The Privacy Act of 1974 requires federal agencies to publish System of Records Notices (SORNs) in the Federal Register.[114] In addition, the E-Government Act of 2002 requires federal agencies to conduct privacy impact assessments if their systems collect and disseminate personally identifiable information.[115] Such an assessment notifies the public of what personally identifiable information is being collected in records systems and how it will be used and shared.[116]

## Does the Privacy Act allow federal agencies to declare that their databases are exempt from Privacy Act protections?

Yes. The Privacy Act allows agencies to declare their records exempt from the Privacy Act for law enforcement and other reasons.[117] For example, DHS exempted its ICEGangs database from the notification, access, and amendment procedures of the Privacy Act, leaving potentially affected people with only the very limited remedy of requesting (but not being entitled to) a record by providing specific information about the record.[118] Likewise, the DOJ exempted the NCIC database from the Privacy Act's accuracy and reliability requirements.[119]

As a result of such self-declared exemptions from Privacy Act protections, citizens and others may not know that their records are included in federal databases or shared with other agencies, and often they have little or no way to correct errors that may directly affect them.

## Is there a comprehensive list of all DHS databases in which immigration information is stored?

No. Multiple SORNs must be reviewed to determine which databases store immigration-related information. This would be a massive undertaking, and it would be very difficult to obtain a comprehensive list of the databases or to learn precisely how they work and how they share information.

## Do the DOJ and DHS SORNs provide timely and complete information about the agencies' databases?

Not always. There are often substantial delays in issuing SORNs, so that systems are up and running before the public is notified. For example, the DOJ issued a SORN for its vast biometric database, NGI, years after its development began.[120]

- Immigrants' fingerprints are stored in the NGI database when they are arrested, fingerprinted with mobile devices, or apply for immigration benefits. And, as described above, NGI is interoperable with DHS's biometric database, IDENT.
- DHS is in the process of replacing IDENT with a vastly expanded biometric database called Homeland Advanced Recognition Technology (HART).[121] Little public information is available about HART, and DHS has not published a SORN about its operation.
- The SORNs tend to leave many questions unanswered. Advocates are forced to rely on FOIA requests and litigation to gain an understanding of databases and information-sharing systems about which information should be available to the public. Although such FOIA requests have uncovered critical information, they are burdensome, time-consuming and expensive, and the results are extremely slow to obtain, and often incomplete. In addition, the Trump administration is now withholding information that previously could be obtained through FOIA requests.[122]

## How is DHS expanding its technological ability to engage in enforcement activities without transparency or oversight?

In 2016, ICE established a new information technology system called Investigative Case Management (ICM).[123] According to *The Intercept*, "ICM allows ICE agents to access a vast 'ecosystem' of data to facilitate immigration officials in both discovering targets and then creating and administering cases against them."[124] Through ICM, users will have access to a wide range of databases, information systems, and commercially available information, creating a "network of interconnected databases."[125] Despite the critical role that ICM will play in immigration enforcement, DHS is relying on a 2010 SORN, issued long before ICM was created, as its authority to create this system.[126]

An opaque, complex, and uncritical 2016 ICE privacy impact assessment describes a system that, in reality, lacks meaningful mechanisms to ensure that its information is accurate, complete and timely, and that people affected by it have notice of or the ability to correct erroneous information. In addition, ICM is not subject to effective and independent reviews to ensure accountability.[127]

## How has the "Enhancing Public Safety in the Interior of the United States" executive order issued January 25, 2017, reduced Privacy Act protections for immigrants?

### Agencies ordered to exclude non–U.S. citizens and non–permanent residents from Privacy Act protections

The Privacy Act, by its terms, covers U.S. citizens and lawful permanent residents.[128] But for years, DHS and other federal agencies applied its provisions to all non–U.S. citizens, treating their records as "mixed records" subject to the Privacy Act's provisions.[129] DHS recognized the "inherent difficulties" in determining people's citizenship and immigration status, which change over time.[130]

The Jan. 25, 2017, executive order on interior enforcement changes this. Section 14 of the order provides that "[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[131]

### Order affects many immigrants authorized to be in the U.S.

The Privacy Act provision doesn't affect only undocumented immigrants. It also excludes several groups of lawfully present people, such as those with nonimmigrant visas, refugees and asylum-seekers, from its protections. The change to Privacy Act coverage dictated by section 14 of the Jan. 25 executive order could have broader implications. DHS will no doubt feel more empowered to disseminate information—regardless of its accuracy—about immigrants and won't need to account for any sharing of data. In addition, many immigrants may not be able to obtain access to or correct their records.

Public dissemination of information about immigrants could expose private information about them and endanger them. But the provision of the Jan. 25 order that affects how agencies are to implement the Privacy Act does not alter or undermine other federal and state laws that protect a person's information.

### Freedom of Information Act (FOIA) and Fair Information Practice Principles (FIPP)

Despite the Jan. 25 order, immigrants will have access to their records through the Freedom of Information Act, which covers "persons," not only citizens or lawful permanent residents. But FOIA does not provide a mechanism for people to correct records that are erroneous.[132]

The DHS Privacy Office recently issued a guidance emphasizing that DHS's ability to share information is limited by Fair Information Practice Principles (FIPPs). These principles—transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing—apply to "all persons, regardless of immigration

status."[133] Unfortunately, the guidance does not offer a remedy to people affected by violations of the FIPPS.

### Privacy Act provision in executive order will be hard to administer

The provision in Trump's Jan. 25 executive order that affects Privacy Act implementation with respect to noncitizens will be difficult to administer. Any dissemination of information would have to distinguish between (1) citizens and lawful permanent residents and (2) other non-U.S. persons. That's a complicated task, particularly because immigration statuses change. Errors are likely, particularly if local law enforcement officers operating under the authority of 287(g) agreements also have the ability to disseminate information.

DHS's ability to disseminate personal information is limited by other federal and state laws, as well as the constitutional right to privacy.

## How do other provisions of the Jan. 25 executive orders affect the privacy and due process rights of immigrants?

### Victims of Immigration Crime Engagement (VOICE) and DHS-Victim Information and Notification Exchange (DHS-VINE)

The interior enforcement executive order and the DHS memorandum implementing it provide that a Victims of Immigration Crime Engagement (VOICE) office will be created within ICE to act as a "programmatic liaison between ICE and the known victims of crimes committed by removable aliens." The memorandum authorizes providing information "about the offender, including the offender's immigration status and custody status."[134]

In April 2017, DHS officially launched VOICE and announced the creation of the DHS-Victim Information and Notification Exchange (DHS-VINE)—"a free, confidential service that provides crime victims/witnesses, their family members, and victim advocates confidential notification of changes in custody status."[135] DHS-VINElink, the online portal to DHS-VINE, allows people to search for immigration detainees (i.e., people who are in civil immigration system custody) and to be notified of custody changes, and to search for people in state (i.e., criminal system) custody and to be notified of custody changes.[136] DHS-VINElink builds on a criminal system victim notification network called VINE.[137]

### New policies and mechanisms violate privacy and due process rights

The executive order, implementation memorandum, VOICE, and DHS-VINE *violate the privacy and due process rights of non–U.S. citizens*. They target noncitizens who have not been convicted of crimes or who have been charged with or convicted of minor crimes, including traffic offenses, and make no distinction between noncitizens who are covered by the Privacy Act and those who are not.

Even more disturbing, information in the DHS-VINE system is not limited to information about people charged with or convicted of crimes. When it was first launched, it included the names of scores of children (including babies, as well as unaccompanied minors in group homes).[138] DHS called this a "lapse in privacy protocols."[139] VINE also includes information on detained people who have sought immigration status as victims of crimes, including human trafficking, even though, under federal law, such information is supposed to be confidential.[140]

And, despite its name and DHS's description of the system, DHS-VINE includes information about people who have no criminal history at all, including asylum-seekers.[141] This is consistent with the Trump administration's ongoing efforts to criminalize immigrants.

**Executive orders mandate that certain information be publicized**

Several provisions of the Jan. 25 interior and border enforcement executive orders require that certain information be publicized: (1) information about crimes committed by immigrants in locales where local law enforcement did not accede to ICE requests ("detainers") that certain people be held in jail beyond the time when they would normally be released, (2) information about incarcerated noncitizens, and (3) information about noncitizens apprehended near the southern border.[142]

The memorandums implementing these provisions do not specifically authorize release of names or other personally identifiable information as part of the reporting requirements.[143] But the Trump administration has made clear its intention to portray immigrants as threats to public safety, and to discredit and pressure localities that have not honored ICE detainers. DHS was forced to suspend issuance of reports identifying jurisdictions that did not honor ICE detainers, because the first reports it issued were wildly inaccurate and soundly criticized by local law enforcement agencies.[144]

## Do the interior and border enforcement executive orders expand information-sharing between different agencies within DHS or with other law enforcement agencies?

While the executive orders certainly affect the privacy of personal information, they do not necessarily mean that information provided for one purpose, such as obtaining an immigration benefit, is more likely to be shared for immigration enforcement purposes. But we can't yet be sure about this, as the absence of safeguards may make it easier to share information.

ICE already has access to information in other DHS databases, and information-sharing among DHS, DOJ, and other law enforcement agencies is already allowed as a "routine use" in many SORNs.[145] In addition, DHS is considered one agency, and—in the absence of specific restrictions[146]—information may be shared within its components,

In addition, as described above, many federal databases affecting immigrants are already exempt from the Privacy Act's protections for law enforcement and other reasons.[147]

## Do the executive orders allow across-the-board dissemination of personal information about immigrants in all circumstances?

No. Specific statutory provisions continue to protect the privacy of information about immigrants and citizens in various contexts. For example:

- Section 6103 of the Internal Revenue Code states that "returns and return information shall be confidential." Return information includes, among other things, "a taxpayer's identity."[148] That section protects the privacy of people who file a tax return using an Individual Taxpayer Identification Number (ITIN).

- Similarly, 42 USC 1396a(a)(7) limits the use and disclosure of information pertaining to Medicaid applicants and recipients.[149]
- The Judicial Redress Act of 2015 provides Privacy Act protections to European Union citizens.[150]

## What can you do to protect the privacy of personal information?

- Learn about particular statutes that protect the privacy of information pertaining to benefit recipients, students, license-holders, and other state and local programs or services.
- Advocate for state statutes that protect *everyone's* privacy and that limit collection, recording, use, and disclosure of information about applicants for or recipients of programs or services.
- Work with privacy and civil rights groups that advocate to protect personal information from disclosure.
- Challenge any public dissemination by DHS of immigrants' personal information.
- Advocate that states and localities make applying Privacy Act standards to all noncitizens a condition of any information-sharing agreements.

# Glossary

**287(g).** A section of the Immigration and Nationality Act that allows the U.S. Department of Homeland Security to enter into agreements with state and local law enforcement agencies to allow them to enforce federal immigration law, either in jails through jail enforcement agreements or in the course of their regular work through task force agreements.

**ATF.** *See* Bureau of Alcohol, Tobacco, Firearms and Explosives.

**Automated Biometric Identification System (IDENT).** The central Department of Homeland Security–wide system for storage and processing of biometric and associated biographic information.

**Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).** Law enforcement agency within the U.S. Department of Justice.

**CalGang.** California gang database that is a repository for personal information about suspected or confirmed gang members and "associates," as well as for information on gang activities.

**CAP.** *See* Criminal Alien Program.

**CARI.** *See* Criminal Alien Removal Initiative.

**CBP.** *See* U.S. Customs and Border Protection.

**COLLECT.** *See* Connecticut On-Line Law Enforcement Communications Teleprocessing.

**Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT).** A statewide criminal justice system for law enforcement and criminal justice agencies in Connecticut.

**Criminal Alien Program (CAP).** U.S. Immigration and Customs Enforcement program that identifies for removal proceedings people who are detained in jails or living in the community.

**Criminal Alien Removal Initiative (CARI).** U.S. Immigration and Customs Enforcement program initially intended to deport noncitizens who had criminal convictions.

**DACA.** *See* Deferred Action for Childhood Arrivals.

**Deferred Action for Childhood Arrivals (DACA).** A Department of Homeland Security program announced in 2012 that allows certain undocumented immigrants who entered the country as minors to receive a renewable two-year period of deferred action from deportation and authorization for employment.

**Department of Homeland Security (DHS).** U.S. Cabinet-level department that includes U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), and other agencies.

**Department of Homeland Security Victim Information and Notification Exchange (DHS-VINE).** An online tool that makes it possible to search for immigrants in civil immigration detention and in state criminal custody and be notified of custody changes.

**Department of motor vehicles (DMV).** Generic name for a state agency that issues driver's licenses and registers motor vehicles.

**DHS.** *See* Department of Homeland Security.

**DHS-VINE.** *See* Department of Homeland Security Victim Information and Notification Exchange.

**DMV.** *See* department of motor vehicles.

**DOJ.** *See* U.S. Department of Justice.

**Eagle Directed Identification Environment (EDDIE).** A mobile biometric software application that allows U.S. Immigration and Customs Enforcement officers and agents working in the field to take fingerprints and photos on mobile devices, transfer them wirelessly to biometric databases, and receive immediate identification results.

**EDDIE.** *See* Eagle Directed Identification Environment.

**Enforcement and Removal Operations (ERO).** Section of U.S. Immigration and Customs Enforcement responsible for immigration enforcement, including detention and deportation proceedings.

**EO.** *See* executive order.

**ERO.** *See* Enforcement and Removal Operations.

**Executive order (EO).** Order issued by the U.S. president to federal agencies and officers.

**Fair Information Practice Principles (FIPP).** Privacy policy and implementation principles based on the Privacy Act of 1974.

**FALCON.** Information technology platform developed by the private company Palantir and used by the Department of Homeland Security.

**FALCON-SA.** *See* FALCON Search & Analysis System.

**FALCON Search & Analysis System (FALCON-SA).** U.S. Immigration and Customs Enforcement case management system in FALCON designed to permit

ICE enforcement agents to search and analyze data from federal, state, local, and foreign sources.

**FALCON Tipline (FALCON-TL).** U.S. Immigration and Customs Enforcement Homeland Security Investigation (HSI) system that receives tips from the public, law enforcement, and others regarding suspected immigration violations and refers the tips to ICE agents for immigration enforcement.

**FALCON-TL.** *See* FALCON Tipline.

**FBI.** *See* Federal Bureau of Investigation.

**Federal Bureau of Investigation (FBI).** U.S. Department of Justice agency that, among many other functions, manages the National Crime Information Center (NCIC) and Next Generation Identification (NGI) databases.

**FIPP.** *See* Fair Information Practice Principles.

**FOIA.** *See* Freedom of Information Act.

**Freedom of Information Act (FOIA).** Federal law governing access to information held by the federal government.

**GangNET.** Commercial intranet-linked software offering a database with information on and photos of individuals and gangs, data analysis, facial recognition software, mapping, a field interview form, and a watch list. Allows information to be shared by federal, state, and local agencies. Used by many states and federal agencies, including U.S. Immigration and Customs Enforcement, in the creation of their own gang databases.

**HART.** *See* Homeland Advanced Recognition Technology.

**Homeland Advanced Recognition Technology (HART).** Vastly expanded biometric database under development by the Department of Homeland Security, intended to replace IDENT.

**Homeland Security Investigations (HSI).** ICE unit authorized to investigate immigration and many criminal violations.

**HSI.** *See* Homeland Security Investigations.

**IAFIS.** *See* Integrated Automated Fingerprint Identification System.

**ICE.** *See* U.S. Immigration and Customs Enforcement.

**ICEGangs.** U.S. Immigration and Customs Enforcement gang database based on GangNET software, created as a repository of personal information about suspected or confirmed gang members and "associates," information on gang activities, and information on immigration status.

**ICM.** *See* Investigative Case Management.

**IDENT.** *See* Automated Biometric Identification System.

**INA.** *See* Immigration and National Act.

**Integrated Automated Fingerprint Identification System (IAFIS).** The Federal Bureau of Investigation's national fingerprint and criminal history system, replaced by Next Generation Identification (NGI).

**Investigative Case Management (ICM).** Information technology that allows U.S. Immigration and Customs Enforcement agents access to a vast range of databases, information systems, and commercially available data to assist immigration officials in identifying and building cases against targets.

**Immigration and National Act (INA).** Comprehensive federal law governing admission and deportation of non–U.S. citizens, immigration benefits, and criminal penalties for immigration violations.

**Interoperability.** Ability of systems and databases to exchange data.

**Interconnection Security Agreement (ISA).** An agreement established between the organizations that own and operate connected information technology (IT) systems to document the technical requirements of the interconnection.

**ISA.** *See* Interconnection Security Agreement.

**Lawful permanent resident (LPR).** A non–U.S. citizen who has been granted lawful permanent residence status, which allows the person to live and work permanently in the U.S.

**LPR.** *See* lawful permanent resident.

**Memorandum of agreement (MOA).** A document (sometimes referred to as a memorandum of understanding, or MOU) articulating an agreement between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.

**MOA.** *See* memorandum of agreement.

**National Crime Information Center (NCIC).** A computerized index of criminal justice information available to federal, state, and local law enforcement and other criminal justice agencies that, among many other files, includes civil immigration records and information about alleged gang members.

**NCIC.** *See* National Crime Information Center.

**Next Generation Identification (NGI).** The Federal Bureau of Investigation's biometric identification system, formerly the Integrated Automated Fingerprint Identification System (IAFIS).

**NGI.** *See* Next Generation Identification.

**Nlets.** An automated, state-owned network, available to federal and state agencies, that permits the exchange of law enforcement, driver's license, criminal justice, and public safety information.

**Operation Joint Effort.** A police initiative between local law enforcement in Escondido, Calif., and U.S. Immigration and Customs Enforcement to create joint DUI (driving-under-the-influence)-immigration checkpoints.

**PEP.** *See* Priority Enforcement Program.

**PIA.** Privacy impact assessment.

**Priority Enforcement Program (PEP).** In place between November 2014 and January 2017 as a successor to the Secure Communities (S-Comm) program. Used S-Comm's interoperability between Federal Bureau of Investigation and Department of Homeland Security databases, accompanied by immigration enforcement priorities that described which foreign nationals DHS should be targeting for removal.

**Privacy Act of 1974.** Governs the collection, maintenance, use, and dissemination of information about people that is maintained in systems of records by federal agencies.

**Privacy impact assessment (PIA).** Required federal agency assessment that notifies the public of what personally identifiable information is being collected in records systems and how it will be used and shared.

**REAL ID Act.** A law that establishes standards for issuing driver's licenses and prohibits federal agencies from accepting for certain purposes driver's licenses and identification cards from states not in compliance with certain standards.

**Repository for Individuals of Special Concern (RISC).** A Next Generation Identification service that allows officers on the street to use a mobile identification device to take fingerprints and check them against NGI databases for an immediate response.

**RISC.** *See* Repository for Individuals of Special Concern.

**S-Comm.** *See* Secure Communities.

**Secure Communities (S-Comm).** A federal immigration enforcement program administered by the Department of Homeland Security from 2008 to 2014 and revived in 2017 that takes fingerprints of anyone arrested and booked and automatically checks them against interoperable Federal Bureau of Investigation and DHS databases.

**SORN.** *See* System of Records Notice.

**System of Records Notice (SORN).** Notice required by the Privacy Act of 1974 to be published in the Federal Register describing a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

**U.S. Customs and Border Protection (CBP).** U.S. Department of Homeland Security agency responsible for border management and control.

**U.S. Department of Justice (DOJ).** U.S. Cabinet-level department responsible for criminal prosecutions and civil cases in which the U.S. has an interest. Includes, among many other agencies, the Federal Bureau of Investigation and the Executive Office for Immigration Review (EOIR), which oversees the immigration court system.

**U.S. Immigration and Customs Enforcement (ICE).** U.S. Department of Homeland Security agency responsible for enforcement of laws pertaining to immigration enforcement and customs, as well as other functions.

**Victims of Immigration Crimes Engagement (VOICE).** Trump administration office within U.S. Immigration and Customs Enforcement intended to be a liaison between ICE and victims of crimes committed by noncitizens.

**VOICE.** *See* Victims of Immigration Crimes Engagement.

# Acknowledgments

NILC consultant and former managing attorney Joan Friedland is the principal author of this report. NILC staff Tanya Broder, Shiu-Ming Cheer, Kamal Essaheb, Melissa Keaney, Avideh Moussavian, and Diana Pliego made valuable contributions to its drafting and review. Also contributing were Neema Singh Guliani and Chris Rickerd of the American Civil Liberties Union, Jennifer Lynch of the Electronic Frontier Foundation, and Lena Graber of the Immigrant Legal Resource Center. NILC's Patrick O'Shea helped shepherd the project. Josh Kalven of Newsbound, Inc., created the illustrations and designed the report's cover. NILC's Richard Irwin edited, designed, and formatted the report.

# Contents: Detailed Table

# Notes

[1] "Interoperability describes the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user." See *What Is Interoperability?* (Healthcare Information and Management Systems Society), www.himss.org/library/interoperability-standards/what-is-interoperability.

[2] ICE is increasingly using sophisticated investigative and case management systems such as FALCON- Search and Analysis (FALCON-SA) and Investigative Case Management (ICM) to conduct immigration enforcement. See "Privacy Act of 1974; System of Records," 82 Fed. Reg. 20905-20909 (May 4, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/html/2017-09025.htm; and *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045* (U.S. Dept. of Homeland Security, June 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf. These systems include civil and criminal data from law enforcement agencies (among many other public and private sources).

[3] *Privacy Impact Assessment for the FALCON Tipline* (U.S. Department of Homeland Security, Nov. 2, 2012), https://www.dhs.gov/sites/default/files/publications/ice-pia-033-falcon-tipline-2012.pdf.

[4] *Next Generation Identification (NGI)* (Federal Bureau of Investigation), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

[5] *DHS's "Secure Communities": No Rules of the Road* (NILC, Mar. 2011), www.nilc.org/scomm-no-rules-of-road-2011-03-0/.

[6] 8 CFR § 287.7(a) (d), https://www.law.cornell.edu/cfr/text/8/287.7.

[7] Alex Stepick, Steve Held, Cynthia S. Hernandez, Cheryl Little and Susana Barciela, *False Promises: The Failure of Secure Communities in Miami Dade County* (Research Institute on Social and Economic Policy, Center for Labor Research & Studies, Florida International University, and Americans for Immigrant Justice, Miami, Florida and Washington, DC, Apr. 2013), http://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1021&context=soc_fac, p. 7.

[8] Kevin R. Johnson, *Doubling Down on Racial Discrimination: The Racially Disparate Impacts of Crime-Based Removals* (66 Case W. Res. L. Rev. 993, 2016), http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=4663&context=caselrev, p. 1027.

[9] *Missing the Point: ICE's Secure Communities "Reforms" Ignore Real Problems* (National Immigrant Justice Center, June 28, 2011), www.immigrantjustice.org/staff/blog/missing-point-secure-communities.

[10] "Secure Communities," memorandum to Thomas S. Winkowski, Megan Mack, and Philip A. McNamara, from Jeh Charles Johnson, Secretary, U.S. Dept. of Homeland Security, Nov. 20, 2014, https://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf, ft. 1. See also *Jimenez Moreno v. Napolitano*, where the U.S. District Court for the Northern District of Illinois, Eastern Division, decided in 2016 that detainers exceeded DHS's statutory

authority to make warrantless arrests. Memorandum opinion and order available at https://www.immigrantjustice.org/sites/default/files/content-type/press-release/documents/2016-11/JimenezMoreno-NDIL-ruling.pdf.

[11] *Priority Enforcement Program* (U.S. Immigration and Customs Enforcement), https://www.ice.gov/pep.

[12] *Id*.

[13] *DHS's New "Priority Enforcement Program"* (Immigrant Legal Resource Center), https://www.ilrc.org/sites/default/files/resources/pep_fact_sheet_final_ilrc.pdf.

[14] *Executive Order: Enhancing Public Safety in the Interior of the United States* (Office of the Press Secretary, The White House, Jan. 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united; "Enforcement of the Immigration Laws to Serve the National Interest," memorandum to Kevin McAleenan, Thomas D. Homan, Lori Scialabba, Joseph B. Maher, Dimple Shah, and Chip Fulgham, from John Kelly, Secretary of Homeland Security, Feb. 20, 2017, https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Enforcement-of-the-Immigration-Laws-to-Serve-the-National-Interest.pdf.

[15] The new priorities cover virtually all noncitizens, including, among other categories, those charged with offenses or who may have committed offenses even if not charged, as well as anyone the immigration officers consider a threat to public safety or national security. See *Executive Order: Enhancing Public Safety in the Interior of the United States, supra* note 14.

[16] *Understanding Trump's Executive Order Affecting Deportations and "Sanctuary" Cities* (NILC, Feb. 24, 2017), www.nilc.org/exec-order-deportations-sanctuary-cities/.

[17] "Privacy Act of 1974; Department of Homeland Security Immigration and Customs Enforcement-007—Alien Criminal Response Information Management System of Records," 78 Fed. Reg. 10623–10630 (Feb. 14, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-14/html/2013-03377.htm.

[18] *The 287(g) Program: An Overview* (American Immigration Council, Mar. 15, 2017), https://www.americanimmigrationcouncil.org/research/287g-program-flawed-and-obsolete-method-immigration-enforcement.

[19] *Executive Order: Enhancing Public Safety in the Interior of the United States, supra* note 14.

[20] *Executive Order: Border Security and Immigration Enforcement Improvements* (Office of the Press Secretary, The White House, Jan. 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/executive-order-border-security-and-immigration-enforcement-improvements.

[21] "Implementing the President's Border Security and Immigration Enforcement Improvements Policies," memorandum to Kevin McAleenan, Thomas D. Homan, Lori Scialabba, Joseph B. Maher, Dimple Shah, and Chip Fulgham, from John Kelly, Secretary of Homeland Security, Feb. 20, 2017, https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Implementing-the-Presidents-Border-Security-Immigration-Enforcement-Improvement-Policies.pdf.

[22] *Delegation of Immigration Authority Section 287(g) Immigration and Nationality Act* [sic] (U.S. Immigration and Customs Enforcement), https://www.ice.gov/287g.

[23] Jose Malgaña-Salgado, *Fair Treatment Denied* (Immigrant Legal Resource Center, June 2017), https://www.ilrc.org/sites/default/files/resources/2017-06-05_ilrc_report_fair_treatment_denied_final.pdf, p. 2.

[24] Memorandum of Agreement between U.S. Immigration and Customs Enforcement and the Etowah County Sheriff's Office, https://www.ice.gov/doclib/foia/memorandumsofAgreementUnderstanding/r_287getowah.pdf, p. 4.

[25] *Id.*

[26] *Interconnection Security Agreement* (U. S. Customs and Border Protection, Mar. 2008), https://apps.cbp.gov/tvpn/electronic_isa_draft_v2.pdf.

[27] CAP has also been expanded into the community to target those on probation or parole or in fugitive operations. See Guillermo Cantor, Mark Noferi, and Daniel E. Martínez, *Enforcement Overdrive: A Comprehensive Assessment of ICE's Criminal Alien Program* (American Immigration Council, Nov. 1, 2015), https://www.americanimmigrationcouncil.org/research/enforcement-overdrive-comprehensive-assessment-ice%E2%80%99s-criminal-alien-program.

[28] *Id.*

[29] Trevor Gardner II and Aarti Kohli, *The C.A.P. Effect: Racial Profiling in the ICE Criminal Alien Program* (The Chief Justice Earl Warren Institute on Race, Ethnicity & Diversity, University of California, Berkeley Law School, Sep. 2009), https://www.law.berkeley.edu/files/policybrief_irving_0909_v9.pdf.

[30] George Joseph, "Where ICE Already Has Direct Lines to Law-Enforcement Databases with Immigrant Data," *NPR.org*, May 12, 2017, www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d. For example, in Los Angeles County ICE has access to the Automated Jail Information System's (AJIS) new arrest data; the Consolidated Criminal History reporting System (CCHRS), which contains criminal history information and is also the repository for Automated Jail Information System's (AJIS) new arrest data, the Trial Court Information System (TCIS) for case management and disposition data, and the Juvenile Automated Index (JAI). CCHRS also interfaces with a variety of other state criminal justice and DMV systems. The Justice Data Interface Controller (JDIC) is a regional law enforcement data communications network (not a database) that gives county law enforcement agencies instant access to local, state and federal files and serves county police and court agencies, as well as other local, state and federal criminal justice agencies. See *Records & Identification Bureau* (Los Angeles County Sheriff's Department), http://shq.lasdnews.net/shq/TSD/ri_ovrview.html. See also *County of Los Angeles, California: Request for Information: Records Management System* (Los Angeles County Sheriff's Department, undated (circa 2006 or early 2007)), http://shq.lasdnews.net/shq/contracts/RMS_RFI_Final_doc.pdf.

[31] Spencer Woodman, "Despite Their Liberal Politics, Connecticut and California Are Sharing Immigrant Data with ICE," *The Verge*, Feb. 22, 2017, www.theverge.com/2017/2/22/14692842/ice-immigration-trump-data-connecticut-california. Officials at an Air Force base in California reportedly used the California Law Enforcement Telecommunications System (CLETS) to identify undocumented workers at the base. Tatiana Sanchez, "California Military Base Construction Workers Detained by ICE, *Mercury News*, May

12, 2017, www.mercurynews.com/2017/05/12/workers-detained-by-ice-while-doing-construction-job-on-military-base/.

[32] *National Crime Information Center (NCIC)* (Federal Bureau of Investigation), https://www.fbi.gov/services/cjis/ncic.

[33] Michael Wishnie and Annie Lai, *Blurring the Lines: A Profile of State and Local Police Enforcement of Immigration Law Using NCIC Database* (Migration Policy Institute, Dec. 2005), www.migrationpolicy.org/research/blurring-lines-profile-state-and-local-police-enforcement-immigration-law-using-ncic, p. 6.

[34] *National Crime Information Center (NCIC), supra* note 32.

[35] *NCIC 2000 Operating Manual: Wanted Person File* (National Crime Information Center, undated), https://www.oregon.gov/osp/CJIS/docs/NCIC%20Manuals/2015/WantedPerson.pdf, pp. 46–47. It is not clear whether records pertaining to the National Security Entry Exit System (NSEERS), a post-9/11 registration program that targeted boys and men from primarily Arab or Muslim countries, that were ordered included in NCIC in 2002 are still housed there, even though the program (which was determined to serve no meaningful national security purpose) was finally terminated in December 2016. According to a recent DHS Privacy Impact Assessment, records pertaining to NSEERS "violators" are a subset of records in an ICE database called LeadTrac. See *Privacy Impact Assessment for LeadTrac System* (U.S. Dept. of Homeland Security, June 22, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leadtrac-july2016.pdf, p. 10.

[36] Congress has specifically provided for inclusion of civil immigration records pertaining to previously deported "criminal aliens" and several other civil categories such as missing persons and civil orders of protection in stalking and domestic violence cases. The Bush administration ordered the inclusion of other civil immigration records after the 9/11/2001 terrorist attacks. See *National Crime Information Center (NCIC), supra* note 32

[37] *Final Report of the President's Task Force on 21st Century Policing* (Office of Community Oriented Policing Services, U.S. Dept. of Justice, May 2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf, p. 18.

[38] *National Crime Information Center (NCIC), supra* note 32.

[39] Michael Wishnie and Annie Lai, *Blurring the Lines: A Profile of State and Local Police Enforcement of Immigration Law Using NCIC Database, supra* note 33, p. 3.

[40] *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes - Channeling* (Federal Bureau of Investigation, May 5, 2008), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/firs-iafis.

[41] These fingerprint checks are authorized by a provision from 1972. See Public Law 92-544 (Oct. 25, 1972), https://www.gpo.gov/fdsys/pkg/STATUTE-86/pdf/STATUTE-86-Pg1109.pdf.

[42] Madeline Neighly and Maurice Emsellem, *Wanted: Accurate FBI Background Checks for Employment* (National Employment Law Project, July 2013), www.nelp.org/content/uploads/2015/03/Report-Wanted-Accurate-FBI-Background-Checks-Employment.pdf.

[43] 28 CFR § 20.3, https://www.law.cornell.edu/cfr/text/28/20.3.

[44] Sara Gates, "California DUI Checkpoint Program Targets Undocumented Immigrants," *Huffington Post*, July 28, 2014, www.huffingtonpost.com/2012/03/12/california-dui-immigration-checkpoint_n_1339772.html.

[45] Michael Todd, "Santa Cruz Police: Homeland Security Misled City with 'Gang' Raids That Were Immigration Related," *Mercury News*, Feb. 23, 2017, www.mercurynews.com/2017/02/23/santa-cruz-police-homeland-security-raids-immigration-status-not-gang-related/. See also Henry Graber, "How ICE Expanded Its Deportation Force Without Asking Congress for a Dime," *Slate* (Moneybox blog), April 28, 2017, www.slate.com/blogs/moneybox/2017/04/28/how_ice_expanded_its_deportation_force_without_asking_congress_for_a_dime.html.

[46] "CBP Rolls Out Biometric Exit Technology at Houston, Las Vegas Airports," *BiometricUpdate.com*, Aug. 11, 2017, www.biometricupdate.com/tag/cbp.

[47] Ali Winston, "Facial Recognition, Once a Battlefield Tool, Lands in San Diego County," *Reveal* (from the Center for Investigative Reporting), Nov. 7, 2013, https://www.revealnews.org/article/facial-recognition-once-a-battlefield-tool-lands-in-san-diego-county/.

[48] *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (U.S. Government Accountability Office, GAO-16-267, May 2016), www.gao.gov/assets/680/677098.pdf, pp. 47–48. See also Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Lineup: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy and Technology, Oct. 18, 2016), https://www.perpetuallineup.org/.

[49] Under the Deferred Action for Childhood Arrivals (DACA) program, DHS can grant temporary permission (deferred action) to stay in the U.S. for certain undocumented youth who came here as children. The program was announced by President Barack Obama on June 15, 2012. For more information, see the resources available from NILC's "DACA" webpage, www.nilc.org/daca/.

[50] Sean Garcia-Leys, Meigan Thompson, and Christyn Richardson, *Mislabeled: Allegations of Gang Membership and Their Immigration Consequences* (Immigrant Rights Clinic, University of California, Irvine, School of Law, April 2016), www.law.uci.edu/academics/real-life-learning/clinics/ucilaw-irc-MislabeledReport.pdf. See also Rebecca A. Hufstader, *Immigration Reliance on Gang Databases: Unchecked Discretion and Undesirable Consequences* (New York University School of Law, 2015), www.nyulawreview.org/sites/default/files/pdf/NYULawReview-90-2-Hufstader.pdf.

[51] Sean Garcia-Leys, Meigan Thompson, and Christyn Richardson, *supra* note 50, p. 8.

[52] *About GangNET* (CSRA Inc.), https://www.csra.com/gangnet.

[53] Arizona, Florida, California, District of Columbia, Florida, Georgia, Maryland, Minnesota, Nevada, New Mexico, North Carolina, South Carolina, Texas, Virginia, Washington. Of those, only some were sharing information in real time. See *White Paper: GangNet® Software* (SRA International, Inc., undated), https://assets.documentcloud.org/documents/1683801/gangnet8-whitepaper2013.pdf.

[54] *Id.*, p. 2

[55] *Id.*

[56] *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.

[57] Sean Garcia-Leys, Meigan Thompson, and Christyn Richardson, *supra* note 50, p. 8.

[58] *Practice Advisory: Understanding Allegations of Gang Membership/Affiliation in Immigration Cases* (Immigrant Legal Resource Center, April 2017), https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170426.pdf, p. 4.

[59] *Privacy Impact Assessment for the ICEGangs Database*, *supra* note 56.

[60] *National Crime Information Center (NCIC), supra* note 32.

[61] "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.

[62] 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, www.nyujlpp.org/wp-content/uploads/2012/10/Jacobs-Crepet-The-Expanding-Scope-Use-and-Availability-of-Criminal-Records.pdf, p. 193.

[63] Rebecca A. Hufstader, *supra* note 50.

[64] *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.

[65] *Id.*, p. 2.

[66] *Id.*, p. 3.

[67] *Id.*, pp. 3-4.

[68] *Id.*, p. 41.

[69] *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)* (U.S. Dept. of Homeland Security, Dec. 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy_pia_usvisit_ident_appendixj_jan2013.pdf, p. 4.

[70] *Id.*, p. 12.

[71] Stephen Mayhew, "NEC and GAI Deliver Mobile Biometric Collection Technology to ICE," *BiometricUpdate.com*, Mar. 28, 2016, www.biometricupdate.com/201603/nec-and-gai-deliver-mobile-biometric-collection-technology-to-ice.

[72] *Id.*

[73] Bianca Spinosa, "EDDIE, ICE and Apps," *FCW.com,* May 28, 2015, https://fcw.com/articles/2015/05/28/eddie-ice-and-apps.aspx. See also Justin Lee, "Immigration and Customs Enforcement App Collects Biometric ID in the Field," *BiometricUpdate.com*, Sep. 26, 2016, www.biometricupdate.com/201609/immigration-and-customs-enforcement-app-collects-biometric-id-in-the-field.

[74] Stephanie Kanowitz, "ICE Agents Collect Biometric IC in the Field," *GCN.com*, Sep. 21, 2016, https://gcn.com/articles/2016/09/21/dig-it-ice-eddie.aspx.

[75] Anthony Kimery, "CBP Updating Categories of Personal Information Input into Border Crossing Database," *Homeland Security Today*, May 11, 2015, www.hstoday.us/channels/dhs/single-article-page/cbp-updating-categories-of-personal-information-input-into-border-crossing-database/faf507d7bada93300899ea023c3d6516.html. See also Justin Lee, "CBP to Include Biometric Data in Border Crossing Database,"

*BiometricUpdate.com*, May 12, 2015, www.biometricupdate.com/201505/cbp-to-include-biometric-data-in-border-crossing-database.

[76] *Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)* (Federal Bureau of Investigation), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-risc.

[77] *Next Generation Identification (NGI), supra* note 4.

> The RISC will be queried by fingerprints (10 or fewer) electronically submitted by authorized NGI users, typically by first responder law enforcement officials in the course of their interaction with potential suspects or similar real-time encounters. The fingerprints will be captured by a mobile fingerprint device and transmitted wirelessly to the user agency's existing criminal justice infrastructure, then on to the RISC. The RISC will accommodate so-called "lights-out" processing using fewer than ten fingerprints. Lights-out processing refers to searches that are conducted entirely by computer automation, without any intervening involvement by humans.[2] The submission will result in an automated search of RISC records and lights-out generation of a response to the requestor's criminal justice infrastructure within ten seconds of the submission. The requestor's criminal justice infrastructure will then forward the response to the requestor's mobile device through its own communication channels. The RISC responses will be either "red," "yellow," "green," or "reject."

See also *Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)* (Federal Bureau of Investigation), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-risc.

[78] Oxdown Diaries, "Electronic Arpaios? FOIA Documents Reveal FBI, Local, Police Using Mobile Fingerprint Devices to Check Immigration Status, Collect Immigration Status, Collect Biometrics in 'Pre-Arrest' Scenarios," *Shadowproof*, Sep. 20, 2013, https://shadowproof.com/2013/09/20/electronic-arpaios-foia-documents-reveal-fbi-local-police-using-mobile-fingerprint-devices-to-check-immigration-status-collect-biometrics-in-pre-arrest/#more-38119.

[79] *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)*, *supra* note 69.

[80] *Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records* (Office of Inspector General, U.S. Dept. of Homeland Security, Sep. 8, 2016), https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-130-Sep16.pdf, p. 4.

[81] Zoe Carpenter, "How the Government Created 'Stop-and-Frisk for Latinos," *The Nation*, Sep. 3, 2014, https://www.thenation.com/article/how-government-created-stop-and-frisk-latinos/.

[82] *Id.*

[83] Ali Winston, *supra* note 47.

[84] *State Laws Providing Access to Driver's Licenses or Cards, Regardless of Immigration Status* (NILC, May 2017), www.nilc.org/state-laws-providing-dl-access/. In some states the "marked" licenses are available to citizens and immigrants (both documented and undocumented) alike. The REAL ID Act of 2005 requires states to meet certain requirements, including proof of lawful presence in the U.S., in order for their licenses to be acceptable as identification for certain federal purposes. States can issue licenses to drivers who cannot prove lawful presence, or can set up tiers

of licenses. Licenses that are not REAL ID compliant must be distinguishable in appearance and will not be not acceptable for federal purposes.

[85] According to immigration expert Margaret Stock, "When DHS wants to find someone, the primary government database it relies upon is the driver license database." See Margaret D. Stock, "Driver Licenses and National Security," *Drivers.com*, Feb. 2008, www.drivers.com/article/971/. And 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. See *Alien Registration: Usefulness of a Nonimmigrant Alien Annual Address Reporting Requirement Is Questionable* (U.S. Government Accountability Office, GAO-05-204, Jan. 2005), www.gao.gov/products/GAO-05-204.

[86] *Documents Obtained Under Freedom of Information Act: How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information* (NILC, May 2016), www.nilc.org/ice-dmvs-share-information.

[87] *Id.*

[88] The Nlets website describes the system as "the premiere interstate justice and public safety network in the nation for the exchange of law enforcement-, criminal justice-, and public safety-related information.... The user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community-cooperatively exchanging data." See *Mission & Vision* (Nlets website), www.nlets.org/about/who-we-are.

[89] *NISP - DL Photo Sharing* (map) (Nlets website), www.nlets.org/our-members/grantmaps?mapid=d26b4e70-934e-11e3-9a61-00155d003202.

[90] Spencer Woodman, "Despite Their Liberal Politics, Connecticut and California Are Sharing Immigrant Data with ICE," *supra* note 31.

[91] *Documents Obtained Under Freedom of Information Act*, *supra* note 86.

[92] *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, *supra* note 48.

[93] *Id.*

[94] *Id.*

[95] Paul Heintz, "Vermont DMV, State Police Play Nice With ICE," *Seven Days*, April 5, 2017, https://m.sevendaysvt.com/vermont/vermont-dmv-state-police-play-nice-with-ice/Content?oid=4953143.

[96] Messages exchanged in 2016 between the Vermont Department of Motor Vehicle and federal immigration enforcement officials, obtained by the ACLU of Vermont via a public records request, https://www.documentcloud.org/documents/3536260-Vermont-Department-of-Motor-Vehicle.html, pp. 48–49.

[97] *Id.,* pp. 12, 27, 49.

[98] *Id.,* pp. 17, 22, 33, 52–53.

[99] *Id.,* p. 71.

[100] *Id.,* p. 74.

[101] *Documents Obtained Under Freedom of Information Act*, *supra* note 86.

[102] *Id.*

[103] Cities include New York City, Newark NJ, Hartford CT, New Haven, CT; San Francisco, CA; Oakland, CA; Richmond, CA; Los Angeles, CA; Asbury Park, NJ; Mercer County, NJ; Trenton, NJ; Princeton, NJ; and Washington, DC. See *Building Identity: A Toolkit for Designing and Implementing a Successful Municipal ID Program* (The Center for Popular Democracy, Nov. 2015), http://populardemocracy.org/sites/default/files/Municipal-ID-Report_WEB_Nov2015.pdf. See also *Who We Are: Municipal ID Cards as a Local Strategy to Promote Belonging and Shared Community Identity* (The Center for Popular Democracy, Feb. 10, 2014), https://populardemocracy.org/news/who-we-are-municipal-id-cards-local-strategy-promote-belonging-and-shared-community-identity.

[104] In New York, several Republican assembly members have challenged New York City's plan to destroy these documents. See Erin Durkin, "NYC Asks Judge If It Can Dump Personal Info on Municipal ID Cards," *NY Daily News*, Jan. 5, 2017, www.nydailynews.com/news/politics/nyc-asks-judge-dump-personal-info-municipal-id-cards-article-1.2936416.

[105] *Powell v. Mayor, City of New Haven* (Immigration Reform Law Institute, Jan. 1, 2016), www.irli.org/single-post/2016/01/01/Powell-v-Mayor-City-of-New-Haven.

[106] Erin Durkin, *supra* note 104.

[107] Liz Robbins, "New York Can Destroy Documents, Judge Rules in Municipal ID Case," *New York Times*, April 7, 2017, www.nytimes.com/2017/04/07/nyregion/new-york-can-destroy-documents-judge-rules-in-municipal-id-case.html. The legislators' appeal of that decision was dismissed. *Matter of Castorina v. De Blasio* (LEAGLE.com), https://www.leagle.com/decision/innyco20170510487. The legislators filed a second challenge in April 2017. Rachel Shapiro, "Defeated in Court over IDNYC, Castorina, Malliotakis File New Suit," *Staten Island Real-Time News*, April 14, 2017, www.silive.com/news/2017/04/defeated_in_idnyc_lawsuit_cast.html.

[108] *About Privacy and Confidentiality* (ID NYC), https://www1.nyc.gov/site/idnyc/about/privacy-and-confidentiality.page.

[109] Tamara C. Daley, Laurel Lunn, Jennifer Hamilton, Artis Bergman, and Donna Tapper, *A Tool of Empowerment: A Mixed-Methods Evaluation of the New York Municipal ID Program* (Westat, Aug. 2016), www1.nyc.gov/assets/idnyc/downloads/pdf/idnyc_report_full.pdf, p. 1.

[110] For detailed information about how to design and implement a successful ID program, see *Building Identity: A Toolkit for Designing and Implementing a Successful Municipal ID Program*, *supra* note 103.

[111] *Privacy Act of 1974* (U.S. Dept. of Justice), https://www.justice.gov/opcl/privacy-act-1974. (The Privacy Act is at 5 USC § 552a, www.law.cornell.edu/uscode/text/5/552a.)

[112] *Id.*

[113] *Id.*

[114] *System of Records Notices (SORNs)* (U.S. Dept. of Homeland Security), https://www.dhs.gov/system-records-notices-sorns.

[115] *Privacy Impact Assessments: The Privacy Office Official Guidance* (U.S. Dept. of Homeland Security, June, 2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf, p. 1.

[116] *Privacy Impact Assessments* (U.S. Dept. of Homeland Security), https://www.dhs.gov/privacy-impact-assessments.

[117] See, e.g., 5 USC § 552a(j)(2) and (k)(2), https://www.law.cornell.edu/uscode/text/5/552a.

[118] "Privacy Act of 1974; U.S. Immigration and Customs Enforcement-006 Intelligence Records System of Records," 75 Fed. Reg. 9233–9238 (Mar. 1, 2010), https://www.gpo.gov/fdsys/pkg/FR-2010-03-01/pdf/2010-4102.pdf.

[119] 28 CFR § 16.96, https://www.law.cornell.edu/cfr/text/28/16.96.

[120] Comments of the Electronic Frontier Foundation Re. Proposed Exemption of FBI's Next Generation Identification (NGI) System from Key Provisions of the Privacy Act of 1974 and Proposal to Modify Existing FBI System of Records Notice JUSTICE/FBI-009 to Apply to the NGI System, July 6, 2016, https://www.eff.org/files/2016/07/06/eff_comments_on_proposed_privacy_act_exemptions_and_sorn_for_fbi_ngi_system.pdf.

[121] *Joint Requirements Council (JRC) Information Based Screening and Vetting Portfolio (IBSV): Biometrics Webinar* (U.S. Dept. of Homeland Security, Oct. 20, 2015), https://www.dhs.gov/sites/default/files/publications/DHS%20Biometrics%20%20Strategic%20Framework%20Webinar%20Slidedeck%20-%20October%2020%202015.pdf.

[122] Alex Newman, "This Is the Data We No Longer Get about Immigration Enforcement under the Trump Administration," *PRI's The World*, Mar. 30, 2017, https://www.pri.org/stories/2017-03-30/data-we-no-longer-get-about-immigration-enforcement-under-trump-administration.

[123] *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045, supra* note 2.

[124] Spencer Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine," *The Intercept*, Mar. 2, 2017, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

[125] *Id.*

[126] *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045, supra* note 2, p. 8, referring to DHS/ICE-009 External Investigations System of Records. See 75 Fed. Reg. 404 (Jan. 5, 2010), https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/FR-2010-01-05.pdf, p. 196.

[127] *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045, supra* note 2.

[128] 5 USC § 552(a)(2), https://www.law.cornell.edu/uscode/text/5/552a.

[129] "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons," memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. Dept. of Homeland Security, Jan. 7, 2009, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2007-01.pdf.

[130] *Id.*, p. 3.

[131] *Executive Order: Enhancing Public Safety in the Interior of the United States, supra* note 14.

[132] *FOIA Update: The Freedom of Information Act, 5 U.S.C. Sect. 552, As Amended by Public Law No. 104-231, 110 Stat. 3048* (U.S. Dept. of Justice, Jan. 1, 1996), https://www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat.

[133] "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information," memorandum to Distribution List, from Jonathan R. Cantor, Jonathan

R. Cantor, Acting Chief Privacy Officer, U.S. Dept. of Homeland Security, April 27, 2017, https://www.dhs.gov/sites/default/files/publications/Privacy%20Policy%20Guidance%20Memo%202017-01%20-%20FINAL.pdf.

[134] "Enforcement of the Immigration Laws to Serve the National Interest," *supra* note 14, p. 4.

[135] "DHS Announces Launch of New Office for Victims of Illegal Immigrant Crime," U.S. Dept. of Homeland Security press release, April 26, 2017, https://www.dhs.gov/news/2017/04/26/dhs-announces-launch-new-office-victims-illegal-immigrant-crime.

[136] *DHS VINE* (Appriss Inc. webpage), https://vinelink.dhs.gov/#/map.

[137] *VINE: Victims Have the Right to Know* (Appriss Inc. webpage), https://vinelink.com/#/home.

[138] Cindy Carcamo, "Babies and Children Listed in Homeland Security's Immigrant Database of Alleged Criminals," *Los Angeles Times*, April 27, 2017, www.latimes.com/nation/la-na-children-in-immigration-database-20170426-story.html.

[139] Julio Ricardo Varela, "DHS Says Publishing Names of Children for Detained Immigrants Database Was 'Lapse in Privacy Protocols,'" *Latino USA*, April 27, 2017, http://latinousa.org/2017/04/27/dhs-says-publishing-names-children-detained-immigrants-database-lapse-privacy-protocols/.

[140] Sam Levin, "Trump Immigration Database Exposes Crime Victims' Personal Info, Lawyers Say," *The Guardian*, May 26, 2017, https://www.theguardian.com/us-news/2017/may/26/us-immigration-crime-database-victim-data-exposed.

[141] Interviews with immigration attorneys. See Cindy Carcamo, *supra* note 138.

[142] Section 9(b) of the Interior Enforcement executive order requires use of the Declined Detainer Outcome Report to, "on a weekly basis, make public a comprehensive list of criminal actions committed by aliens and any jurisdiction that ignored or otherwise failed to honor any detainers with respect to such aliens." In addition, section 16 requires a quarterly report on incarcerated noncitizens. *Executive Order: Enhancing Public Safety in the Interior of the United States, supra* note 14. In addition, Section 14 of the border enforcement executive order requires statistical reporting regarding noncitizens apprehended near the southern border. See *Executive Order: Border Security and Immigration Enforcement Improvements, supra* note 20.

[143] "Implementing the President's Border Security and Immigration Enforcement Improvements Policies," *supra* note 21. See also "Enforcement of the Immigration Laws to Serve the National Interest," *supra* note 14.

[144] Ron Nixon, "Trump Administration Halts Reports on Immigration Cooperation," *New York Times*, April 10, 2017, https://www.nytimes.com/2017/04/10/us/politics/trump-administration-immigration.html.

[145] See, e.g., "Privacy Act of 1974; Systems of Records and Implementation; Notice and Proposed Rule," 81 Fed. Reg. 27284–27287 (May 5, 2016), https://www.federalregister.gov/articles/2016/05/05/2016-10120/privacy-act-of-1974-systems-of-records.

[146] Preventing the Systematic Alien Verification for Enforcement (SAVE) system from being used for immigration enforcement purposes. See, e.g., 42 USC § 1320b-7 notes, https://www.law.cornell.edu/uscode/text/42/1320b-7.

[147] See, e.g., 5 USC § 552a (j)(2) and (k)(2), https://www.law.cornell.edu/uscode/text/5/552a.

[148] 26 USC § 6103, https://www.law.cornell.edu/uscode/text/26/6103.

[149] 42 USC § 1396a(a)(7), https://www.law.cornell.edu/uscode/text/42/1396a.

[150] *Judicial Redress Act of 2015* (U.S. Dept. of Justice), https://www.justice.gov/opcl/judicial-redress-act-2015; 5 USC § 552a, https://www.law.cornell.edu/uscode/text/5/552a.