May 20, 2009

Dangerous Data: The Use and Abuse of Gang Databases

Heather Walczak
Introduction

For decades, law enforcement officials have attempted to compile extensive lists of information related to gangs in the United States. Through the use of the Internet and computers, officers have been able to move from time-consuming, burdensome, decentralized, and unhelpful classification systems to fully searchable databases. As the databases grow in popularity, the defects that were once invisible hiccups in the process have become large-scale issues that threaten the future of the gang database system. Research indicates that “documentation procedures suffer from a general lack of quality control and oversight in maintaining the database, causing erroneous documentation.” Without proper oversight and management, these flawed databases can lead to serious legal complications that far outweigh the benefit of their use.

This article explores the idea that the growing popularity and use of gang databases is dangerous and potentially unconstitutional unless there are restrictions on who can access and modify the information contained within the files. Part I of this article describes the history of gang databases and discusses how they are currently being used by law enforcement and other agencies to track, arrest, and convict gang members. Part II explores the legal ramifications of using the databases during the criminal investigation, sentencing, and paroling of gang members and those incorrectly labeled as gang members. Part III

---

suggests improved and constitutional methods for securing the information, verifying the accuracy of the input, and purging incorrect or outdated data.

**Part I: Overview of Gang Databases**

Databases have been in use for decades, stemming back to the most basic computer programs. Most commonly used in corporate settings, databases have become increasingly useful in other professions as well. One of the various ways in which they are employed is in law enforcement, specifically related to the prevention of organized street-crime. There are several regional gang database systems throughout the United States. Most notable are the Northeast Gang Information System (NEGIS) and CAL/GANG.

NEGIS was launched in 1996 and was created to facilitate the sharing of information between law enforcement officers in several Northeastern states.\(^2\) NEGIS started in Massachusetts when two state police offices began to customize the Lotus Notes program for use within the police department.\(^3\) Several Northeastern states connected to the database through dial-up connections that linked servers in individual states to the central hub in Massachusetts.\(^4\) This basic framework was made more successful when President Clinton urged the National Institute of Justice (NIJ) to fund the development further.\(^5\) The NIJ responded by awarding $425,000 in 1997 to get the NEGIS system off the ground.\(^6\)

While NEGIS has been a very useful communication tool for law enforcement officers in the Northeast, another database has been even more successful in the war against

---


\(^3\) Pilant, *supra* note 2.

\(^4\) Chu, *supra* note 2, at 113.

\(^5\) Pilant, *supra* note 2.

\(^6\) Id.
street gangs. CAL/GANG started in the 1980’s as a grass-roots campaign by the Los Angeles Sheriff’s Department. Originally known as Gang Resistance Education and Training (GREAT), California’s CAL/GANG program was the first crime database and investigations tool that was focused entirely on street gangs. The database was originally a DOS-based system and it experienced considerable growing pains as it attempted to keep up with the massive amounts of information compiled as gangs gained popularity and spread to areas outside Los Angeles.

The original GREAT system was very expensive and not user-friendly. The average street cop, who would benefit the most from the database’s use, could not operate it easily. Officers complained that “[y]ou had to re-learn the system and the commands everyday” and even entering the tiniest amount of information could take several difficult command sequences. So in 1993 the California Department of Justice began developing the program now known as CAL/GANG. After several years and hundreds of thousands of dollars, the programs was up and running and quickly became one of the most used gang databases in the country.

CAL/GANG is an intranet-based systems that is accessible through any webbrowser. Law enforcement officers can connect to the system through their headquarters, the laptops in their police cruisers, and even by mobile PDA system. The information contained within CAL/GANG is virtually limitless:

In addition to text-based data, CAL/GANG catalogues just about every piece of information imaginable, including tattoos, mug

---

8 Id.
9 Id.
10 Id.
11 Id.
shots, vehicle types and photographs, nicknames, and known associates... Through an easy graphical user interface (the web browser), CAL/GANG allows officers to use collected gang data and images to track, retrieve, and analyze gang-related information.\textsuperscript{12}

Access to this vast amount of information can be very useful to law enforcement officers when working on an investigation or speaking to a suspect or victim. Officers can search the database with tiny threads of information and create instant photo line-ups for identification of suspects. They can also use the information to find addresses and common hang-outs in order to execute warrants. Fourteen states currently use CAL/GANG, or Gangnet, as the program is called in some parts of the country, and while it is no substitute for good police work, it has certainly been beneficial to law enforcement officers.\textsuperscript{13}

\textbf{A. Information Gathering}

Regardless of which database program is studied, the program itself would be inconsequential without the input of data. This data is completely user-generated by law enforcement personnel and is obtained through a variety of means. There are two main paths of documentation: field interviews and active criminal investigations.\textsuperscript{14} Field interviews are consensual contacts involving law enforcement officers and known or suspected gang members. Officers ask the individuals about gang membership, tattoos, clothing, identity of associates, vehicles, addresses, and monikers and then record the information in the database with references to when and where the stop took place.\textsuperscript{15}

\textsuperscript{12} Id. at 3
\textsuperscript{14} Wright, supra note 1, at 120.
\textsuperscript{15} Id. at 121.
In addition to field interviews, law enforcement regularly conducts photostops as part of its information gathering efforts. A photostop occurs in one of five ways:

1. “Long-range Lens”--photographs obtained without investigatory detention;
2. “Mug Shot”--photographs obtained incident to arrest;
3. “Illegal Stop”--photographs obtained during a stop that was not originally justified by reasonable articulable suspicion;
4. “Unrelated Investigatory Stop”--photographs obtained during an investigatory stop originally justified by reasonable articulable suspicion, but the photographs are not related to the investigation of the suspicion that initially justified the stop, and;
5. “Related Investigatory Stop”--photographs obtained during an investigatory stop originally justified by reasonable articulable suspicion and the photographs are related to the investigation of the suspicion that initially justified the stop.16

Most commonly, photostops are used to generate information about gang members for future investigations and are not typically used for active investigations.17 Through digital technology, these pictures can be loaded almost instantaneously into gang databases and become immediately available for any officer on the network to access. Interestingly, these field interviews and photostops are routinely performed by regular patrol officers rather than specialized gang unit personnel who have considerably more training in the subject matter.18

Data also comes from less traditional and more controversial sources. The Internet has played an important role in the identification and tracking of suspected gang members. At the click of a button anyone can run an Internet search for information about gangs and come across a wealth of information. Sites like knowgangs.com provide articles, photos, videos and commentary about everything from gang signs, tattoos, drugs, and even law related to gangs.19 These sites even include pictures submitted by users who openly identify

---

16 Bruder, supra note 13, at 1702.
17 See id. at 1696.
18 Wright, supra note 1, at 121.
19 Know Gangs Homepage, Knowgangs.com (last visited Nov. 5, 2008).
themselves as gang members.\textsuperscript{20} Even sites like Wikipedia.org and HowStuffWorks.com have entries related to gangs.\textsuperscript{21} These resources offer the public, as well as law enforcement officers, instantaneous education about a variety of gang related topics and can provide up-to-date information about new gang members and emerging trends.

Many law enforcement offices now have Internet crime units that monitor the Internet not only for cybercrimes, but also for Internet connections to real-life criminals, including gang members. Detectives in the Chicago area monitor the Internet daily and use the information to educate themselves about gangs in their area. One officer believes that with “close monitoring and gang know-how, police can learn a lot. ‘You’d be surprised the amount of information they’ll put out on the web.’”\textsuperscript{22} Officers will use “screen grabs” and photos from the website to add to the databases for later reference.\textsuperscript{23} Sometimes the officers have real names or street nicknames to identify the individual, and sometimes they have little or no information to link the photos and comments to a particular individual and just make general entries into the database.

Often these Internet fishing trips only yield information that can be used in a very general way and does not help law enforcement make connections to individual members or gang-related crimes. Law enforcement officers admit that “by itself, material gleaned from the sites is of limited value. Although many departments said they monitor the sites for information, they can’t rely on them for evidence.”\textsuperscript{24} Officer Wistocki noted, “you’re not

\begin{thebibliography}{9}
\bibitem{20} Id.
\bibitem{23} Id.
\bibitem{24} Id.
\end{thebibliography}
going to get a case just off the Internet. This just helps us to maybe link some people to other people, get information about who they hang with, where they go.”

The Internet has, however, yielded more specific information on potential gang members under active criminal investigation. The growth and popularity of social networking sites has provided law enforcement personnel with another resource for identifying and tracking potential and known gang members on a more individual basis. MySpace.com touts itself as “A Place for Friends” but it has also become an especially useful tool for law enforcement officers throughout the country. Gangs all over the United States have “embraced the massive online community as a new way to fly their colors, brag about their exploits and talk trash about rival gangs.” This bragging and boasting has provided law enforcement with valuable information. The officers might only have a street nickname for a potential criminal suspect, but after doing a search of MySpace profiles, they might get more information including territory, known associates, and evidence of previous crimes.

In Stockton, California, for example, the Loc Town Crips (LTC) used the Internet and text messages to deal drugs, and members posted pictures of themselves on MySpace flashing their “L” gang sign and listing their street names. Law enforcement officers used this information to fill in the holes in the database for several suspected gang members and eventually made over thirty arrests and seized weapons, drugs, and $50,000 in drug

B. Database Documentation

It is relatively easy to understand and accept where the information is coming from, but slightly more worrisome is the entry and use of that information. Many states have processes known as “documentation,” but these processes are highly subjective in nature and employ loose or questionable criteria. Colorado, Florida, Illinois, Minnesota, North Dakota, Texas, and Virginia are some of the states with statutes specifically enabling the use of gang databases. Several of the enabling statutes specifically address how data may be entered and when a person may be labeled as a known gang affiliate.

Some states allow for immediate entry of data so long as the “minimum level of data specified by the Department is available.” That threshold can be between two and three criteria out of a list of six to eight. For example, the Texas Code of Criminal Procedure requires that information collected and entered into databases related to criminal street gangs must be relevant to the identification of an organization that is reasonably suspected of involvement in criminal activity, and it must also:

- consist of any two of the following: (A) a self-admission by the individual of criminal street gang membership; (B) identification of the individual as a criminal street gang member by a reliable informant or other individual; (C) a corroborated identification of the individual as a criminal street gang member by an

---

31 See id.; Alleged Stockton Gang Used Internet to Organize.
32 Id.
33 Wright, supra note 1, at 115.
35 See id.
36 Illinois Code § 2640/10(b).
37 Id.
informant or other individual of unknown reliability; (D) evidence that the individual frequents a documented area of a criminal street gang, associates with known criminal street gang members, and uses criminal street gang dress, hand signals, tattoos, or symbols; or (E) evidence that the individual has been arrested or taken into custody with known criminal street gang members for an offense or conduct consistent with criminal street gang activity.  

Some states impose additional restrictions on information related to children and teens. Many states will not allow entry of information or photographs of children under fourteen unless that child is a habitual juvenile offender, the juvenile has been adjudicated as an adult, or in some places if the parent or guardian is notified of the child’s potential association with a criminal street gang. North Dakota’s statute allows law enforcement officers to take photographs of minor suspects between the ages of fourteen and eighteen if the court finds several factors.

[T]hat a child at least fourteen years of age at the time of the offense is delinquent and the finding involves the unlawful use or possession of a handgun or the commission of an act proscribed by the criminal laws of this state and punishable as a felony or a class A misdemeanor committed for the benefit of, at the direction of, or in association or affiliation with any criminal street gang, with the intent to promote, further, or assist in the activities of a criminal gang, the juvenile court shall order upon the request of the state’s attorney the taking and retention of a photograph of the child for purposes of identification. 

The code goes on to restrict the maintenance and removal of authorized photographs of children by stating that they “may be maintained on a local basis and sent to a central state

---

38 TEX. CODE CRIM. PROC. ANN. art. 61.02 (Vernon 2007).
40 WEST'S FLA. STAT. ANN. § 985.047 (West 2008).
41 See MINN. STAT. § 299C.091 (2008).
42 TEX. CODE CRIM. PROC. ANN. art. 61.04 (Vernon 2007).
depository but must be maintained separate from those of adults and must be destroyed in accordance with section 27-20-54.”

These criteria and age restrictions do offer a little protection when properly enforced, but that protection is of little consequence when there is little to no monitoring of the content. Most gang databases allow multiple users to edit profiles at the same time from different locations. This can be very helpful for officers working on the same case but following different leads and speaking to different people, however, it can be disastrous for any effort to control the quality of the entries. Though some states have attempted to implement quality control measures, their efforts can be ineffective. For example, Illinois’s statute merely suggests, but does not require, that the Department of State Police “create a quality control program regarding confirmation of organize gang membership and organized gang affiliation data, timeliness and accuracy of information entered into and performance audits of all entering agencies.”

C. Use of the Database

The mere existence of information on potential and known gang members alone does not automatically generate problems. Even with issues of accuracy and monitoring, data alone does not necessarily generate legal concerns without actual use. To understand the problems that arise from gang databases, then, one must first examine how the data they contain is used. It turns out that law enforcement officers can use gang databases in nearly every step of the criminal justice process from investigations to arrests, injunctions, convictions, sentencing, and even parole.

44 Id.
45 20 ILL. COMP. STAT. 2605/10 (2008).
As previously discussed, gang databases are extensively used by law enforcement officers in the investigation of crimes. In addition to finding information about potential suspects, officers have taken advantage of the photographs contained in the database to make instant photo line-ups at the scene of a crime to allow victims to make identifications while their memories are fresh.

Gang databases are also being used to compile lists of gang members in an area for injunctive purposes. The injunctions are essentially nuisance restraining orders that restrict the known and alleged gang members from congregating with other alleged gang members, displaying colors, or merely being in a suspected gang territory. Anyone in the database who has information that might link them to the gang being enjoined could be subject to the restrictions, whether or not they are a confirmed member or affiliate of the gang.

In the criminal procedure context, gang databases are often used by prosecutors to bolster their case, transfer cases against minors from juvenile courts to general district and circuit level courts, as well as to trigger sentence enhancements. According to the National Youth Gang Center, at least twenty-three states have gang-related sentence enhancements, and the trend appears to be growing. During the 2008 election, California voted on Proposition 6, legislation aimed at decreasing gang violence and crime that would, among other things, increase sentences for youth labeled as gang members. Though the

---

46 Supra Part I(A).
47 Wright, supra note 1, at 117.
48 See id.
proposition was defeated, it indicates a trend of governmental interest in enhancing sentences and limiting parole for gang members.⁵²

**Part II: Legal Ramifications of the Use of Gang Databases**

**A. Access and Accountability Issues**

There are roughly 18,000 separate major law enforcement agencies in North America.⁵³ The feasibility of sharing paper files and information across these groups is nearly impossible, but the advent of intranets, the Internet, and other digital communication tools has allowed for easy compilation and a more free exchange of data. In fact several of the major gang databases, including CAL/GANG, have mobile components that can be accessed by cell phone, PDA, or laptop by any field officer with a password.⁵⁴

With so many users logging on to the system and making changes and additions to the database, it may become difficult to track the author, custodian and source of the information. This presents a difficult evidentiary problem. In order for the gang information to be admissible at trial, it must be authenticated under Federal Rule of Evidence 901, which establishes “authentication or identification as a condition precedent to admissibility” and requires “evidence sufficient to support a finding that the matter in question is what its proponent claims.”⁵⁵ A complicated matter arises with authentication of electronic data in criminal cases, as noted by the Advisory Committee on Rules.

Today, such available procedures as requests to admit and pretrial conference afford the means of eliminating much of the need for authentication or identification ... However, the need

---

⁵² *Id.*
⁵³ Chu, *supra* note 2, at 110.
⁵⁵ *Fed. R. Evid.* 901.
for suitable methods of proof still remains, since criminal cases pose their own obstacles to the use of preliminary procedures, unforeseen contingencies may arise, and cases of genuine controversy will still occur.\textsuperscript{56}

Some judges have attempted to circumvent the Rule 901 problems by treating all documents supplied by the government in response to discovery requests as authentic.\textsuperscript{57} Though removing the 901 hurdle for prosecutors can help bring valuable evidence into the case, it also eliminates the defendant’s protection against fraudulent or inaccurate evidence being treated as genuine.

Another potential problem arises out of the sheer number of people in agencies accessing the databases. In addition to detectives in large gang units and other traditional law enforcement officials, new agencies are beginning to use the information stored in gang databases.\textsuperscript{58} Several parole boards and smaller departments with limited security resources have tapped into the systems, raising concerns about the confidentiality of the data.\textsuperscript{59}

The concern about confidentiality also extends to the usefulness of the data if it is freely spread among groups not directly related to law enforcement. There are serious police concerns surrounding the information in gang databases. “Like the military, much of the data law enforcement gathers is sensitive. It is intelligence. [If disclosed], [i]t could jeopardize ongoing cases, fellow officers working undercover or in the field, even compromise prosecutions.”\textsuperscript{60}

\textbf{B. Sixth Amendment Issues}

\textsuperscript{56} \textit{Fed. R. Evid.} 901 advisory committee’s notes.
\textsuperscript{57} United States v. O’Keefe, 537 F. Supp. 2d 14, 20 (D.C. 2008). The magistrate recommended that the district court treat all documents supplied by the government as authentic, avoiding the Rule 901 and 902(11) issues of authentication and certification.
\textsuperscript{58} Kavanaugh-Brown, \textit{supra} note 51.
\textsuperscript{59} \textit{Id.}
\textsuperscript{60} \textit{Id.}
Perhaps more troubling than which agencies have access to the gang databases is who does not—criminal defendants. As law enforcement officials increasingly turn towards electronic sources of information as investigation tools and evidence at trial, Constitutional issues are raised. The Sixth Amendment states, in part, that “[i]n all criminal prosecutions, the accused shall enjoy the right ... to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.”\(^\text{61}\)

One major setback for defendants when confronting gang database evidence is the lack of a human witness to cross-examine. When examining the database evidence, a gang defendant must rely on the information provided by the prosecution during discovery because the information in the gang database is not readily available through other discovery tools.\(^\text{62}\) Adding to this problem is the unclear discovery requirements contained in the Federal Rules of Criminal Procedure. Rule 16(a)(1)(E) requires that upon request,

the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government’s possession, custody, or control and:

(i) the item is material to preparing the defense;
(ii) the government intends to use the item in its case-in-chief at trial; or
(iii) the item was obtained from or belongs to the defendant.\(^\text{63}\)

Two major issues arise from Rule 16. The first issue relates to subsection (a)(1)(E)(ii). While the prosecution may not plan to use the gang database evidence in its

\(^{61}\) U.S. CONST. amend VI.


\(^{63}\) FED. R. CRIM. PRO. 16(a)(1)(E), emphasis added.
case-in-chief, that information can be used in the sentencing portion of the trial. At least twenty-three states have gang-related sentence enhancements\textsuperscript{64} which can range increase the charges from misdemeanors to felonies and add on additional time in prison or on probation.\textsuperscript{65} In order to avoid these enhancements, defendants would need access to the gang database information in order to refute the classification. Yet, the prosecution might not be compelled to provide that access because they weren’t planning to use the information in the case in chief and because the information is not material for preparing a defense but rather for lessening a sentence enhancement after trial.

Second, even if the prosecution is compelled under 16(a)(1)(E)(ii) to provide some information from the gang database, Rule 16(a)(2) might limit that information to a form that is not useful for the defense. Rule 16(a)(2) limits discovery of internal government documents that are “made by an attorney for the government or other government agent in connection with investigating or prosecuting the case.”\textsuperscript{66} Even if the full contents of the gang database is provided, the search terms and methodology used by the investigating agents is the key to unlocking the information that is useful and relevant for the purposes of the trial. That information may be protected.\textsuperscript{67}

To clear up some of the confusion arising from the Rules of Criminal Procedure, some judges have turned to the Federal Rules of Civil Procedure.\textsuperscript{68} In \textit{United States v.}
O’Keefe, the District Court held that the Federal Rules of Civil Procedure may be used in criminal cases to determine whether the production of documents by the government has been in a form that is proper.\textsuperscript{69} Moreover, when electronic information is requested in criminal case, but the defense does not specify a form of production, the prosecution must produce it in the form in which it is ordinarily maintained or in a reasonably usable form.\textsuperscript{70} To be usable, a database must be searchable, lest it become the electronic equivalent of a massive box of documents without order or labels.\textsuperscript{71}

In the case of electronic gang databases, the form necessary for use should include the methodology used to obtain the search results. Without technical information about how the database works and what search terms were used, a defendant can not effectively cross-examine the prosecution’s witnesses that rely on the database information.\textsuperscript{72}

\section*{C. The Fourth Amendment and Public Exposure}

Among other concerns related to gang databases is the issue of individual privacy. The Fourth Amendment protects the “rights of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”\textsuperscript{73} The Court has long recognized that Fourth Amendment rights exist where an individual has an actual expectation

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{69} O’Keefe, 537 F. Supp. 2d at 19.
\item \textsuperscript{70} Id. at 19.
\item \textsuperscript{71} Id. at 20.
\item \textsuperscript{72} See Ken Strutin, Examination of Source Code Evidence, N.Y.L.J., Nov. 13, 2007, at 5.
\item \textsuperscript{73} U.S. CONST. amend. IV.
\end{itemize}
\end{footnotesize}
of privacy that is recognized by society to be reasonable.\textsuperscript{74} This right of privacy is weighed against governmental interests in the information. In many cases, an individual’s right to protect their good name and privacy and avoid having their personal information shared throughout multiple agencies might outweigh the government’s interest in whatever minuscule piece of information the database entry gives.

Putting aside issues about how the information was gathered, the compilation and continued use of the information after any initial suspicion of gang activity violates the spirit of the Fourth Amendment. Though the Supreme Court rarely addresses the issue of continued use of evidence when considering the reasonableness of privacy intrusions, it is a major factor related to the use of gang databases.\textsuperscript{75}

Some legal scholars suggest that unlimited use of evidence that was correctly obtained has no impact on an individuals privacy rights.\textsuperscript{76} However, this interpretation is increasingly outdated based on the evolution of technology and its effect on investigation techniques. The Supreme Court has occasionally indicated that when considering search and seizure, it is not only the initial evidentiary acquisition that matters, but also the later use of that evidence.\textsuperscript{77} Databases provide an infinite lifespan for the information they contain; far longer than that of human capabilities alone. Unlike with traditional paper file-based information systems in which a single investigation file can take enormous amounts of physical space to store and may be susceptible to destruction, electronic information aggregated from many case files can be stored on tiny microchips, with several copies and

\textsuperscript{74} Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
\textsuperscript{75} See Davis v. Mississippi, 394 U.S. 721 (1969) (discussing only how fingerprint evidence was obtained, not how it was later used).
\textsuperscript{76} See Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 TEX. L. REV. 49, 64 (1995) (arguing that “reasonableness cannot be assessed apart from consideration of that government’s use of the items seized”).
\textsuperscript{77} See Sherry F. Colb, What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 STAN. L. REV. 119, 179 (2002).
back-ups stored on additional servers. With that extended lifespan of the aggregated information comes the problem of future use of the now eternal data.

In United States v. Kincade, the court found that multiple searches of a DNA database did not constitute an additional intrusion into the individual’s privacy. However, the dissent in that case argued that the continual storage of Kincade’s DNA affected the reasonableness of the initial search. The majority failed to properly consider that each time the DNA database is searched in relation to a crime, Kincade is automatically considered a suspect. Similarly, when the gang database is searched any documented individual is treated as a potential suspect until additional information rules them out.

**D. Due Process Implications**

Even more serious are the due process concerns surrounding the gang databases. The Fifth and Fourteenth Amendments protect individuals from governmental deprivation of “life, liberty, or property.” An individual has a “‘liberty interest’ in [his] name, reputation, and integrity.” The “liberty interest” evolved out of line of cases beginning with Wisconsin v. Constantineau. This case revolved around law enforcement officers who posted signs in liquor stores and bars identifying Constantineau as a heavy drinker and encouraging proprietors not to serve her. The Supreme Court held that labeling a person in that way brought about questions of the individuals “good name, reputation, honor or integrity” and therefore the individual is entitled to notice.

---

78 397 F.3d 813 (9th Circ. 2004) (en banc).
79 Id. (Kozinsky, J., dissenting).
80 U.S. CONST. amend. V, XIV, § 1.
81 Wright, supra note 1, at 131.
82 400 U.S. 433 (1971).
83 Id.
84 Id. at 437.
In today’s society being branded as a gang member unquestionably carries certain negative connotations, and when an individual is entered into a gang database they could be classified in a damaging light. However, gang databases are not generally publicly accessible and so one’s reputation in the community will most likely not suffer. As additional governmental groups gain access to the database for various reasons, however, the likelihood that information will remain confidential and encapsulated in the criminal context diminishes. For example, a family services worker might have access the database for unrelated reasons and stumble across information that could impact a suspected gang member’s opportunity to gain custody of children. Clearly, stigma alone is not enough to trigger a due process issue, but the database presents larger legal issues than reputation. The critical question is whether documentation “significantly alters [an individual’s] status as a matter of state law.”

Though being in the database alone will not necessarily directly detain or strip an individual of his liberty and send him to jail, it does impact his rights in the criminal justice process.

A core objection to documentation by many individuals, documented and not, is that it: (1) increases the probability that they are charged with crimes committed by gang members by secondary liability; (2) increases the probability of conviction if they are charged; and (3) guarantees harsher penalties if they are convicted.

Guilt by association is a common problem with the gang database because documented individuals are linked to other documented individuals based on gang affiliation,

---

85 Paul v. Davis, 424 U.S. 693, 701 (1976) (rejecting the idea that “reputation alone, apart from some more tangible interests such as employment, is either ‘liberty’ or ‘property’ by itself sufficient to evoke the procedural protection of the Due Process Clause.” )
86 Id.
87 Wright, supra note 1, at 134.
regardless of whether the individuals are actually in the gang or have ever had a criminal record. When a gang war occurs involving multiple members of rival gangs, it is sometime difficult to pinpoint who is responsible for what and large groups may be rounded up and charged with the same crime. Once rounded up and charged, law enforcement officer may testify as to the individual’s documentation status at trial to establish motive, thereby increasing the likelihood that a jury will find the individual guilty. Once found guilty, the officer’s testimony regarding an individual’s gang status will open the door to enhanced sentencing and may even preclude an option of parole. Clearly the link between documentation and state law is strong and demonstrates that a documented individual’s status under those laws is altered based on information in the gang database.88

One of the other major due process concerns is the lack of notice given to individuals classified within the databases. The secrecy involved is necessary to a point, because as mentioned earlier, knowledge of who and what is in the database could compromise current investigations and prosecutions. Some documented individuals “are not entitled to notice, a hearing on the merits, or the opportunity to challenge the documentation decisions. Indeed, documented individuals are without recourse for agency failure to purge the names that should be thrown out of the system according to departmental and federal guidelines.”89

This lack of notice is particularly important because of a lack of clear guidelines for automatic removal of outdated or inaccurate information. If a person never knows they are wrongly in a gang database, they are never given the opportunity to challenge that documentation or the accuracy of the information relating to it. And because nobody knows for sure whether they are documented, there is no external pressure to remove the

---

88 See id. at 136.
89 Id. at 118.
information, and it remains in the database, sometimes indefinitely. Even in the rate cases where an individual is able to find out that they were documented, any process that exists for petitioning for removal is exhausting.\(^\text{90}\)

Like many areas of law enforcement, data processing appears to be heavy on work and light on staff to do it.\(^\text{91}\) It is far less burdensome to keep outdated information in the system for whatever incremental value it may have than to careful review and delete entries. Gang information may be at least six months behind and it is even more hit-or-miss as to whether it gets updated at all.\(^\text{92}\)

Delays in updating information may also mean delays in purging information. Several states have statutory instructions for purging information, but purging processes are often completely ignored. Minnesota Code § 299C.091 requires the government to destroy information stored in the database “when three years have elapsed since the data were entered into the system” or “until three years have elapsed since the last record of a conviction or adjudication or stayed adjudication of the individual.”\(^\text{93}\) The statute also allows data to be destroyed at the request of law enforcement officials regardless of whether three years have elapsed, though it is doubtful that many officers make such requests.\(^\text{94}\) Either way, the statute lays out a requirement of deletion without plan for its execution.

Additionally, Texas requires that data be maintained past its statutory three-year threshold where the individual is “confined in the institutional division or the state jail division of the Texas Department of Criminal Justice.”\(^\text{95}\) The statute does not specify

\(^{91}\) Wright, *supra* note 1, at 123.
\(^{92}\) *Id.* at 123-24.
\(^{93}\) MINN. STAT. § 299C.091 (2008).
\(^{94}\) *Id.*
\(^{95}\) TEX. CODE CRIM. PROC. ANN. art. 61.06(c) (Vernon 2007).
whether the charge must be related to gang activities or not. In theory, an individual who was wrongly documented and later serves jail time or is institutionalized could remain in the database for their entire sentence. Because gang affiliations can affect parole opportunities, the Texas statute forces individuals who are repaying their debt to society to be continually punished for alleged affiliations that may be decades old.

Privacy concerns also arise related to the sharing of information between government entities and the linking of gang databases to existing governmental databases. Numerous other governmental groups maintain databases, including the Immigration and Naturalization Service (INS), The National Sex Offender Registry, and the FBI Counterterrorism unit, as well as local mental health and parole boards. 96 Though it may be beneficial for there to be some sharing of information, the more eyes that see it, the less confidential it truly is.

E. The Exclusionary Rule

In addition to the evidentiary issues discussed in Part II(B), the privacy issues of Part II(C) and the due process concerns of Part II(D) another constitutional question arises based on how the evidence was entered into the database. The exclusionary rule holds that evidence collected or analyzed in violation of the defendant's constitutional rights may be inadmissible as part of the prosecution’s case-in-chief. 97 The exclusionary rule is a judicially created means to protect Constitutional rights; especially the rights previously discussed involving the Fourth, Fifth, Sixth and Fourteenth Amendments. 98 It can be argued that information

97 Weeks v. United States, 232 U.S. 383 (1914). Weeks established the exclusionary rule on the federal level, however it was not until Mapp v. Ohio, 367 U.S. 643 (1961) that the exclusionary rule was also held to be binding on the states through the Fourteenth Amendment.
98 Id.
contained within databases may be riddled with constitutional violations.\footnote{People v. Hernandez, 55 Cal. App. 4th Supp. 225 (1997).} Information gathered from searches and seizures that arise without probable cause should not be allowed into evidence; however, due to the problems of tracking entries it is highly possible that such information is being used by investigators and prosecutors.

An extension of the exclusionary rule applies to evidence that may be derived indirectly from the violation of the defendant’s rights.\footnote{Mapp v. Ohio, 376 U.S. 643 (1961).} Further evidence and information obtained during an investigation may be tainted and ultimately inadmissible if the underlying data from the gang database was corrupt or unconstitutionally obtained. A computer does not “have the power to transform hearsay from police report into non-hearsay evidence,”\footnote{Hernandez, 55 Cal. App. 4th at 241.} nor does it have the ability to ascertain whether the data was legally obtained. Evidence that would otherwise not be admissible in court should not suddenly be considered reliable regardless of its origins simply because it came from a computer.\footnote{Id.}

One major source of unconstitutional evidence is a confession of gang affiliation. As discussed in Part I, a large portion of the information contained in the gang databases comes from photostops, field interviews and direct communication with suspected gang members. During conversations with police, instigated without probable cause, suspected gang members may divulge information about their own gang membership, their associates and may even demonstrate gang signs or other identifying information.\footnote{Wright, supra note 1, at 120.} These confessions may be taken without Miranda warnings because the suspect is not under arrest, but it is likely that the gang member does not know that the information he or she gives to police will later
be entered in a gang database and used throughout the judicial process against him or her. Courts have held that these confessions are not admissible.\textsuperscript{104}

A confession is inadmissible if made after an illegal search or seizure, made after the police confront a suspect with evidence obtained through an illegal search or seizure, or made after an illegal arrest, unless the causal connection between the illegal act and the confession is broken so that the confession is not an exploitation of the initial illegality.\textsuperscript{105}

In the case of gang confessions entered into the database, even if the confession was a voluntary act and therefore out of the Fifth Amendment scope, there are underlying issues related to the Fourth and Sixth Amendments and so evidence should still be excluded.\textsuperscript{106}

Clearly, one unconstitutionally obtained piece of information can present problems for the admissibility of all the information in the gang database. While the exclusionary rule provides some protections to defendants against unconstitutional evidence being admitted, it can seriously impede investigators and prosecutors. However, rather than viewing the rule as a restriction, investigators should look at it as an incentive to better monitor and maintain the information in the database.

\textbf{Part III – Suggestions for Improvement}

There is no question that gang databases are extremely useful tools in the fight against street crime. However, without proper regulation, security and constitutional safeguards the databases have the potential to be more harm than help. Proper steps to protect the databases

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{105} \textit{Id.}
\item \textsuperscript{106} \textit{Brown v. Illinois, 422 U.S. 590, 601-02 (1975).}
\end{itemize}
\end{footnotesize}
would be relatively simple to implement and could significantly increase the integrity of the stored information.

The most logical place to begin protecting information is at the moment of access. Requiring an active case number to access the database would significantly reduce the number of unauthorized and improper users viewing the information. This would limit, and possibly eliminate, unauthorized users and third party agencies that have the clearance, but not necessarily a valid reason, to be accessing the database. It would also limit unnecessary field investigations and random photostops because there would be no where to input the data without an active case number or investigation file.

While the simple act of tracking active investigation entries would eliminate many of the problems itself, it would also serve as an incentive for self patrol by agencies that have access to the information. Self regulation by these groups of the entries made by their officials, as well as information about cases and suspects in their jurisdiction could lead to a significant decrease in Constitutional issues related to the data.

It is likely that some evidence used in trials may be found to be gathered in violation of the Fourth, Fifth, Sixth or Fourteenth Amendments; however, that rules on that information may not be widely know by all jurisdictions. By having each agency monitor their cases and adjust the contents of the database related to the inadmissible evidence, they can prevent future problems related to derivative evidence, or fruit of the poisonous tree.

For those to whom that solution may seem a bit drastic and or labor intensive, there may be less invasive solutions. If there is little or no restriction on who can access the
information, there must at least be logging and reporting of who made changes to the information, when they made the changes, and why. This minimally disruptive measure would increase the integrity of the information by forcing each law enforcement officer to be personally accountable for any inappropriate, inaccurate, or defamatory information. It could also assist prosecutors in establishing a chain of custody of the information, as well as providing a way for defendants to confront the modifier in court and cross examine them on their probably cause for investigation and entry of the information.

Moreover, with proper identification of the modifiers of the data, it would be possible to track corruption or racial profiling by certain officers. That information could provide wrongly identified gang members with legal recourse against profiling agents who routinely targeted certain groups or individuals without cause. This increased accountability would encourage law enforcement officers to be extra careful to verify information before it entered the system with their names attached to it.

Properly entered data from authorized users can still present legal problems when it becomes outdated or irrelevant. Scheduled purges of information could be used to remedy this potential problem. Even if several states currently require purging of outdated information every few years, these purges may never happen. A simple programming change could force the automatic purge of records with no activity after a certain amount of time regardless of who is notified and what the information is. The length of storage could be based on several factors, including: the reason the individual was labeled initially, convictions for gang related offenses, the age of the individual, and requests for purging by individuals proven to be non-gang members.
Cleaning the databases by ridding them of unconstitutional and outdated data will certainly lead to more reliable search results that carry a more persuasive impact in the courtroom. However, without more precise rules on discovery rules in the criminal context it may still be difficult for defendants to dispute allegations backed by database information. A revision to the Federal Rules of Criminal Procedure and the Federal Rules of Evidence to include specific language related to discovery of databases and the search methods used to obtain the information at issue would help clarify the requirements on the prosecution. Moreover, it would allow defendants of all income and technical expertise to have access to the information the prosecution may introduce and a change to use the information in the formulation of their defense.

**Conclusion**

Gang databases may once have been a creative solution to the growing problem with street crime, but in recent times they have raised more issues than they have alleviated. The seriousness of the penalties facing documented individuals drastically outweighs the incremental benefit to law enforcement officers dealing with gang problems. Without changes to the current system, the documentation process will continue to infringe on the rights of Americans. Simple solutions could be incorporated to modify the current system but ultimately, major changes based on current and future technological capabilities need to be made to insure a more secure and constitutional system.