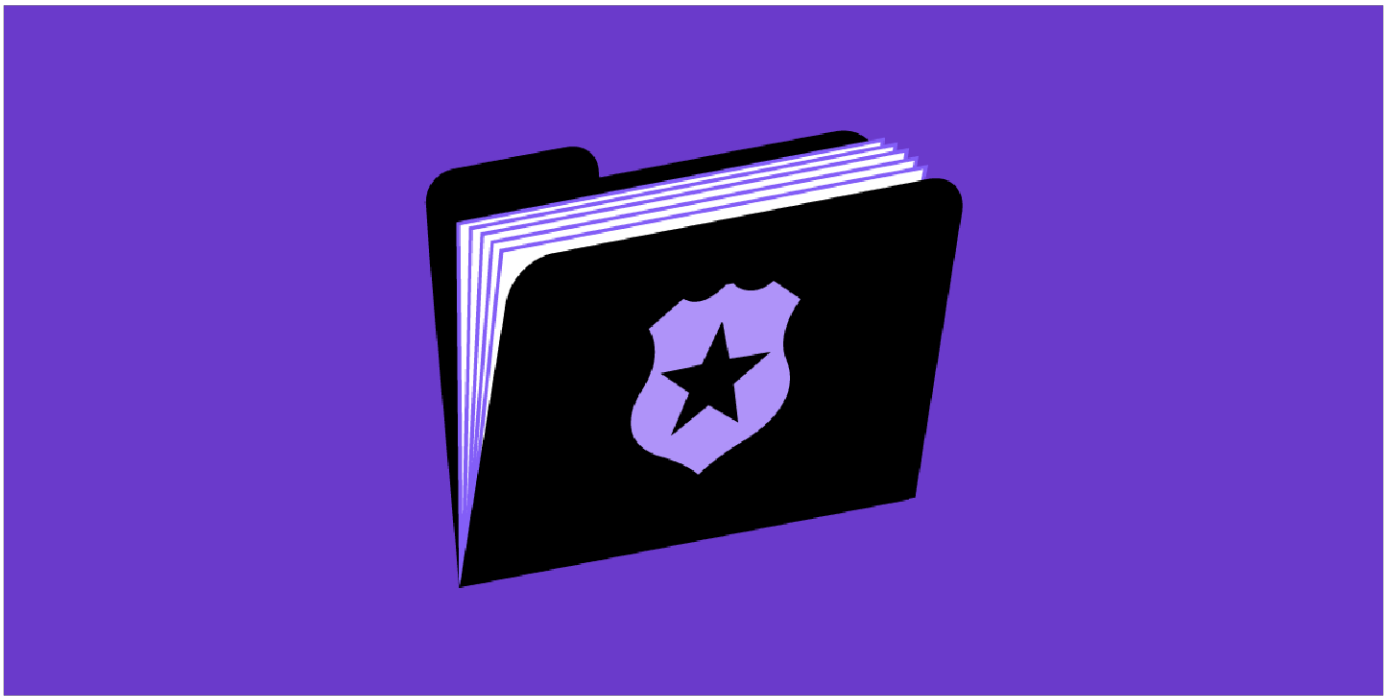
STREET LEVEL SURVEILLANCE



POLICE DATABASES

Law enforcement agencies maintain silos of data on individuals who have come into contact with the criminal justice and related systems, ranging from databases of RAP sheets to alleged gang members. This data is frequently shared regionally, across states, and nationally through data switchboards operated by both government and non-government services. Many law enforcement agencies also purchase data off the commercial market from a variety of data brokers catering to the public safety sector.

Federal Law Enforcement Networks

The FBI's Criminal Justice Information Services (CJIS) operates at least five distinct criminal justice information systems: National Crime Information Center (NCIC), Next Generation Identification (NGI), National Data Exchange (N-DEx), National Instant Criminal Background Check System (NICS), and Law Enforcement Enterprise Portal (LEEP). However, each of these may be comprised of other database systems. For example, LEEP connects to the Regional Information Sharing Systems Network (RISSnet), the National Gang Intelligence Center, and eGuardian.

been the United States' central database of criminal justice information since 1967, when it was founded by the J. Edgar Hoover administration. It contains data such as criminal record history information, fugitives, stolen properties, missing persons, and other data.

CJIS established security standards for all law enforcement agencies, including local and state agencies, that access or integrate data from these systems, including everything from password complexity to the vetting for maintenance workers.

Nlets

The National Law Enforcement Telecommunications System (Nlets) serves as a switchboard for data across the United States. It is not a government agency, but rather a non-profit organization with a board of directors composed of law enforcement officers.

State agencies, often including motor vehicle departments, connect their databases to Nlets, which allow for sharing of data across state lines. It also allows access to data to and from Canadian entities and Interpol.

Nlets provides law enforcement access to dozens of data systems. The organization maintains a public, interactive map that allows users to see which agencies are allowed to send or receive data from each source.

State and Local Police Databases

Most state governments maintain a statewide network, such as the California Law Enforcement Telecommunications System (CLETS), the Oklahoma Law Enforcement Telecommunications System (OLETS), and the Florida Crime Information Center (FCIC). These systems typically provide access to various state-level databases and connect data sources between local law enforcement agencies. These systems also share data with out-of-state agencies, usually through Nlets.

Local and regional law enforcement agencies also maintain their own systems. For example, in the San Diego area, a regional organization called SANDAG maintained the Automated Regional Justice Information System (ARJIS), while the Los Angeles Police Department operates the Network Communications System (NCS)

Threats and Harms

Law enforcement personnel are regularly caught accessing criminal justice information in inappropriate and illegal ways, according to research by the Associated Press and EFF. This often takes the form of an officer using official data to target women, be it for dates, as was the case in Bradenton, Florida, or as part of a pattern of domestic abuse, such as an incident in Akron, Ohio. There have also been cases of police officers accessing databases to assist criminals or adding false information to databases to exact retribution.

Interstate sharing of police data can also threaten vulnerable populations. For example, a prosecutor in a state with an abortion ban may try to access data from a state where abortion access is a protected right to try to identify individuals seeking or assisting with abortion services. Federal agencies, such Immigration and Customs Enforcement (ICE) may attempt to access these databases to apprehend undocumented immigrants in states with “sanctuary” laws.

The more data a government agency collects, the greater the risk of a data breach. Recent examples include the leak of personal information belonging to concealed carry permit holders in California or "Blueleaks," the massive dump of records from hacked agencies, including many fusion centers.

Since 2015, EFF has been documenting abuse of CLETS by California agencies, including successfully campaigning for the California Department of Justice (CADOJ) to improve how it collects misuse data. EFF also supported the California Values Act, a law that bans federal agencies from accessing certain types of criminal justice data for immigration enforcement. EFF successfully lobbied CADOJ to pass rules classifying immigration enforcement as formal misuse of the data, leading to ICE's deportation arm, Enforcement and Removal Operations, being removed from CLETS and other data systems in 2019. EFF also supported AB 1242, a bill signed into law by Gov. Gavin Newsom to prevent law enforcement from releasing data to out-of-state agencies investigating abortions.

Gang Databases

Gang databases are law enforcement databases that identify people who authorities have connected to gangs, often based on unsubstantiated evidence such as who someone associates with, what clothing they wear, or what tattoos they have. In some

information. Gang databases are typically unaudited, and individuals placed on them have no way to challenge their inclusion in a database or petition for removal–even if there is no evidence linking them to gang activity.

In California, activists have pushed local police departments to dissociate from CalGang, the statewide gang database, which, in 2020, contained information on over 90,000 people. In 2020, the LAPD announced it was discontinuing its use of the database. In 2023, a San Diego city subcommittee began studying how the San Diego Police Department used CalGang, prompting debate about whether the Department should cease use of the database amid accusations that it infringes on civil rights and liberties, has been used punitively and arbitrarily, and requires too much staffing to keep updated.

In 2023, Chicago planned to re-launch its gang database after its previous iteration was criticized by the city's inspector general and became the subject of a federal lawsuit for being racially biased and unconstitutional. Opponents of the program claimed that the 134,000 people on the list, which had little to no oversight or accountability mechanisms, "were at risk of severe sentencing, high bond, deportation or losing jobs because of it."

Threats and Harms

As evidenced above, inclusion in a gang database can have serious repercussions on a person's life, including leading to stops, interrogations, and use of force by law enforcement; enhanced punishment in the criminal legal system; and ill effects on a person's employment prospects. Despite these serious threats, there is often no oversight for these databases. The lists are often so poorly maintained that in Cook County, Illinois, ProPublica reported that hundreds of people in a 25,000-entry gang database managed by the Sheriff's Office's were actually deceased.

The victims of the exacerbated harassment brought on by gang databases are also disproportionately people of color, making gang databases one of the most pressing racial justice issues at the intersection of technology and the criminal justice system. In 2019, nearly 99% of the 18,000 person New York City gang database were people of color, with 88% of people in the database being Black and Latine. ICE has also used gang databases in its deportation efforts, including instances when individuals have been erroneously entered into these wildly unregulated systems.

2020, EFF joined a coalition of civil rights, immigration, and criminal justice reform organizations in calling for CADOJ to place an immediate moratorium on the use of the system, and have supported legislation to reform it.

Like gang databases, predictive policing algorithms often use amassed or questionable information to label a person a potential threat to public safety and make them vulnerable to police harassment and surveillance. EFF has also advocated for a ban on predictive policing algorithms.

Commercial Databases

Law enforcement agencies often purchase subscriptions to privately-managed intelligence databases. In addition to law enforcement data, these systems often provide access to commercially acquired data, ranging from consumer records to utility data. In some cases, the software claims to use artificial intelligence to develop leads or connections between suspects.

Common products include Thomson Reuters's CLEAR, Lexis-Nexis's Accurint, Transunion's TLOxp, and CoplinkX.

Police also are able to purchase access to real-time location databases, face recognition databases, and automated license plate reader databases from commercial providers.

Suggested Additional Reading

Spotlight: The Dangers of Gang Databases and Gang Policing (The Appeal)

TECHNOLOGIES