UNalienable

DATA SHARING BETWEEN AGENCIES

Data sharing practices like Secure Communities (S-Comm) and advanced surveillance allow law and immigration enforcement agencies to share individuals' personal data with little to no accountability. This study shines a light on this issue and the harmful consequences on both citizens and non-citizens alike.

Secure Communities

Through S-Comm, fingerprints collected by local police are automatically sent to DHS, which runs the scans through its own database to review individuals' immigration histories. Rather than promote national security, this program in fact introduces a number of public safety hazards:

- **Disempowerment of Local Law Enforcement:** Local law enforcement has no say on whether fingerprints are shared nor on how that data is used, complicating any attempt at community policing.
- **Police Profiling:** Research shows that S-Comm **enflames** discriminatory policing and corresponds with the disproportionate arrest and deportation of Hispanics.
- **Failure to Advance Public Safety:** There has been **no meaningful reduction** in crime due to S-Comm. The program has, however, been used to target crime victims and low-level offenders that pose no threat to public safety.
- **US Citizens as Collateral Damage:** S-Comm has resulted in the **detention** of thousands of US citizens, and the FBI continues to use the program as a **pretext** to develop its own surveillance initiative.

Surveillance

Government and private entities across the country employ many different kinds of surveillance technologies to spy on Americans. Public information on the scope of their use is limited, but what we do know confirms that their unchecked application poses an ongoing threat to civil rights:

- Several surveillance companies with which DHS and ICE contract have documented histories of abuse. Palantir, for example, is likely "contributing to serious human rights violations of migrants and asylum-seekers" according to a report that identified the company's involvement as crucial to ICE's 2019 Mississippi raids.
- Dozens of Mississippi agencies have used advanced surveillance technologies such as outdoor video surveillance, fusion centers, surveillance drones, and automated license plate readers, sometimes sharing that data with hundreds of other local, federal, and private agencies around the country and in close collaboration with ICE.
- Chronic unresponsiveness to public records requests allows for the discriminatory collection of personal data against immigrants and their advocates without accountability.

Recommendations

For State and Local Bodies

- End contracts that facilitate unfettered data-sharing with ICE
- Implement policies that regulate the use of surveillance technology by local governmental bodies

For the Biden Administration and Federal Agencies

- End S-Comm and any other compulsory programs or private contracts that facilitate civil immigration enforcement through interjurisdictional data sharing
- Develop guidelines and legislation to directly address biometric privacy concerns

For Local, State, and Federal Bodies

- Improve transparency and accountability with regard to the collection and use of individuals' sensitive personal information

ACLU
Mississippi

Read the full brief: www.aclu-ms.org

#unalienable