UNalienable

DATA SHARING BETWEEN AGENCIES

MARCH 2021

ACLU
Mississippi

Background/Executive Summary

While much of the cooperation between local, state, and federal agencies occurs in plain sight, advancements in technology have facilitated a separate and more secretive arena in which this entanglement also takes place. Through data sharing programs like **Secure Communities** (S-Comm) and interjurisdictional surveillance, law and immigration enforcement agencies at every level of government are able to share individuals' personal data under the guise of public safety. Evidence shows, however, that these practices have the contrary effect of interfering with local policing, facilitating discrimination, and violating our constitutional values with little to no accountability.

This policy brief outlines the harms that arise when government agencies exchange individuals' personal data for the purposes of immigration enforcement, and shares recommendations to mitigate abuse.

Secure Communities

At the time of an arrest, state or local law enforcement officers collect fingerprint data that is automatically sent to the Federal Bureau of Investigation (FBI) and checked against its biometric identification system. Through S-Comm, which was briefly replaced with the Priority Enforcement Program, fingerprint data is also shared with the Department of Homeland Security (DHS), which runs the data through its own biometric system in order to review individuals' immigration history. The suggestion of an immigration violation often triggers Immigration and Customs Enforcement (ICE) to send the arresting agency a **detainer request**, which may ultimately lead to the detainee's transfer to ICE custody and eventual deportation. ICE removed **over 600** undocumented Mississippians from their communities in fiscal year 2018 using S-Comm. But while this program's supporters champion it as a useful investigative tool, S-Comm introduces a number of damaging challenges at the local level and in practice.

Disempowerment of Local Law Enforcement

S-Comm disempowers local law enforcement by **forcibly integrating** ICE into their operations. Jurisdictions have no say on whether or not to be included in the S-Comm program, nor on which data are shared with their local ICE field office or what immigration enforcement action is appropriate following a detainer. This imposition by the federal government has come against strong **resistance** from state and local bodies. Local law enforcement offices know best how to keep their communities safe, but S-Comms hinders their ability to do so. Sonia Lin of Cardozo School of Law's Immigration Justice Clinic has **cautioned** that, in pushing S-Comm as a mandatory program, federal agencies "ignored serious concerns about community policing, the burden on local and state partners, privacy rights, and the increased risk of racial profiling."

Police Profiling

Research by organizations like the American Immigration Council suggests that S-Comm enflames profiling and facilitates arbitrary and discriminatory policing practices. For example, an officer might arrest a person of color simply to verify their immigration status. Through S-Comm, these practices play out most devastatingly against the Hispanic community: While they make up only 77 percent of the undocumented American population, Hispanics comprise **93 percent** of those identified for deportation through the program.

Failure to Advance Public Safety

Shifting control away from local actors, S-Comm expectedly fails to advance public safety. ICE claims that S-Comm only targets serious criminals and violent offenders, but **studies show** that low-level offenders, crime victims (including domestic violence victims), and those who were wrongfully arrested often get wrapped up in its operation. These collateral effects arise because fingerprints are automatically shared with DHS, **even when** the arrest was unlawful and/or the criminal charge was dismissed. One **2014 study** published in the Journal of Law & Economics found that, despite the over-250,000 detentions that had occurred under S-Comm by that time, "the program has not served its central objective of making communities safer." There was no meaningful reduction in crime across the 3,000 counties studied, including amongst violent crimes.

U.S. Citizens as Collateral Damage

Database errors and other defects in S-Comm procedure have had an alarming impact on many **United States citizens**, as well. **Data** collected in Oct 2011, only three and a half years after S-Comm's initiation, found that ICE had already arrested about 3,600 American citizens through the program. Over one-third of all individuals arrested under S-Comm also reported having a United States citizen as a spouse or child.

Database errors and other defects in S-Comm procedure have had an alarming impact on many United States citizens.

Freedom of Information Act (FOIA) records **obtained** by the Center for Constitutional Rights (CCR), the National Day Laborer Organizing Network, and the Cardozo Immigration Justice Clinic in 2011 further highlight the scope of abuse possible under S-Comm. These records show that, while ICE was using S-Comm to expedite immigration enforcement, the FBI was using the program as a pretext to develop its Next Generation Identification (NGI) initiative: a surveillance system that, according to the CCR, "seeks to collect and distribute massive amounts of biometric information on citizens and noncitizens alike." One decade later, the FBI **continues** to harvest a range of biometric data including fingerprints, palm prints, face maps, and iris scans through this secretive and **dangerous** operation. Given S-Comm's lack of empirical justification as a public safety tool, it is unreasonable to survive the program as a feeder to federal surveillance operations more broadly.

Advanced Surveillance

There are many **different kinds** of surveillance technologies, all of which require careful application in order to avoid violations of Americans' constitutional rights. While surveillance operations remain relatively obscure, what we know about their use for immigration enforcement in Mississippi and across the country makes clear that greater oversight and regulation is needed.

Private Brokers

At the federal level, ICE rarely collects or maintains databases itself, relying on intermediary companies to do so, instead. However, many of these private brokers have a documented history of violating civil and human rights. For example, the contract between ICE and Clearview AI—a facial recognition company that once pitched its software to a **white supremacist** politician as a tool for "extreme opposition research"—is currently under public **scrutiny** and facing **litigation** following news that it scraped **billions** of images from social media and other internet sites without users' consent in order to build their facial recognition database.

Another broker implicated in government surveillance is Palantir, a data analytics company that serves **DHS** and whose software allows ICE to develop detailed profiles of private individuals. One recent investigation and **report** on the company led Amnesty International to conclude, "[T]here is a high risk that Palantir is contributing to serious human rights violations of migrants and asylum-seekers." There is no denying this claim in Mississippi, as ICE relied on Palantir's software to conduct the 2019 poultry factory raids that targeted hundreds of undocumented community members, including many Indigenous Guatemalans who immigrated to escape genocide.

Deserving of particular scrutiny, Vigilant Solutions' automated license plate readers (ALPRs) also play an increasingly significant role in data sharing between local and federal agencies. Through a two-year, $6.1 million contract with ICE signed in 2018, the company, which is also a popular vendor with local law enforcement, gave over 9,000 ICE officers access to 500 million license plate locations collected by over 80 local law enforcement agencies across the country, adding to the 5 billion records the database already gathered through private businesses. Vigilant Solutions and ICE are able to access an average of 150 to 200 million unique license plate scans per month by actively targeting local law enforcement agencies to enlist for this program. On its website, Vigilant Solutions claims to local agencies that joining its "sharing network" is "as easy as adding a friend" on social media. ICE, on the other end of the recruitment effort, offers training sessions to federal agents and a step-by-step guide on how to pull local law enforcement into these data sharing arrangements.

In the absence of robust safeguards, ALPR technology is vulnerable to abuse; for example, a DC police officer once confessed to using his agency's ALPR system to look up the license plates of cars parked near a gay bar and blackmail their owners.

Automated License Plate Readers

All surveillance practices pose some threat to Americans' civil liberties, and records collected by the Electronic Frontier Foundation show that several jurisdictions across Mississippi have used outdoor video surveillance, fusion centers, and/or surveillance drones as of 2017. But of the advanced surveillance technologies utilized in our state, ALPRs seem to be amongst the most common.

ALPRs are high-speed cameras that record the license plate, location, time, and date, of every passing car. The recorded license plates are not solely of cars stopped at immigration checkpoints or police roadblocks—they are plausibly of every car on the road, regardless of the criminal or immigration history of the driver. ALPR cameras on police cars, road signs, and highway overpasses make this broad scoop of personal data possible. The gathered information is stored for years and creates detailed profiles of residents' private lives, including how they worship, when they go to the doctor, and where their children attend school.

ICE privacy guidance technically limits ALPR use around sensitive locations, but that guidance is impossible to apply when data is streamed en masse, and ICE regularly circumvents these and other privacy rules through "fusion centers" like that in Mississippi in which multiple law enforcement agencies collaborate (for example, when federal agents ask local detectives to run plate numbers).

While ICE policy also requires that all ALPR use be documented and justified, FOIA records collected by the ACLU of Northern California show that much of the exchanges between local law enforcement and ICE are informal and unchecked. In the absence of robust safeguards, ALPR technology is vulnerable to abuse; for example, a DC police officer once confessed to using his agency's ALPR system to look up the license plates of cars parked near a gay bar and blackmail their owners.

Agencies in Mississippi that use or have used ALPRs include but are not limited to the Ridgeland, Madison, and Hattiesburg police departments; Lamar and Jones County sheriff's offices; Mississippi Department of Public Safety Office of Homeland Security; and Mississippi Highway Patrol. In response to a records request by MuckRock, the Lamar County Sheriff's Office reported in 2018 that they were sharing ALPR data with over 500 other local, federal, and private agencies across the country. With a population just over 60,000, Lamar County's exchange of personal data at this scale is senseless.

Surveillance agreements often operate in secret, and the information available on their role in Mississippi is ultimately limited. Rankin County, for example, has ignored 48 records requests from MuckRock as of February 2021 on information related to its 2017 contract with Vigilant Solutions. Other Mississippi agencies that have shared data with ICE through Vigilant Solutions include the Jasper County Sheriff's Office and the Oxford Police Department; however, the details of these agreements, including whether or not they are still in force, remain unclear. Between December 2020 and January 2021, DHS, ICE, Customs and Border Protection (CBP), and the United States Citizenship and Immigration Services (USCIS) have all been hit with lawsuits, one by the **Center for Democracy and Technology** and another by the **ACLU**, for a failure to respond to FOIA requests on their data harvesting practices.

Public Safety and Security

Agencies that utilize surveillance technologies have argued that sharing personal data allows them to enhance public safety. For example, biometric data sharing might help officers identify recurring offenders and make arrests of known violent offenders before they are able to reoffend. Others claim that these practices are necessary to protect national security, and calls for more of them have **increased** since the January 6 insurrection. In practice, however, surveillance by law enforcement offers little verified benefit to the American public, while inflicting broad subversions of individuals' personal privacy and security.

Surveillance by law enforcement offers little verified benefit to the American public, while inflicting broad subversions of individuals' personal privacy and security.

Those who suffer most from these violations are invariably members of marginalized groups. Rep. Bennie Thompson and Kathleen Rice are amongst the many lawmakers who have **criticized** the use of taxpayer resources by immigration enforcement agents to surveil Americans, including United States citizens and especially those who advocate for immigrants, while they exercise their First Amendment rights to peaceful assembly. This law enforcement strategy follows in a tradition of government surveillance against civil rights leaders including now-celebrated minister and activist **Dr. Martin Luther King Jr.**

The Department of Justice (DOJ) offers **guidance** to federal law enforcement agents in order to protect against discriminatory conduct, but this guidance includes exceptions for when there is a suspicion of "a threat to national or homeland security" or "a violation of Federal immigration law," which has created space for the continued profiling of immigrants. For example, the DOJ states that FBI agents may reasonably pursue individuals of a particular ethnic group if there is a known gang whose members are of that group. This loophole once justified the surveillance of a broad swathe of the Latin American population that included, for example, Mexicans—who make up over one-third of Mississippi's **immigrant population**—due to threats posed by a **gang** that was founded by Salvadoran immigrants.

Conclusion

Across the country, there are over a dozen **different kinds** of surveillance technology used against United States residents, often indiscriminately, in secret, and with little oversight or accountability. In a **2017 case** on interjurisdictional data sharing, one Ninth Circuit Judge cautioned that the absence of reliable accountability mechanisms "allows immigration and other law enforcement agencies to prey on migrant and working-class communities." Without these mechanisms, he writes, "[l]aw enforcement officers can unconstitutionally round up migrant-looking individuals, elicit their names, and then search through government databases to discover incriminating information." Four years after this judgment and still shrouded in secrecy, data sharing and surveillance by local, state, and federal enforcement agencies raise serious cause for concern.

Recommendations

For state and local bodies

- End data sharing contracts
  - that allow unfettered information-sharing technologies and biometric collection to and from ICE, and
  - with private data brokers that work with ICE.
- Implement regulations on the purchase and use of surveillance technology, such as:
  - Community Control Over Police Surveillance (CCOPS) policies and/or ordinances that involve community members in decision-making processes regarding if and how their personal data is gathered and used;
  - Targeted bans on specific surveillance technologies, such as the ban on facial recognition in Jackson, Mississippi and 13 other municipal governments as of January 2021; and/or
  - General regulations on the acquisition and use of new technology by local law enforcement.

For the Biden administration and federal agencies

- End compulsory data sharing arrangements between federal, state, and local agencies.
  - Direct DHS to end S-Comm and dismantle all electronic information-sharing that redirects fingerprint submissions from local police to DHS for civil immigration enforcement.
  - End any arrangements or contracts that provide ICE with access to state and/or local databases for the purposes of civil immigration enforcement.
- Prioritize public safety and security.
  - Overhaul existing security guidelines to include objective evaluations of the extent to which an individual poses a significant flight risk of genuine danger to the community, and direct resources accordingly.
  - Pass legislation similar to the National Biometric Privacy Act to explicitly extend privacy rights to include biometric data.

For local, state, and federal bodies

- Enhance transparency and accountability.
  - Conduct an investigation into racial profiling by police, prohibit bias-based profiling, implement safeguards, and ensure accountability for abuse.
  - Improve the transparency of data sharing programs through regular public reporting.
  - Create clear guidelines for when it is appropriate for employees of government agencies to release individuals’ sensitive personal information.