May
2014
Volume 62
Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Monty Wilkinson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0 22(b)

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

Managing Editor
Jim Donovan

Associate Editor
Carmel Matin

Law Clerk
Jennifer Jokerst

Internet Address
www usdoj gov/usao/
reading_room/foiamanuals
html

Send article submissions and address changes to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201

Gang Prosecutions

In This Issue

Indicia of Association: Using Indicia Search Warrants in Gang Prosecutions

Gretchen C. F. Shappert
Assistant Director
Indian, Violent and Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

I. Introduction

The prosecution of criminal gangs is oftentimes premised upon evidence that gang members participated in a criminal organization—either a conspiracy or racketeering enterprise—with a shared identity and criminal purpose. The U.S. Constitution prohibits the criminalizing of mere association with a particular organization. *See Scales v. United States*, 367 U.S. 203, 225 (1961). However, association with a group of individuals engaged in criminal activity is not protected conduct and, indeed, may implicate federal criminal law. In order to establish the existence of a criminal gang, prosecutors frequently rely on search warrants to collect evidence of the criminal gang's organizational structure, membership, and of the criminal activity conducted by gang members.

Indicia search warrants are frequently used in biker gang investigations to collect indicia of affiliation, such as items bearing the logo or symbol of the biker gang—the leather jackets (colors), vests, belts, jewelry, plaques, t-shirts, tattoo stencils, hats, photographs, membership lists, club or gang documentation, calendars, clocks, or motorcycles. *See generally United States v. McConney*, 728 F.2d 1195, 1198 (9th Cir. 1984) (en banc) (affirming conviction involving an indicia search warrant that authorized search and seizure of indicia of membership in or association with the Hell's Angels Motorcycle Club), *overruled on other grounds by Estate of Merchant v. Comm'r*, 947 F.2d 1390, 1392–93 (9th Cir. 1991). Indicia search warrants are powerful tools that can be used to establish compelling evidence of the defendants' membership in a gang or enterprise. Indicia search warrants can also facilitate the collection of evidence to support the Government's contention that the defendants' association in the gang or enterprise was, at least in part, for purposes of criminal activity. However, the use of these warrants may raise unique First and Fourth Amendment issues for both prosecutors and agents.

II. Probable cause: the particularity of items to be seized and "scrupulous exactitude"

Two related cases from the District of Nebraska highlight the exactitude required when drafting indicia search warrants. *United States v. Apker*, 705 F.2d 293 (8th Cir. 1983), involved the prosecution of three members of the Hell's Angels of Omaha and the widow of a Hell's Angels member. The four were indicted, along with six other individuals, on conspiracy charges that alleged that the Hell Angels attempted to gain a monopoly on the methamphetamine traffic in Omaha and used threats, beatings, torture, and murder against competitors in the drug trade. Ten days after the indictment was returned, indicia search warrants were issued for premises of some of the Club associates, including the four defendants. "The indicia [search] warrants did not authorize the seizure of contraband or fruits or instrumentalities of crime[.]" *Id.* at 296. Rather, the search warrants "authorized the seizure of indicia of membership in the Hell's Angels [Motorcycle Club]." *Id.*

All the indicia search warrants were identical in their description of items to be seized. The affidavits supporting the search warrants stated that the indicia were necessary to prove the defendants' association with the Hell's Angels and their involvement in the Hell's Angels drug conspiracy. The description of items to be seized included: plaques, mirrors, and other items bearing the names of Hell's Angels members; sleeveless leather and jean jackets with a Death's Head insignia; "Hell's Angels" written above the Death's Head and "Nebraska" written beneath; a "Hell's Angels" belt buckle; photos depicting association with Hell's Angels members; telephone books and phone numbers of Hell's Angels local and national members; "papers relating to Club activities, including expenditures, financial records, Club rules and regulations;" and red t-shirts emblazoned with "Hell's Angels." *Id.*

When the indicia search warrants were executed, guns and drugs were confiscated at the various search locations. A superseding indictment was subsequently returned, and all four defendants were convicted of various drug and gun offenses. All four appealed, raising constitutional challenges to the use of indicia search warrants. *Id.* at 296–97.

The issues raised were matters of first impression for the Eighth Circuit. In its consideration of the validity of the indicia search warrants, the Eighth Circuit noted that, to the best of its knowledge, indicia search warrants had been used only once before in a federal case, in the 1979 racketeering prosecution of the California Hell's Angels. Only one prior appellate court decision, *United States v. Chesher*, 678 F.2d 1353 (9th Cir. 1982), discussed the indicia search warrants, but *Chesher* was decided on an issue not raised in the *Apker* case. *Apker*, 705 F.2d at 297. *See Chesher*, 678 at 1362–64 (holding that defendant was entitled to a hearing on the issue of whether probable cause for issuance of an indicia warrant was based upon a recklessly false statement that defendant was a current member of the motorcycle club and that "[i]f [defendant] does not prevail at the hearing, he may then raise again the challenges to the indicia warrant that we need not reach at this time"). Hence, the *Apker* court reasoned that it was "largely writing on a clean slate." *Apker*, 705 F.2d at 297.

The appellants in *Apker* argued that the indicia search warrants were invalid because they violated both the First and the Fourth Amendments to the Constitution. With regard to the Fourth Amendment, appellants made four arguments: (1) membership in a legal organization, such as Hell's Angels, cannot provide an adequate basis for a search because "there is not a sufficient nexus between the evidence sought and the crime being investigated," (2) the indicia warrants "failed to describe the [items] to be seized with sufficient particularity" and, therefore, amounted to no more than general warrants, (3) the affidavit in support of the search warrants "did not establish probable cause to believe that there would be indicia of membership in the Hell's Angels at the searched premises," and (4) "the indicia warrants were obtained as a pretext to search for guns and drugs." *Id.*

The Eighth Circuit began its analysis by citing the well-settled rule that searches are "not limited to instrumentalities or fruits of crime or contraband." *Id.* at 298. Searches may include "mere evidence" of a crime where there is a sufficient nexus between the items seized and criminal conduct. The issue for the warrant-issuing magistrate is "whether there is probable cause to believe that the evidence sought will 'aid in a particular apprehension or conviction.' " *Id.* (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)).

The Government argued that appellants' membership in the Hell's Angels "tend[ed] to show their association with each other in support of the conspiracy charge." *Id.* Furthermore, proof of membership helped "establish the charge in the indictment that appellants and others used the Hell's Angels [Motorcycle Club] for criminal activity, i.e., controlling the methamphetamine traffic in Omaha." *Id.* The Eighth Circuit noted that establishing membership in the Hell's Angels did not establish that the appellants were engaged in criminal activity. However, proof of club membership did help demonstrate appellants' association with each other and their opportunity to use the motorcycle club for illegal activity. *Id.*

The Eighth Circuit also rejected appellants' claim that the indicia search warrants lacked probable cause. The indictment, which was incorporated by reference, satisfied the probable cause requirement of the probability of criminal activity. "If an indictment can be used to establish the probability of criminal activity for an arrest warrant [there is] no reason why an indictment should not be able to establish probability of criminal activity for a search warrant." *Id.* at 303. Furthermore, the second element of the probable cause to support the issuance of the search warrant was established by the reasonable inferences drawn from the fact that the four residences to be searched were occupied by three Hell's Angels members and by the widow of a Hell's Angels member. Appellants' links to the four residences were based upon utility, ownership, and postal records, in addition to information from confidential informants and law enforcement surveillance, which were all referenced in the affidavit in support of the warrants. *Id.* at 303–04.

Appellants' contention that the indicia warrants were obtained merely as a pretext for a general search for guns and drugs was rejected as well. The "true purpose or bad faith" of law enforcement is a question of fact, and here, the district court found that officers "did not use the indicia warrants as a pretext" to search for other items beyond the scope of the warrants. *Id.* at 304. The district court rejected appellants' argument that the "true purpose" of the search was demonstrated by the pre-search meeting, where officers were instructed to be on the lookout for guns and drugs, and the fact that plans were discussed to seek state search warrants if necessary. The Government responded that the persons to be arrested were precluded from possessing firearms because of their previous felony convictions, a rationale that was accepted by the district court. The Eighth Circuit determined that the district court's conclusion was not clearly erroneous. *Id.*

More persuasive to the Eighth Circuit than the challenge to the warrants' probable cause was appellants' argument that their First Amendment rights to free association were implicated and that the court should apply a heightened scrutiny to its Fourth Amendment analysis. *See id.* at 302–05, (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Because they had freely proclaimed their association with the Hell's Angels, appellants argued that the indicia evidence of association had no relevance. The court rejected appellants' contention, noting that law enforcement cannot be expected to know what elements of proof suspects will concede or contest at trial. *Id.* at 302 ("We are not asking law enforcement officials to assess exactly how much evidence is needed for a conviction."). However, the court did agree that the first amendment right of association necessitated a higher level of scrutiny with regard to the particularity of items to be seized pursuant to the indicia search warrants. Some items, the court noted, were described with particularity, such as the Hell's Angels' leather and jean jackets, red t-shirts, belt buckle, and photos. Less specifically described items, such as telephone books, members' phone numbers, and papers relating to Hell's Angels activities, expenditures, rules, and regulations, failed to achieve the "high degree of specificity [that] is particularly needed with an indicia warrant." *Id.*

"Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.' " *Zurcher*, 436 U.S. 564 (quoting *Stanford v. Texas*, 379 U.S. at 485). The Eighth Circuit rejected the Government's argument that the "scrupulous exactitude" standard was not applicable because "the documents to be seized were not being sought for the ideas they contained, rather they were sought because they constituted indicia of membership in an organization appellants allegedly used for unlawful activities." *Apker*, 705 F.2d at 300. The court stressed that "[e]vidence of membership in a [given] organization [may] severely affect the exercise of First Amendment rights . . . ." *Id.* at 301. Of course, not all associations implicate the First Amendment. *Id.* at n.8. The court acknowledged that it could not find any case law recognizing freedom of association constitutional protections for criminal conspiracies. In this case, however, it was "membership in the Hell's Angels, not membership in the alleged [criminal] conspiracy," that was protected. *Id*.

The *Apker* court reasoned that a high degree of specificity is particularly necessary for indicia search warrants because these warrants are used to obtain evidence for just one purpose, to establish indicia of membership in a given organization:

> Unlike most warrants, the evidence on this issue would be needlessly cumulative once enough evidence was obtained to establish membership. While additional evidence would usually show the breadth of criminal activity, in the instant case additional evidence would at some point have no additional probative value in determining membership. Therefore, some of the items in the indicia warrants would do nothing to aid in the conviction. An indicia warrant allows an almost unlimited search for the purported purpose of obtaining evidence on a very narrow matter for which only a limited amount of evidence would be useful.

Id. at 302. Given the potential for abuse, the Eighth Circuit stated that the "indicia sought should be specifically identified in the warrant." *Id.* Where that was not possible, an explanation should be provided as to why it was not possible to specify, and "whether the non-specified items could actually aid in the conviction." *Id.* Because of the lack of specificity, the court concluded that the indicia warrants were inadequate and, therefore, invalid under the Fourth Amendment. *Id.* at 301. *See generally* Dennis T. Ducharme, *Taking the Mere Evidence Rule Too Far: Is Mere Suspicion Grounds for a General Search? United States v. Apker, 705 F.2d 293 (8th Cir. 1983), cert. denied, 104 S. Ct. 996 (1984)*, 22 AM. CRIM. L. REV. 67, 78 (1984) (analyzing the Eighth Circuit's holding in *Apker* that indicia of membership in the Hell's Angels Motorcycle Club was sufficiently linked to the Club's alleged criminal activities to support a finding of probable cause to search for such indicia); Wayne C. Holcombe, *Scope of the Fourth Amendment*, 73 GEO. L.J. 253, 298 (1984) (discussing the extent of Fourth Amendment protection).

Appellants also argued that the indicia search warrants were invalid under the First Amendment, as well as the Fourth Amendment, because the warrants tended to infringe upon the free right of association. In rejecting appellants' contention, the Eighth Circuit reiterated that there was a sufficient nexus between the items to be seized and the alleged criminal conduct to justify a search warrant, and, in the context of this case, members of the group in question "sometimes publicly identify themselves as Hell's Angels members by their dress, so additional harm from disclosure of membership lists is unlikely." *Apker*, 705 F.2d at 305. Finally, because of its disposition of the Fourth Amendment issue, the court concluded that it "need not determine the potential harm from Hell's Angels membership disclosure or whether there is a sufficient state interest to justify membership disclosure." *Id.* at 306.

Next, the *Apker* court turned to the question of whether firearms seized during the execution of the search warrants were admissible against the appellants. The Government argued that the firearms were admissible under the "inevitable discovery exception" and urged that even if the indicia warrants were invalid, guns associated with three of the four appellants "were properly seized during execution of the arrest warrants or were seized or would have been seized" upon execution of the subsequent state search warrants. *Id.* The court agreed that "[i]n this case the illegal [indicia search] warrant clearly did no more than hasten the discovery of the guns." *Id.* at 307. The majority, however, declined to adopt the analysis favored by the dissent to sever the general parts of the search warrant and only suppress those items which could not have been seized pursuant to the specific parts of the warrant. *See id.* at 307–08.

The *Apker* court acknowledged that four circuits had adopted the approach of severing the general parts of a warrant, rather than considering the entire warrant to be invalid. *Id.* at 307 (citing *United States v. Riggs*, 690 F.2d 298 (1st Cir. 1982); *United States v. Christine*, 687 F.2d 749 (3d Cir. 1982); *United States v. Cardwell*, 680 F.2d 75 (9th Cir. 1982); *United States v. Cook*, 657 F.2d 730 (5th Cir. 1981)). The *Apker* court, however, reasoned that a severance approach was particularly inappropriate in cases involving indicia search warrants. Indicia warrants are "by their nature" subject to possible abuse because of the potential for pretextual searches by law enforcement. *Id.* at 308. Hence, the three-judge

panel affirmed the convictions of three of the four defendants, but reversed the conviction of the fourth defendant, Fitzgerald, on a divided vote. *Id.* at 309–10.

The Government petitioned for a rehearing en banc, which was granted, limited to the question of whether firearms discovered in plain view during the execution of a federal indicia search warrant were admissible, where the warrant failed to describe some of the objects of the search with sufficient particularity. *See United States v. Fitzgerald*, 724 F.2d 633 (8th Cir. 1983) (en banc). Following the approach adopted by the First, Third, Fifth, Sixth, and Ninth Circuits, as well as several states, the Eighth Circuit in *Fitzgerald* adopted the severance approach and held that the indicia warrant was valid as to those portions that authorized a search for particular items, that is, certain articles of clothing, belt buckles, plaques, mirrors, and photographs tending to show association with the Hell's Angels. The court emphasized that five of the seven clauses of the indicia warrants met the particularity requirement in describing the objects of the search. The remaining two clauses were deficient only in that they failed to satisfy the "scrupulous exactitude" test. *Id.* at 636. Nothing in the record suggested bad faith on the part of law enforcement or that the search was pretextual. *Id.* at 635–36.

Applying its findings, the Eighth Circuit concluded that at least one of the weapons introduced against Fitzgerald was properly received into evidence. Valid portions of the warrant authorized officers to search for, among other things, certain jackets, t-shirts, and belt buckles. The officers searched the bedroom closet for these items, and it was there that they found the shotgun. A pistol located in the pocket of an overcoat was not admissible because officers had no reason to search coat pockets for Hell's Angels indicia. Likewise, the record failed to disclose sufficient information pertaining to recovery of a rifle behind a dresser drawer, so the rifle was not admissible, either. *Id.* at 637.

A recent Ninth Circuit case also addresses issues raised in *Apker*, including the higher level of scrutiny required of the magistrate, in order to ensure that the application for a search warrant contains a particularized description of the items to be seized. *United States v. Vasquez*, 654 F.3d 880 (9th Cir. 2011), *cert. denied*, 132 S. Ct. 1778 (2012), originated from a racketeering investigation of the Mongols Motorcycle Club. The Government sought and obtained a warrant to search the home of the defendant and to seize evidence of racketeering law violations. The affidavit accompanying the search warrant was common to the search of 121 residences of members of the Mongols Motorcycle Club, an organization engaged in racketeering activity, including murder, drug trafficking, robberies, hate crimes, and theft of motorcycles. The affidavit provided a detailed description of the organizational structure of the Mongols Motorcycle Club. The defendant was listed as the President of the Hemet Chapter of the Mongols. The affidavit noted that "the Mongols are different from many other criminal enterprises in that they keep extensive written documentation of their rules and activities." *Id.* at 882. According to the affidavit, these documents, including minutes of meetings and financial records, often contain evidence of criminal activity. Finally, the affidavit stated that Club officers (including the defendant) typically maintained these documents in a secure location, such as their respective residences.

When agents subsequently executed the search warrant at the defendant's residence, they retrieved an unloaded Beretta and ammunition, hidden inside a pair of socks that were in the pockets of sweatpants found in the garage. Also in the garage were photos of the Mongols, including the defendant. Adjacent to those items was a t-shirt bearing the defendant's alias name. Elsewhere in the garage, agents recovered a Cobray Mac-11 and several hundred rounds of ammunition, a black cooler airbrushed with the Mongols insignias, the Hemet Chapter bylaws, a member phone list, and photos of prospective Mongol members.

Following the search, the defendant was indicted for being a convicted felon in possession of a firearm and ammunition. The defendant moved to suppress the evidence obtained pursuant to the search warrant. He argued that there was insufficient probable cause in the search warrant particularized to him and that the affidavit falsely alleged that he was the president. The district court held that any falsity was immaterial, because if the defendant were the treasurer and not the president, he was still an officer in the

Club. The district court concluded that there was "probable cause aplenty in the search warrant and denied the motion to suppress." *Id.* at 882 (internal quotation marks omitted).

On appeal, the defendant renewed his challenge to the sufficiency of the search warrant, contending that the warrant was invalid and that the evidence should have been suppressed. The Ninth Circuit concluded that, based on the affidavit accompanying the warrant, the magistrate judge had a substantial basis for concluding there was probable cause to support the issuance of the warrant. *Id.* at 883. With regard to the issue that the *Apker* court focused on—the less-specifically described documentary items to be seized, including members' phone books and papers relating to Club activities—the Ninth Circuit applied a three-step analysis. First, the stated premise of the search was that the defendant was the Club president. The affidavit noted that undercover agents and confidential informants collected phone lists and rosters and attended Club meetings where they were able to observe the Club officers. The magistrate could reasonably infer that there was evidence to support the assertion that the defendant was the Club president. Second, the affidavit stated that informants, who were members or leaders of various Mongols chapters, observed others maintaining notes of activities or themselves participated in the note-taking. Club organizational rules required presidents to maintain club documents, including minutes. Therefore, it was reasonable for the magistrate to infer that the defendant maintained similar notes in his leadership role for the Hemet Chapter. Finally, the affidavit provided sufficient probable cause to believe that the records would contain evidence of a crime. Mongols retained notes and minutes of their meetings during which they discussed illegal activity, including engaging in narcotics and firearms trafficking. Therefore, the magistrate judge had a substantial basis for concluding that the documentation maintained at the residences of Club officers would contain evidence of criminal activity. *Id.*at 883–84.

According to the Ninth Circuit, the search warrant was not an indicia search warrant. The warrant sought minutes of Club meetings not to establish membership in the Mongols, but because these documents contained evidence of criminal activity. The Ninth Circuit emphasized that unlike the affidavit in *United States v. Rubio*, *infra*, further discussed below, the affidavit in *Vasquez* provided probable cause to believe that the records being sought would contain evidence of specific crimes. The affidavit described how the Mongols Motorcycle Club conducted its affairs through racketeering activity, including narcotics and firearms transactions. Club notes and minutes incorporated information about these transactions. Therefore, the magistrate had a substantial basis for believing that documentation maintained at the residences of Club officers would contain evidence of criminal activity. *Id.* at 884.

Prosecutors in gang investigations seeking indicia evidence of association or documentary evidence of criminal activity would be well advised to consider a detailed statement of the underlying facts that support probable cause in both situations. Indicia search warrants focus on a discrete element of the investigation—the association of gang or enterprise members—and must be supported by a detailed explanation of the nexus between the indicia evidence to be seized and the criminal conduct of the gang or enterprise, as well as a nexus to the place to be searched. *See generally Messerschmidt v. Millender*, 132 S. Ct. 1235, 1246–49 (2012) (§ 1983 action and claim for qualified immunity regarding the scope of a search warrant, authorizing the seizure of guns, ammunition, and indicia of gang membership; held that given the defendant's known gang affiliation, it was not unreasonable for officers to conclude that gang paraphernalia found at the residence would be an effective means of demonstrating the defendant's control over the premises or to the evidence found therein; the Fourth Amendment does not require probable cause to believe that evidence will conclusively establish specific facts in order to authorize a search, but only probable cause to believe that the evidence sought will aid in apprehension or conviction).

III. Establishing the nexus between criminal activity and the criminal gang or enterprise

In *Apker*, the Eighth Circuit held that a sufficient nexus existed between defendants' membership in the Hell's Angels Motorcycle Club and the criminal activity alleged in the bill of indictment to justify searches for indicia of club membership. The indictment, which alleged that the Hell's Angels Motorcycle Club was used to control the methamphetamine trade in Omaha and that the defendants were either members or associates of the Club, was incorporated by reference and thereby satisfied the probable cause requirement of likely criminal activity. *Apker*, 705 F.2d at 303–04. The Ninth Circuit, however, reached a contrary conclusion in *United States v. Rubio*, 727 F.2d 786 (9th Cir. 1984), a racketeering prosecution. The *Rubio* court's analysis underscores the need for a detailed and fact-specific showing of probable cause to believe that evidence to be seized pursuant to the indicia search warrant is connected to the alleged criminal activity. The Ninth Circuit in *Rubio* concluded that the affidavit in support of the indicia search warrants failed to adequately describe probable cause that the defendants engaged in a pattern of racketeering activity that was necessary in order to justify the indicia warrants. *Id.* at 792.

In *Rubio*, 33 defendants were charged in a 3-count indictment, which alleged racketeering violations in the conduct of the affairs of the Hell's Angels Motorcycle Club. Arrest warrants and indicia search warrants were executed simultaneously. The indicia warrants authorized the search for and seizure of "indicia of membership in or association with the Hell's Angels." *Id.* at 790. In addition to evidence of membership or affiliation with the Hell's Angels, execution of the search warrants resulted in the seizure of substantial quantities of evidence of criminal activity not covered by the indictment. These seizures, the Government contended, were made in reliance on the plain view doctrine. Shortly after the seizures, a superseding indictment was returned adding additional criminal charges as a result of the evidence seized in the searches. *Id.* at 791.

With the exception of Rubio, all defendants were convicted only of offenses added to the superseding indictment. Rubio was convicted of a charge in the original indictment, but much of the evidence pertaining to that charge was obtained from a search pursuant to the indicia search warrant. Similar to the allegations raised in *Apker*, defendants in *Rubio* raised a First Amendment challenge that the indicia warrants were facially invalid and violated the Club members' First Amendment guarantee of free association. The Ninth Circuit acknowledged the Club members' right to associate, but noted that when activities protected by the First Amendment become the subject of a criminal investigation, protections afforded by the Fourth Amendment come into play. *Id.* (citing *Zurcher*, 436 U.S. at 565). The court concluded that a narrowly drawn and properly issued and executed warrant for indicia of membership or association with a particular enterprise does not violate the First Amendment. *Id.* at 792.

The Ninth Circuit's analysis of the indicia warrants in *Rubio* focused on the sufficiency of the probable cause and, more specifically, the nexus between indicia of association evidence seized and the criminal activity alleged. All 5 affidavits were identical through paragraph 23 and contained voluminous detail about the indicia customarily kept by members and associates of the Hell's Angels Motorcycle Club. The remaining paragraphs of the five affidavits provided facts about each of the defendants, tending to establish each defendant's affiliation with the Club and the indicia of membership likely to be found at the defendant's residence. Finally, each affidavit referenced the racketeering indictment which charged the named defendant with associating with a racketeering enterprise—the Hell's Angels Motorcycle Club—for a specific period of time. None of the affidavits contained any statement of probable cause to believe that any defendant had conducted the affairs of the Club through a pattern of racketeering activity. Rather, the affidavits were limited to establishing association with the enterprise. The Ninth Circuit determined that these affidavits were insufficient to provide information tending to show the requisite nexus between the association of the defendants and the enterprise and some form of criminal activity. *Id.* at 794.

As previously discussed, the Eighth Circuit in *Apker* concluded that where the racketeering indictment was incorporated by reference into the affidavit in support of the search warrant, the probable cause requirement of the probability of criminal activity was satisfied. *Apker*, 705 F.2d at 303–04. The Ninth Circuit in *Rubio*, however, drew a distinction between probable cause as determined by a grand jury to support the return of an indictment and probable cause found by a neutral and detached magistrate within the four corners of the affidavit submitted in support of the search warrant. *Rubio*, 727 F.2d at 794–95. According to the *Rubio* court, an indictment alone cannot supply probable cause to search. *Id.* (citing *United States v. Ellsworth*, 647 F.2d 957, 964 (9th Cir. 1981) ("A Grand Jury is not a court, and its spectrum of responsibility does not include the duty of determining probable cause or lack thereof to search, nor the making of a decision as to whether a search warrant should issue.")).

The *Rubio* court concluded that the magistrate in this case had no substantial basis for finding that probable cause existed to support issuance of the indicia search warrants. But for the reference to the indictment, the affidavit furnished "no basis whatsoever" for believing that the defendants conducted the business of the Club through a pattern of racketeering activity. *Id.* at 795. Instances of individual criminal behavior by members and associates of the Club failed to establish a "connection between such individual activity and the conduct of the affairs of the enterprise as a whole." *Id.* The Ninth Circuit emphasized that applications for indicia search warrants must be examined carefully, because of the innocuous nature of the evidence to be seized—clothing, documents, and photographs. It explained that "the privacy interests that stand as the foundation of the Fourth Amendment are highly vulnerable here." *Id.* Indeed, the only protection for those privacy interests is probable cause to support the search. Because the Government failed to establish the requisite probable cause in the affidavits supporting the indicia search warrants, the court concluded that evidence obtained in the searches should have been suppressed. *Id.*

The nexus between illegal acts of individual Club members and the criminal activities of the gang or enterprise necessary to support issuance of an indicia search warrant was also examined in *United States v. Killip*, 819 F.2d 1542 (10th Cir. 1987), a racketeering prosecution of past and present members of the Oklahoma City Chapter of the Outlaws Motorcycle Club. *Killip* is noteworthy because unlike the indicia warrants discussed in *Apker* and *Rubio*, the Tenth Circuit in *Killip* concluded that the indicia warrant was sufficiently specific and that the affidavit in support of the indicia warrant adequately described the nexus between the indicia evidence to be seized and the pattern of racketeering activity alleged. *Id.* at 1550. *See generally Messerschmidt*, 132 S. Ct. at 1246–49 (although the affidavits in support of the search warrant application contained no facts directly linking firearms or evidence of gang activity to the residence, the Court held that the officers could reasonably rely upon the warrant to search for those items).

Following the return of a racketeering indictment, the Government in *Killip* sought a search warrant allowing agents to search the Oklahoma City Outlaws Motorcycle Clubhouse for indicia of membership in the Club. The affidavit in support of the warrant was signed by an FBI agent who had participated in the investigation of the illegal activities of the Club. It identified the defendants, explained that they kept indicia of Club membership at the clubhouse, and described many of the facts and episodes underlying the indictment. The magistrate authorized the search warrant.

Upon execution of the search warrant, agents seized guns, wearing apparel, flags, a police scanner, and assorted papers, including Club mottos, mailing lists, house rules, and Christmas cards. These items were subsequently introduced by the Government at trial. One of the issues raised on appeal was the validity of the indicia search warrant. Citing the Ninth Circuit opinion in *Rubio*, appellants argued that the magistrate in *Killip* had no basis for finding probable cause to believe that the evidence sought would show a violation of the RICO statute. The Tenth Circuit's analysis is instructive. The court distinguished *Rubio*, noting that the affidavit in support of the search warrant in *Killip* did not merely state that an indictment had been returned. Rather, the affidavit listed specific facts from the indictment that tended to support the conclusion that the Outlaws Motorcycle Club is a RICO enterprise and that association with that enterprise may be illegal. Facts detailed in the affidavit provided the magistrate

judge with probable cause to believe that a connection existed between alleged violations of the RICO statute and the indicia evidence sought by the Government. Therefore, the indicia warrant was valid and evidence from the search was admissible. *Killip*, 819 F.2d at 1550.

IV. Drafting considerations for the affidavit and indicia search warrant

In sum, prosecutors intending to use an indicia search warrant to collect evidence of a criminal gang in support of a conspiracy or racketeering prosecution must ensure that the affidavit and warrant are scrupulously exact. The affidavit must demonstrate probable cause to believe that the gang is engaged in criminal activity. It must show a connection between the defendants and the gang. The affidavit must explain that the indicia to be seized are necessary to prove the defendants' association with the gang and the gang's involvement in criminal activity. Finally, the affidavit must establish a nexus between the items to be seized and locations to be searched.

Prosecutors would be well advised to follow the example in *Killip* and verify that the affidavit in support of the search warrant lists specific, discrete facts or episodes of criminal activity tending to support the conclusion that the gang is a RICO enterprise or a criminal conspiracy and that association with the gang may be illegal. This verification is necessary to establish that there is probable cause to believe that the evidence sought is connected to a violation of federal criminal law. *See id.*

The prohibition of "general warrants" imposes a particularity requirement, requiring search warrants to specify the items to be seized and the locations to be searched. This is especially true with indicia warrants, because the items to be seized are not necessarily contraband and constitute "mere evidence." *Apker*, 705 F.2d at 297–98. Care must be taken to describe the items to be seized as specifically as possible. The *Apker* court was especially critical of portions of the warrant referring to "other items" with names of members. *Id.* at 299. Descriptions of jackets, belt buckles, t-shirts, photographs, mirrors, and plaques were sufficiently specific. General references to telephone books and papers relating to the Hell's Angels were not. "For instance, a search of a suspect's personal telephone book to see if alleged co-conspirators were listed would not be needlessly cumulative. . . . A search for indicia for the purpose of proving membership in an organization should be limited to specifically enumerated items whose relevance and probative value is shown." *Id.* at 303.

The particularity of the description of items to be seized was also a focus of the Ninth Circuit in *Vasquez*. As noted, in *Vasquez* the search warrant was not, strictly speaking, an indicia search warrant because the items to be seized were not indicia of association, but rather records of the Mongols Motorcycle Club that contained evidence of criminal activity, including notes and minutes of Club meetings. Where applicable, information tending to show that a gang maintains records of criminal activity should be included in the affidavit in support of the search warrant. Specific facts tending to show that the Club minutes memorialize, for example, its drug dealings will help to establish probable cause to believe that the records contain evidence of a crime. *See Vasquez*, 654 F.3d at 883–84.

V. Indicia warrants and the reasonableness of the search

Precise drafting of the affidavit and search warrant are not the only challenges confronting prosecutors and agents who use indicia search warrants in gang investigations. The manner of execution and the scope of the search are equally important. As the *Apker* court noted, indicia warrants are useful for obtaining evidence "on a very narrow matter for which only a limited amount of evidence would be useful." *Apker*, 705 F.2d at 302. The test for what is necessary to execute a search warrant effectively is reasonableness. Agents who disregard this provision of the Fourth Amendment operate at their own peril. An unfortunate example of the unreasonable execution of indicia search warrants appears in *San Jose Charter of Hell's Angels Motorcycle Club v. City of San Jose*, 402 F.3d 962 (9th Cir. 2005) (Bea, J., concurring in part and dissenting in part), a 42 U.S.C. § 1983 civil rights action against city police officers and a deputy sheriff, alleging that searches of residences of Hell's Angels affiliates violated the

Fourth Amendment. Defendants moved for summary judgment based upon their qualified immunity. The district court denied defendants' motions, and the matter was appealed to the Ninth Circuit.

San Jose Charter arose following the simultaneous execution of indicia search warrants at the residences of members of the Hell's Angels and at the Hell's Angels clubhouse in the Santa Clara and Santa Cruz counties of California. The searches were executed during the investigation of the murder of a patron of the Pink Poodle nightclub in San Jose. Local investigators concluded that one of the nightclub's bouncers, a member of the San Jose Chapter of the Hell's Angels, was a prime suspect in the murder. The suspect was ultimately charged, and local law enforcement officers applied for search warrants to search the Hell's Angels clubhouse and the residences of various Club members on two separate occasions. The second set of indicia search warrants were for the clubhouse and residences of nine Hell's Angels members. The affiant for the second set of warrants submitted a 24-page affidavit, which incorporated by reference his initial 27-page affidavit, describing the investigation. The second set of 10 warrants was substantially identical except for location and the names of the residents. *Id.* at 966–67.

The warrants authorized the seizure of a suspected security videotape of the murder, notes, or records of the Hell's Angels meeting following the murder, and indicia of Hell's Angels affiliation, including "any evidence of membership in, affiliation with, activity of, or identity of, any gang, including but not limited to, any reference to 'Hell's Angels.' " *Id.* The district court concluded that there was insufficient probable cause to believe that either the videotape or the meeting minutes would be found at the residences, and that the warrants were supported by probable cause only with respect to the search for evidence with indicia of Hell's Angels affiliation. Hence, the Ninth Circuit's analysis focused upon the reasonableness of the search for indicia. *See id.* at 976. The purpose of the indicia provision in the search warrants was to obtain evidence supporting a street gang enhancement against the defendant pursuant to California criminal law because the murder had allegedly been committed in furtherance of the Hell's Angels, a criminal gang. *Id.* at 966–67.

During the execution of the search warrants, search teams located numerous items that bore indicia of Hell's Angels affiliation. Fearing that they might confiscate too many items, some of the officers contacted the deputy sheriff affiant, who instructed them to take everything that constituted indicia of Hell's Angels affiliation as defined in the warrant, including belts, jewelry, plaques, t-shirts, clocks, hats, watches, vests, calendars, sculptures, photographs, and correspondence. Officers conducting the search also seized motorcycles, a mailbox, a refrigerator door with decals, and a cement portion of the driveway in front of the clubhouse containing the signatures of the Hells Angels members. At the conclusion of the searches, officers carted away "literally truckloads of Hell's Angels indicia" and proceeded to rent a special off-site storage facility to accommodate all of the evidence. *Id.* at 970.

In the process of executing the search warrants, officers also shot and killed a total of three dogs at two residences. At the first house no one was home. At the second house, one of the residents was located and handcuffed just yards from where her dog lay dead and bleeding. None of the residents were charged with crimes.

After a detailed review of the underlying facts, the Ninth Circuit expressed no hesitation in concluding that the execution of the indicia search warrants violated the Fourth Amendment and that the officers responsible were not entitled to qualified immunity. The test of what is necessary to "execute a warrant effectively" is reasonableness, and the Fourth Amendment's mandate of reasonableness applies "from the moment of the officer's entry until the moment of departure." *Id.* at 971 (quoting *Lawmaster v. Ward*, 125 F.3d 1341, 1349 (10th Cir. 1997)). The Fourth Amendment analysis of reasonableness focuses on both the purpose disclosed in the application for the search warrant and the manner in which it is executed. *Id.* (citing *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978)). Here, the authority to seize indicia evidence to support a sentencing enhancement did not justify the level of intrusion and excessive property damage that occurred during the searches. The indicia to be seized were not evidence of a crime. Its limited probative value in a sentencing hearing was not sufficient to excuse the property

damage suffered by individuals who were neither codefendants in the murder case nor charged with any criminal offense.

The Ninth Circuit was unpersuaded by the affiant's argument that he instructed his fellow officers to seize anything bearing Hell's Angels indicia, because the search warrants referred to "any evidence of membership . . . any reference to 'Hell's Angels.' " *Id.* at 967. He surmised that "any" meant "all" and that the officers had no discretion. Thus, they were required to seize everything listed in the warrant. The Court noted that "any" as used in the search warrant did not mean "all" and that the warrant did not mandate that officers were to seize everything. *Id.* at 974–75. Rather, the officers retained discretion as to how they would reasonably execute the warrant. *Id.* at 973–74 (citing *Marron v. United States*, 275 U.S. 192, 196 (1927)). *See also Strauss v. Stynchcombe*, 165 S.E.2d 302, 307 (Ga. 1968) ("We do not believe that it was the intention of the Supreme Court . . . to lay down any such rule . . . that the searching and seizing officer be left no room to make a judgment as to what particular documents or things are subject to seizure under the warrant which he is executing."). Finally, evidence in the record indicated that other officers participating in the searches understood that they had discretion not to seize every item of Hell's Angels indicia and, indeed, declined to seize some items, including a blue bus. *San Jose Charter*, 402 F.3d at 974. The unreasonableness of the search was underscored by the fact that none of the indicia seized in the searches—not even the photographs—were introduced at trial. *Id.* at 974–75.

Finally, the Ninth Circuit addressed the reasonableness of shooting and killing three dogs during the execution of the search warrants. Citing the record developed by the district court below, the Ninth Circuit emphasized that the officers had a week to plan for the entry and had advance notice of the existence of the dogs. Despite this, the officers had developed no operational plan for immobilizing the dogs, except to shoot them. The court was unpersuaded by the defendant's contention that stealth and speed in the execution of the warrants, coupled with officer safety, justified shooting the dogs. *Id*. at 976.

Having concluded that the officers violated the plaintiff's Fourth Amendment rights for purposes of the first step in the qualified immunity analysis, the court went on to conclude that the constitutional right was clearly established and that a reasonable official would have understood that what he was doing violated that right. The Ninth Circuit cited a long list of cases standing for the proposition that unnecessary destruction of property in the course of executing a search warrant is unconstitutional. *Id.* at 977. *See generally Liston v. County of Riverside*, 120 F.3d 965, 979 (9th Cir. 1997). In assessing reasonableness under the Fourth Amendment, whether the officers considered alternatives before undertaking intrusive activity is an appropriate factor to consider. *See San Jose Charter*, 402 F.3d at 977–78 ("[T]he Fourth Amendment forbids the killing of a person's dog, or the destruction of a person's property, when that destruction is unnecessary—i.e., when less intrusive, or less destructive, alternatives exist."). In sum, a lack of adequate planning prior to execution of the warrants, coupled with a less than compelling need for the destruction of property, and the violation of a clearly established constitutional right supported the district court's denial of the defendants' motion for qualified immunity. *See id.* at 978–79.

VI. Conclusion

In sum, indicia search warrants afford prosecutors a powerful tool for locating and seizing "mere evidence" of association, not limited to the instrumentalities or fruits of the crime or contraband. The sheer variety and scope of evidence that may be covered by an indicia search warrant has caused federal courts to scrutinize affidavits in support of these warrants, and the warrants themselves, with care. The advantages for prosecutors of indicia evidence are obvious. What better way to demonstrate the existence of the gang than the clothing, personal effects, symbols, and slogans that tie them together as an organization? But the challenges associated with indicia warrants and searches are noteworthy also. Concise, specific drafting of the affidavit to demonstrate the shared identity and criminal purpose of the gang is essential. Specific information tending to show that indicia evidence to be seized has a nexus to

the gang associated and criminal activity alleged is imperative. The nexus between the known gang members, the indicia evidence, and the place to be searched must also be specified. The warrant itself must describe precisely the items sought. Finally, officers executing an indicia warrant must be prepared to demonstrate their compliance with the reasonableness requirement of the Fourth Amendment. Was there sufficient planning prior to the execution of the search warrant? Were reasonable efforts made to minimize property damage? Was discretion exercised appropriately insofar as the manner of seizure and the quantity of evidence seized?

With careful drafting and well-planned execution, indicia search warrants afford prosecutors the opportunity to locate and introduce some of the most powerful and vivid evidence of a gang's criminal association. This evidence helps a jury understand the very nature of what constitutes a criminal gang or enterprise. ❖

ABOUT THE AUTHOR

❑ **Gretchen C. F. Shappert** is the Assistant Director for the Indian, Violent and Cyber Crime Staff at the Executive Office for U.S. Attorneys. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004 to 2009. She was also an Assistant U.S. Attorney from 1990 to 2004 and specialized in violent crime and outlaw motorcycle gang prosecutions. ✠

Gangs, Guns, Drugs, and Money

Jason F. Cunningham
National Narcotics Coordinator
Office of Legal and Victim Programs
Executive Office for United States Attorneys

Sharon R. Kimball
Associate Director
Organized Crime Drug Enforcement Task Forces

I. Introduction

A quick Internet search of gangs in America revealed a plethora of Web sites and books devoted to the culture and history of gang life in the United States. The FBI estimated that 1.4 million people belong to 33,000 gangs in this country. *See* THE FBI: GANGS (2014), *available at* http://www.fbi.gov/about-us/investigate/vc_majorthefts/gangs. The books and articles delve deeply into why young persons from particular neighborhoods join certain gangs and how the gang provides security, alternate values, culture, and familial structure. The Department of Justice (the Department) employs investigators and prosecutors who have prosecuted gangs for their entire careers and who can speak readily to gang life. This article focuses on the narrow goal of prosecuting major street gangs utilizing the Department's Organized Crime Drug Enforcement Task Forces Program (OCDETF).

As its name suggests, the OCDETF Program explicitly targets organized crime. The criminal organizations targeted in OCDETF cases very often include major gangs. Established in 1983, OCDETF is a multi-agency program that combines the resources and expertise of investigative agents from three

federal executive Departments—the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Drug Enforcement Administration (DEA), the FBI, and the U.S. Marshals Service in the Department of Justice; Homeland Security Investigations/Immigration and Customs Enforcement and the U.S. Coast Guard in the Department of Homeland Security; and the Internal Revenue Service, Criminal Investigation Division, in the Department of the Treasury—together with state, local, and tribal investigators, as well as prosecutors in all the U.S. Attorneys' offices and the Department's Criminal Division.

OCDETF's mission is to identify, disrupt, and dismantle the transnational, national, and regional criminal organizations most responsible for the illegal drug supply in the United States, the diversion of pharmaceutical drugs, and the violence associated with the drug trade. *See* ORGANIZED CRIME DRUG ENFORCEMENT TASK FORCES (2014), *available at* http://www.justice.gov/criminal/taskforces/ocdetf.html.

The organizations targeted by OCDETF's multi-agency task forces include the international sources of supply of illegal drugs, their international and domestic transportation organizations, their regional and local distribution networks, their money launderers and financial infrastructure, and their violent enforcers. In addition to drug trafficking, these organizations typically engage in multiple forms of organized criminal activity, such as violence, terrorism, corruption, human smuggling, trafficking in persons, weapons trafficking, complex financial crimes, and other illegal activities that threaten the safety of our society and the security of our nation. Consequently, OCDETF agents and prosecutors have always targeted major street gangs.

At a certain point, some street gangs turn a corner from having a loose affiliation with a subculture that controls small street drug sales to "become more organized, adaptable, and influential in large-scale drug trafficking." NAT'L GANG INTELLIGENCE CTR., FED. BUREAU OF INVESTIGATION, NATIONAL GANG THREAT ASSESSMENT—EMERGING TRENDS 11 (2011), *available at*, http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment (National Gang Threat Assessment). Increasingly, gang membership and drug trafficking reaches across state and national boundaries. According to the 2011 National Gang Threat Assessment, prepared by the National Gang Intelligence Center, "[m]any US-based gangs have established strong working relationships with Central America and Mexico-based DTOs to perpetuate the smuggling of drugs across the US-Mexico and US-Canada borders." *Id.* Criminal gangs protect their growing enterprise through the use of violence and intimidation. *Id.* The Department targets violent and multi-jurisdictional street gangs through a "multifaceted approach" that includes balancing strong enforcement with prevention programs. *Beyond the Streets: America's Evolving Gang Threat: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security Committee on the Judiciary*, 113th Cong. (2012) (Statement of the U.S. Dep't of Justice), *available at* http://www.justice.gov/ola/ testimony/112-2/07-25-12-doj-statement.pdf. The OCDETF mission of prosecuting the most serious drug trafficking organizations fits comfortably within this strategy and can prove a valuable enforcement vehicle to tackle this public safety problem. OCDETF offers partnership, coordination, additional resources, and experience that can prove essential in tackling a criminal enterprise such as a violent street gang.

II. OCDETF Program Guidelines

The OCDETF Program Guidelines are very specific and define the types of investigations appropriate for OCDETF designation and, consequently, for use of OCDETF investigative and prosecutorial resources. The OCDETF Program Guidelines do not require that every OCDETF prosecution include specific drug charges, but every OCDETF prosecution must be drug-related. That is, the specific charges may be Racketeer Influenced and Corrupt Organizations Act charges (RICO), tax, money laundering, currency, weapons, explosives, immigration, customs, or other non-drug violations, as long as the targets have been identified as major drug violators and otherwise meet the OCDETF standards.

If a criminal organization or gang engages in violence or weapons trafficking in the course of producing or distributing illegal drugs in multiple judicial districts or localities, a federal prosecutor seeking OCDETF certification should highlight this associated violence or weapons trafficking aspect in the case proposal. An investigation targeting a criminal organization or violent gang that distributes small amounts of illegal drugs in a single judicial district or locality may be appropriate for OCDETF designation if the OCDETF case proposal demonstrates intent to work up the chain of supply to the organization's or gang's source of supply. In such instances, the proposal must: (1) demonstrate that the organization or gang currently has linkage to, or has the demonstrated potential to link to, components and/or facilitators of regional, nationwide, or international drug trafficking or money laundering organizations, and (2) explain the investigative plan to further identify, disrupt, and dismantle the components or facilitators of the regional, nationwide, or international organization.

OCDETF designation is also appropriate for investigations against violent criminal organizations or gangs that may not yet have linkage to, or the demonstrated potential to link to, components and/or facilitators of regional, nationwide, or international drug trafficking or money laundering organizations, but are actively engaged in violence and produce or distribute large amounts of illegal drugs in multiple judicial districts or localities.

In its more than 30-year history, OCDETF has targeted more than 1,000 gangs nationwide. OCDETF also keeps a single, interagency list of the most significant criminal organizations operating in or impacting each of OCDETF's nine Regions. These are designated as Regional Priority Organization Targets (RPOTs). The FY 2014 OCDETF RPOT List includes many well-known national gangs, such as the Almighty Latin King and Queen Nation, Barrio Azteca, Black Disciples, Black Mafia Family, Black Guerilla Family, Bloods, Gangster Disciples, Insane Spanish Cobras, Mexican Mafia, Mickey Cobras, Nuestra Familia, Sons of Silence, Sureños, and Vice Lords. According to statistics provided by OCDETF, in fiscal year 2013 alone, OCDETF components in 64 districts, from all 9 OCDETF Regions, initiated 143 new cases targeting gangs.

III. OCDETF case examples

Three recent OCDETF investigations highlight the powerful tools that the OCDETF program can bring to major street gang investigations that involve significant investigative resources and considerable state and local assistance.

A. Operation Victory

Chicago, Illinois made national headlines for registering more total homicides than any city in the nation in 2012. Clarence Page, *Treat Chicago's homicide surge as an epidemic*, CHICAGO TRIBUNE (Jan. 9, 2013), *available at* http://articles.chicagotribune.com/2013-01-09/news/ct-oped-0109-page-20130109_1_homicide-surge-street-gangs-gun-control. Chicago is home to approximately 600 gangs or gang factions, and local public officials attributed a spike in murders in 2012 to gang warfare between these factions. Jeremy Gorner, *Gang factions lead to spike in city violence*, CHICAGO TRIBUNE (Oct. 3, 2012), *available at* http://articles.chicagotribune.com/2012-10-03/news/ct-met-street-gang-bloodshed-20121003_1_gang-violence-gangster-disciples-black-p-stones. This OCDETF investigation targeted members of the largest street gang in Chicago, the Gangster Disciples. Chicago police attributed approximately 400 murders to the Gangster Disciples in 2012. *Id.* As noted above, they are an OCDETF RPOT. On August 12, 2012, a federal judge sentenced a longtime, high-ranking member of the Gangster Disciples street gang, Victor Thompson, to more than 28 years in federal prison for distributing quantities of crack cocaine, heroin, and marijuana in low-income neighborhoods throughout the city of Chicago over the course of a decade.

Founded in the 1960s, the Gangster Disciples expanded from a loose affiliation to a multistate drug distribution network with a corporate structure. DEA and the Chicago Police Department arrested

Thompson and seven codefendants for conspiracy to distribute crack cocaine in May 2007. Agents recovered a loaded firearm with a defaced serial number in Thompson's bedroom during his arrest. At the time of his arrest, law enforcement believed Thompson held the status of a "Board Member" within the Gangster Disciples hierarchy. In this leadership role, he controlled a crack cocaine trafficking organization that included fellow Gangster Disciples, as well as non-gang members in the West Pullman neighborhood on the south side of Chicago. Law enforcement had seized a chart depicting the Gangster Disciples hierarchy from a previous investigation into the head of the Gangster Disciples in 1995. At that time, the chart indicated Thompson oversaw 200 members of the gang. Thompson also charged local drug dealers "street taxes" to deal drugs in the area under his control. Thompson and his codefendants enforced this system through torture and violence, according to court records. Specifically, Thompson and his codefendants used a heated coat hanger to persuade drug dealers to part with some of their proceeds. At sentencing, the Government provided information to the court that Thompson was responsible for overseeing a system that channeled approximately 13,505 kilograms of crack cocaine, 739.6 kilograms of heroin, and 425,412 kilograms of marijuana into Chicago's neighborhoods. All defendants in *United States v. Thompson* have been convicted and sentenced to lengthy prison terms. *See* Indictment, *United States v. Thompson*, 1:07-cr-00263-1(D. Ill. 2007).

B. Operation Knock-Out

On June 24, 2005, Varrio Hawaiian Gardens gang member Jose Orozco gunned down Los Angeles County Sheriff's Deputy Jerry Ortiz. Press Release, Federal Bureau of Investigation, Investigation Targeting Varrio Hawaiian Gardens Gang and Associates is Largest Gang Case in U.S. History with Nearly 200 Defendants Named in Federal Indictments (July 8, 2002), *available at* http://www.fbi.gov/losangeles/press-releases/2009/la070809.htm. While the state successfully prosecuted Orozco, and he currently sits on death row, the investigation expanded exponentially into the Varrio Hawaiian Gardens gang as OCDETF Operation Knock-Out. A task force led by the U.S. Attorney's Office for the Central District of California and comprised primarily of the FBI, DEA, IRS, and the Los Angeles County Sheriff's Department, Operation Knock-Out led to the prosecution of George Manuel Flores in 2009 as the lead defendant in a 57-count racketeering indictment. *See id.*; Indictment, *United States v. Flores*, CR 09-445-DSF (C.D. Ca. 2002). Operation Knock-Out aimed to dismantle the Varrio Hawaiian Gardens leadership through the use of the RICO Act, but it also endeavored to disrupt the drug supply flowing to the gang. The Flores indictment served as the centerpiece of the largest gang prosecution in U.S. history, comprised of 7 multi-defendant federal indictments charging 212 defendants. The Los Angeles County district attorney charged additional defendants in state court. During the takedown, law enforcement seized 33 pounds of methamphetamine and 125 firearms. Press Release, Federal Bureau of Investigation, Investigation Targeting Varrio Hawaiian Gardens Gang and Associates is Largest Gang Case in U.S. History with Nearly 200 Defendants Named in Federal Indictments (July 8, 2002), *available at* http://www.fbi.gov/losangeles/press-releases/2009/la070809.htm.

A Hispanic multi-generational gang, the Varrio Hawaiian Gardens gang (VHG) dates back to the 1950s. Comprised primarily of Hispanic men, VHG started out as a low-level street gang that committed street robberies and corner drug deals. At the time of the OCDETF investigation, it had an estimated 1,000 members from 4 family generations. As a Sureños gang, VHG operates under the control of La Eme, or the Mexican Mafia. Members of the Mexican Mafia also come from the ranks of Hispanic street gangs, including the Hawaiian Gardens. The VHG pays a tribute to the Mexican Mafia to solidify control over their territory and to assure protection of VHG members when they enter the California penal system. Failure to pay the tribute would open up VHG members to retribution from other Sureños street gang members.

The VHG takes its name from the location of its birthplace and current principal location in the city of Hawaiian Gardens, California. Hawaiian Gardens has around 14,000 residents and takes up one square mile in Los Angeles County. VHG is the only street gang operating in Hawaiian Gardens. Yet,

according to the lead Assistant U.S. Attorney, the large size of the street gang and the small size of the city provided Hawaiian Gardens with the moniker "gang city." Narcotics trafficking provided the primary source of funding for the VHG. The gang itself distributed methamphetamine, cocaine base, heroin, crack cocaine, and marijuana. However, VHG also extorted a tax from non-VHG drug dealers within Hawaiian Gardens. All drug dealers who paid the tribute received protection from the gang. Gang members referred to themselves as the "Hate Gang" due to their systematic hate crime campaign against the African American community within their turf. Once a potential new member has committed a sufficiently violent crime, witnessed by other members, the new member is initiated into the gang by getting a physical beating. Committing crimes of violence gives greater prestige to certain members of the VHG referred to within the gang as a "shot caller." George Flores was one such shot caller who organized meetings, collected taxes from drug dealers, and issued orders to other members of the gang.

For more than a decade, the lead defendant, Flores, with the assistance of other defendants, ran multiple houses that dealt cocaine, heroin, methamphetamine, and marijuana 24 hours a day, 7 days a week. The indictment also alleged numerous crimes of violence, perpetuated by Flores and other members of the conspiracy, against African American community members, solely due to their race. Flores pleaded guilty on March 26, 2010, to five counts: racketeering conspiracy; conspiracy to distribute and possess with the intent to distribute crack cocaine, methamphetamine, heroin, and marijuana; two counts of possession with the intent to distribute heroin; and being a felon in possession of ammunition. The court sentenced Flores to 30 years in prison. Other VHG shot callers that received significant sentences included: Alberto Martinez (sentenced to 260 months), Alberto Vera (sentenced to 234 months), and Brian Viramontes (sentenced to 210 months). Additionally, the Operation Knock-Out investigation and the subsequent prosecutions removed from the community many of the suppliers who provided VHG with narcotics. Suppliers included: Marcus Romero (sentenced to 291 months), Vincent Ramirez (sentenced to 264 months), Frank Henley (sentenced to 262 months), Leobardo Valenzuela (sentenced to 188 months), Luis Magana (sentenced to 173 months), and John Sotelo (sentenced to 168 months).

The Los Angeles County Sheriff's Department estimates that gang-related crime decreased 75 percent in Hawaiian Gardens since 2005, and VHG current membership in Hawaiian Gardens has declined 30 percent.

C. Operation Petticoat

Craig Petties, also known as "Lil C," received nine concurrent life sentences from a federal judge in the Western District of Tennessee, on August 22, 2013. Petties ran a drug trafficking organization in Memphis, Tennessee, that distributed hundreds of kilos of Colombian cocaine in Georgia, Mississippi, North Carolina, South Carolina, and Tennessee, on behalf of a Mexican cartel, but he got his start as a member of the Gangster Disciples street gang selling crack rocks on the street corners in South Memphis.

The U.S. Attorney's Office for the Western District of Tennessee prosecuted Petties in *United States v. Petties*, No: 02-20449, 2011 WL 6826656, at *1 (W.D. Tenn. Dec. 28, 2011), as part of OCDETF Operation Petticoat. Due to his prolific regional drug distribution activities and a penchant for murdering rivals and associates, OCDETF designated Petties as an RPOT. On January 30, 2008, a grand jury returned a 56-count indictment (sixth superseding) against Petties and six others for committing crimes that included murder, drug trafficking, violent crime in aid of racketeering activity, and financial charges during the period 1995 to 2008. The financial charges included 39 individual money laundering counts.

In the mid-1990s, Petties developed a reputation as a major supplier of cocaine in the Memphis area, who could move his product at a fast clip. The Petties drug trafficking organization (Petties DTO) included friends and family members within the Gangster Disciples. This success landed him on Edgar Valdez Villarreal's radar screen. A Texas-born and high ranking member of the Beltran Leyva Mexican

cartel, Villarreal had the ability to provide Petties with an ample supply of Colombian cocaine that arrived in Mexico on submarines and barges. The cocaine progressed across the Texas border on FedEx and other trucks to its ultimate destination in Tennessee. Sometimes the drugs were heavily wrapped and hidden in shipments, such as food headed to local grocery store chains. Petties and his cococonspirators would then ship the cash proceeds back to Texas and, ultimately, Mexico.

With his cocaine proceeds, Petties purchased real estate in Memphis and a $2.3 million house in Las Vegas, a fleet of cars, and thousands of dollars' worth of jewelry. The OCDETF investigation identified, and the Government forfeited, vehicles that included a 2002 Bentley valued at $339,000, a 1998 Chevrolet Corvette, a 1997 Jaguar XK8, a 2000 Jaguar S-Type, a 2000 Land Rover, a 2000 Mercedes CL500, a 2002 Ford F150 Harley Davidson Edition Pickup Truck, and a 2003 Mercedes 500-SL valued at $111,650. In total, this investigation led to the seizure of approximately $2,962,046, including $633,577 in cash and 40 vehicles.

OCDETF Operation Petticoat had humble beginnings. In 2001, Petties' girlfriend called the police to their home when the couple got into a fight. Responding officers smelled marijuana and noticed a partially smoked joint in an ashtray. A subsequent search turned up 600 pounds of marijuana in a bedroom closet. Petties had a few juvenile arrests, and investigators had received information that Petties moved substantial quantities of narcotics. However, this incident confirmed to law enforcement that Petties was indeed a major narcotics drug trafficker in the Memphis area. A federal grand jury indicted Petties in 2002 and issued a warrant for his arrest. Petties successfully fled to Mexico, where he remained in hiding under the protection of the cartel for the next five years. The evolving investigation established that Petties continued to run his drug trafficking operation from Mexico. The U.S. Marshals added him to their Top 15 List of Most Wanted Fugitives in August 2004, and the "America's Most Wanted" TV show featured his case. Petties' flight from justice ended when Mexican military and police officers raided his white stucco home in an upscale suburb 136 miles northwest of Mexico City in January 2008.

Petties pleaded guilty to charges including RICO, violent crime in aid of racketeering (VICAR), conspiracy to commit murder for hire, conspiracy to distribute narcotics, and money laundering. He admitted to having a role in four murders as well as ordering a man's kidnapping and torture. Petties committed these acts based on the belief that these individuals either provided information to the Government as informants or stole drugs from his organization. Two of his main associates in the Petties DTO, Martin Lewis and Clinton Lewis, elected to go to trial on the charges against them. The trial lasted seven weeks in February and March of 2012. The jury returned a guilty verdict on all counts against Martin Lewis, including charges of RICO, money laundering and conspiracy to commit murder for hire, and returned a guilty verdict on all but one count against Clinton Lewis, including a guilty verdict on charges of RICO, VICAR, conspiracy to distribute narcotics, money laundering, and conspiracy to commit murder for hire. Both Martin Lewis and Clinton Lewis received life sentences. Over 30 defendants have been charged and convicted as part of this investigation.

IV. Conclusion

The common threads that weave these gangs together involve large membership, established drug trafficking, cohesive organization, and the ready use of violence to promote the gang's objectives of trafficking drugs and making money. The defendants in these cases faced a myriad of charges that went beyond drug trafficking and included RICO, financial charges, and weapons charges. Their charges revolved around gangs, guns, drugs, and money. As the song *Love and Marriage* by Frank Sinatra goes, "Try, try, try to separate them, it's an illusion. Try, try, try and you only come to this conclusion. . . . You can't have one without the other." Frank Sinatra, *Love and Marriage*, on THIS IS SINATRA! (Capitol Records 1955).

Often these major street gangs impact and involve multiple jurisdictions, but as Operation Victory demonstrates, the absence of this factor does not preclude having the case brought to OCDETF. Operation

Knock-Out shows how prosecutors and investigators in the field developed a dual purpose mission to both use RICO to charge and prosecute a significant amount of gang members, and also to proactively work the case to the drug-supply level. Operation Petticoat illustrates the transition of a low-level gang member to a leader of a violent drug trafficking organization. Importantly, this prosecution also tackled the financial gains generated by this DTO.

These cases illustrate the conclusions reached by the National Gang Threat Assessment in 2011: that street gangs have the ambition and ability to elevate beyond a loose affiliation engaged in corner drug deals and turf protection, to become cohesive and violent enterprises that distribute narcotics on a large-scale level. In turn, federal prosecutors must also elevate their cases to the OCDETF level to increase resources, expertise, and coordination between federal, state, and local law enforcement to combat these threats to public safety. ❖

ABOUT THE AUTHORS

❑ **Jason F. Cunningham** currently serves as the National Narcotics Coordinator within the Office of Legal and Victim Programs at the Executive Office for United States Attorneys (EOUSA). He has worked within EOUSA since 2009 and is a prior contributor to the U.S. Attorneys' Bulletin. From 2011 to 2012, he served as a Special Assistant U.S. Attorney within the U.S. Attorney's Office in the District of Columbia, and he served a detail to the White House in 2010. ✠

❑ **Sharon R. Kimball** was an Assistant U.S. Attorney for 18 years, first in the Northern District of Texas and later in the District of New Mexico. She began prosecuting OCDETF cases in 1990 and continued to do so until 2008, when she moved to Washington, DC to become the Associate Director of OCDETF. ✠

The authors wish to thank Assistant U.S. Attorneys Rachel Cannon, Michael Lowe, and David Pritchard for their assistance with the details of the cases.

Sex Trafficking and Gangs: A Deliberate Approach

Adrian L. Brown
National Civil Rights Coordinator
Office of Legal and Victim Programs
Executive Office for United State Attorneys

"These guys are criminals out to make money and they don't care who they exploit, who they damage, to get their ultimate goal, which is their own financial gain. If they weren't trafficking girls, they might be trafficking in firearms or other illegal contraband." Interview by Junior League of Portland with S. Amanda Marshall, U.S. Attorney, District of Oregon, in Portland, Or. (Aug. 31, 2013), *available at* http://vimeo.com/73541715. (Marshall Interview).

"You have a product that you don't have to keep in inventory. You don't have to purchase it. You don't have to wait for the money to come back on this product and then buy it from the supplier. You are not as exposed as you are if you are caught with drugs to being caught with a woman or a girl." Interview

by Amita Sharma with Laura Duffy, U.S. Attorney, Southern District of California, in San Diego, Cal. (Jan. 27, 2014), *available at* http://www.kpbs.org/news/2014/jan/27/sex-trafficking-overtakes-drugs-san-diego-county-g/.

I. Introduction

These quotes from two of our U.S. Attorneys, at opposite geographical ends of the west coast, illustrate how gangs have become deliberate in choosing to sell minor girls and women whom they have coerced into being sex slaves. In turn, U.S. Attorneys' offices must be even more deliberate about the investigation and litigation of these cases to keep our communities and our children safe.

A deliberate approach to these cases does not just mean being diligent about efforts to combat sex trafficking. Ensuring that the prosecutors assigned to these cases are familiar with the unique and complex contours and layers involving a gang-controlled, gang-related, or gang-affiliated enterprise will best serve the community, the victims, and justice. And, because these cases rest on victim testimony, they must be approached by investigators and prosecutors with a victim-centered mindset. As J.R. Ujifusa, a Deputy District Attorney in Multnomah County, Oregon and a Special Assistant U.S. Attorney for the District of Oregon, stated in his interview with the Junior League of Portland, these cases are "domestic violence, gang, drug, sexual assault, all built into one case." Interview by Junior League of Portland with J.R. Ujifusa, Special Assistant U.S. Attorney, District of Oregon, in Portland, Or. (Sept. 3, 2013), *available at* http://vimeo.com/73672801 (Ujifusa Interview).

An example of the culmination of all of these types of cases being wrapped into a single sex-trafficking case can be found in *United States v. Jose Ciro Juarez-Santamaria*, 513 F. App'x 306 (4th Cir. 2013), from the Eastern District of Virginia. In that case, the leader of the Pino Locos clique of the MS-13 gang was convicted of the sex trafficking of a 12-year old girl, whom the defendant had encountered at a party. She informed the defendant that she had run away from home and needed help. The defendant and his associates took the victim in and began to sell her in the commercial sex market the very next day. In addition to selling the victim for cash, the defendant and coconspirators allowed other MS-13 members to engage in sex acts with the victim, free of charge. Throughout the course of the conspiracy, the defendant and his coconspirators plied the 12-year old with marijuana and alcohol prior to sex acts. The defendant was convicted at trial and sentenced to life imprisonment. *Id.* at 307–08.

This article by no means captures all of the complexity and issues in gang-related sex trafficking cases. Rather, this article intends to share information and resources enabling prosecutors to approach gang-related sex trafficking cases in a deliberate manner, separate and distinct from labor trafficking cases. Indeed, the issues and complexity in labor trafficking cases deserve a separate discussion. Viewing gang-related sex trafficking cases through the lens of domestic violence, gangs, drugs, and the sexual assault of minors and adults may allow for more of a focus on the victims and, subsequently, more of an impact at trial and sentencing.

II. Five deliberate approach efforts

A. Victim focus

As U.S. Attorney Marshall explained in her interview with the Junior League of Portland, "you may have a loose network of pimps between Seattle, Portland, Las Vegas where girls are going between cities. It facilitates their criminal activity to keep these girls moving so that they don't form connections with people, so that their families can't find them, so that they remain isolated." Marshall Interview. And the more a child or vulnerable woman is isolated and dependent on her pimp for her basic self-care needs, the more she may feel allegiance to him.

The approach to these trafficking cases must be different simply because of the fact that they involve extremely vulnerable and damaged children and women. Child victims must have a separate and distinct protocol for intervention from that used in adult labor trafficking cases. Their cases should involve child abuse assessment and sexual assault response personnel. Certainly, being mindful of the impact of trauma on victims does not mean prosecutors should do whatever the victim thinks is best. Indeed, a victim may very well believe the best thing for her is to run away. So, while a material witness warrant is not ideal (and typically a last resort), it may be necessary. Moreover, being informed and attentive to a victim's trauma and vulnerabilities is consistent with keeping the target, the pimp, the center of the prosecution.

The District of Oregon provides a model for such a deliberate approach. Instead of combining adult foreign-born labor trafficking and sex-trafficking cases into one human trafficking unit, U.S. Attorney Marshall deliberately placed the labor trafficking with her civil rights prosecutors and the child sex-trafficking cases with her gang unit prosecutors who work with the state, local, and federal gang task forces. As a result, the District of Oregon filed three times the number of sex trafficking cases in 2011 than in the previous few years. And, with the ability for labor trafficking cases to be given their own focus and necessary community outreach, for the first time, the District now has several ongoing labor trafficking investigations. Marshall Interview.

B. Utilization of local resources

Not only is each district required to participate in a Human Trafficking Task Force, much of the success in prosecuting gang-related sex trafficking cases is tied to the work of such a task force. For example, in the Eastern District of Virginia, the Northern Virginia Human Trafficking Task Force (NVHTTF) is a collaboration of federal, state, and local law enforcement agencies dedicated to: (1) investigating and prosecuting those engaged in sex trafficking, forced labor, and closely related crime; (2) identifying, rescuing, and providing services to victims of human trafficking; and (3) conducting training, community outreach, and public awareness efforts.

Such a task force may receive crucial resources through the Bureau of Justice Assistance and the Office of Victims of Crime. In October 2012, the NVHTTF was awarded a $1 million grant over a two-year period. Half of the funding is being used to support a full-time detective and a crime analyst to work in a newly-formed Human Trafficking Unit at the Fairfax County Police Department, as well as supporting law enforcement training, investigative travel, equipment, and related efforts to combat human trafficking. The NVHTTF is using the remaining $500,000 to support the Polaris Project, a leading anti-trafficking organization. Such support will serve victims of human trafficking through referrals to other non-governmental organizations engaged in similar efforts in northern Virginia, as well as initiatives to increase training, community outreach, and public awareness related to human trafficking.

Utilization of local resources may also come in the form of research by local universities. For example, in 2011, Portland State University published research on the efforts by the Clark County Juvenile Court in Vancouver, Washington, to identify and divert children of sex trafficking from juvenile detention to advocates and community resources. *See* EMILY J. SALISBURY & JONATHAN D. DABNEY, DIVISION OF CRIMINOLOGY AND CRIMINAL JUSTICE, PORTLAND STATE UNIVERSITY, YOUTH VICTIMS OF DOMESTIC MINOR SEX TRAFFICKING IN CLARK COUNTY JUVENILE COURT: IMPLEMENTING AN IDENTIFICATION AND DIVERSION PROCESS 14 (2011), *available at* http://www.pdx.edu/cjpri/sites/www.pdx.edu.cjpri/files/DMST%20CCJC%20Report-Without%20Appendices_0.pdf. In 2013, U.S. Attorney Marshall collaborated with the same university to gather statistics concerning the extent of the child sex trafficking crisis in the Portland metropolitan area. *See* Press Release, U.S. Attorney's Office, District of Oregon, Hundreds Of Children Are Being Trafficked For Sex In Portland (Aug. 5, 2013), *available at* http://www.justice.gov/usao/or/news/2013/20130805_CSEC.html. Without such data on the scope of the problem, local law enforcement may not be provided with adequate resources by local policymakers.

C. Mindful collaboration of stakeholders

> Like domestic violence and child abuse, addressing this issue really takes a collaborative community-based response. There is room for everybody at the table because everybody is needed. This isn't just a law enforcement issue, it's a child welfare issue, it's a social and moral values issue. It's really an issue that we all need to stand up and decide whether or not this is the community we want to live in is a community where children are raped in hotel rooms for money.

Marshall Interview.

Portland's strong, collaborative, community-based participation to address child sex trafficking provides a go-by for a mindful collaboration of stakeholders. Such a group of stakeholders includes:

- Victim advocates and social workers who are knowledgeable of the issues that plague juvenile victims, such as hostility and allegiance to pimps
- Survivors who have made it out of the life of sex trafficking and can help with peer mentorship
- State, federal, and local law enforcement who work gang investigations
- State child welfare workers who may be familiar with the victims and their medical and mental health issues
- Juvenile justice workers who have encountered victims previously
- Local legislators (both city and county council)

To ensure ongoing collaboration in combating sex trafficking in Portland, the law enforcement and child welfare stakeholders meet on a monthly basis. Assistant U.S. Attorneys (AUSAs) and county prosecuting attorneys, along with FBI Agents on the Child Exploitation Task Force, local sex crimes detectives, Prostitution Coordination Team officers, and county jail intelligence deputies, meet together with staff from the state's Department of Human Services (DHS). AUSA Leah Bolstad, one of U.S. Attorney Marshall's gang prosecutors in Portland, attests to this type of collaboration resulting in a more deliberate pursuit of gang involved sex trafficking cases. An example of such collaboration is offered below.

> A jail deputy reports to the group about how a minor girl visited a newly booked inmate and known gang member. The DHS case worker then recognizes the girl's name as being involved in state dependency proceedings and has family or other contact information. The PCT officers also recognize her as a girl they previously picked up on the streets and she had agreed to a consensual search of her phone (that is, a "phone dump" or "phone download") that later becomes helpful in the investigation of another pimp.

AUSA Bolstad succinctly describes these collaborative meetings as being "incredibly helpful." Interview by Adrian L. Brown with Leah Bolstad, Assistant U.S. Attorney, District of Oregon, in Portland, Or. (Apr. 14, 2014). While she was initially amazed at how each of the stakeholders was familiar with the names of the girls or the girls' families, within a year of attending, she too became well-versed in these inter-agency discussions. *Id.*

D. Understanding the pimps and recruitment—follow the money

A defendant's motivation may help direct your case strategy, and gang-related sex trafficking is no different. Simply stated, it is all about the money. However, a gang-related or gang-affiliated pimp may not fit your typical thuggish gang-member profile. Instead, these defendants may have a legitimate

day job, and they may be attractive and well spoken. Furthermore, they may be connected to the trade through familial networks.

"Some of these pimps come from multi-generational families of sex traffickers. So, these are kids that grow up watching uncles, fathers, or big brothers be involved in the business. Sometimes they are organized with each other. Sometimes the pimps are sharing girls." Marshall Interview.

They will almost certainly use the latest social media and smartphones to sell their "product." For example, in the case of *United States v. Strom*, Nos. 1:12cr159, 1:13cv555, 2013 WL 6271932, at *1 (E.D. Va. Dec. 4, 2013), five members or associates of the Crips gang were arrested in the Eastern District of Virginia for sex trafficking high school girls. The girls were not only recruited in schools and in metro stations, but also on Facebook, MySpace, and DateHookUp.com. The defendants then advertised their victims through online sites including Craigslist.org and Backpage.com. Justin Strom was convicted and sentenced to 40 years' imprisonment. *Id.*

Indeed, conducting a sex trafficking threat assessment in your district can assist in understanding pimps' sources for vulnerable children and women. At the National Advocacy Center's recent Human Trafficking Seminar, Hilary Axam, the Director of the Human Trafficking Prosecution Unit in the Civil Rights Division, explained that conducting such an assessment can assist in identifying sex trafficking cases. Such an assessment may include asking the following questions in your taskforce or other stakeholder meetings:

- Where is commercial sex prevalent or tolerated?
- Which businesses have contact with prostitution activity? Strip clubs, massage parlors, tattoo parlors, hotels, motels, cantinas and nearby stores, bodegas, or clinics
- Where are concentrations of male customers? Casinos, hunting lodges, oil fields, military bases, migrant labor camps
- Where are concentrations of vulnerable children and women? Halfway houses, drug and alcohol rehabilitation centers, youth detention centers, youth and domestic violence shelters, foster homes
- What are the frequented Internet and social media sites in your district for sex advertisements?

E. Make an impact on demand: holding the johns accountable

It is not only important to deliberately conduct outreach to educate your community about the problems, but also to hold the johns accountable and make them aware of the realities of what their money is actually buying. In Multnomah County, Oregon, an eight-hour "John School" is held every other month to educate these men about the realities for the victims of their crimes and to dispel misconceptions. Such a program sheds light on what the victims are made to do and how they may be beaten, tattooed, and branded by the pimps to whom they are enslaved. The curriculum consists of the following:

- A pre-test gets information on the john's background.
- The health department provides graphic images and describes the risks of engaging in the crime.
- A Sexual Assault Response Coordinator discusses her work with minor victims to dispel the notion that this is a victimless crime.
- A survivor discusses her experiences, how her life and relationships have been affected.

- A program called "Lifeworks" provides information on forming healthy relationships and where to find help.
- Law enforcement personnel provide information about the profile of sex traffickers.
- The district attorney's office discusses the consequences of the crimes.
- A community member from a high vice area discusses the impact of sex trafficking in the neighborhood and the impact on the quality of life for children who are unable to play safely outside.

A key to the success of the program is that the material in the program is constantly revised to make it fresh and up-to-date. According to Special Assistant U.S. Attorney Ujifusa, a recent social media post by law enforcement in Portland, Oregon counted that 1800 men viewed one advertisement for an underage girl on one Web site in just a 24-hour period. *See* Ujifusa Interview.

While the federal prosecution of johns is not yet mainstream, it is not unprecedented and is a powerful tool for U.S. Attorneys' offices to make an impact on demand. For example, in the District of Oregon, a john is pending trial on charges of sex trafficking of a child under 18 U.S.C. §§ 1591(a)(1), (b)(2), (c), and production of child pornography under 18 U.S.C. §§ 2251(a), (e), as well as a criminal forfeiture allegation. *United States v. Ben Allen Riggs*, 3:13-cv-00294-JO (D. Or. filed June 26, 2013). While this case is pending trial, the Eighth circuit has upheld a similar case in which johns were convicted of attempted sex trafficking of a minor under 18 U.S.C. §§ 1591 and 1594(a). *See United States v. Jungers*, 702 F.3d 1066, 1075–76 (8th Cir. 2013). Continuing the federal prosecution of johns provides for a way to impact the demand on children and vulnerable women.

III. Conclusion

Traditional gang related enterprises are expanding from drug and weapons trafficking to sex trafficking, which involves lower risk and higher profit for gangs. With vulnerable juveniles being the frequent targets of predatory recruitment practices, investigations and prosecutions of criminal gang members requires a deliberate and victim-focused approach by law enforcement officers, prosecutors, and the community at large. The resources and examples provided in this article are just a few of the ways that such a deliberate approach may begin. ❖

ABOUT THE AUTHOR

❑ **Adrian L. Brown** is an Assistant U.S. Attorney in the District of Oregon, joining the office in 2007. She is currently serving a one-year detail as the National Civil Rights Coordinator for the Office of Legal and Victim Programs in the Executive Office for U.S. Attorneys. Prior to joining the Department, she served for seven years in the U.S. Air Force JAG Corps. ✠

Gangs and White Collar Crime

Stephen Kubiatowski
White Collar Crime and Health Care Fraud Coordinator
Office of Legal and Victim Programs
Executive Office for United States Attorneys

Drugs and guns have always been the bread and butter of violent street gangs. But, with increasing frequency, headlines report that gangs are expanding their operations into a variety of white collar crimes. This expansion should come as no surprise. Not only is white collar crime profitable, as it provides the funds for a gang's more traditional endeavors, but it is far less dangerous than dealing drugs or trafficking firearms. And even if you're caught, there's no exposure to the stiff mandatory minimums that are typically associated with federal narcotics and firearms offenses.

Real estate purchases have always been a means for laundering illicit funds, but with the arrival of the housing boom in the mid-2000s, gangs recognized the ease and profitability of mortgage fraud. According to the FBI's 2011 National Gang Threat Assessment, gangs such as the Bloods and Gangster Disciples began committing sophisticated mortgage fraud schemes by purchasing properties with the intent to receive seller assistance loans and, ultimately, retain the proceeds from the loans or comingle illicit funds through mortgage payments. NAT'L GANG INTELLIGENCE CTR., FED. BUREAU OF INVESTIGATION, 2011 NATIONAL GANG THREAT ASSESSMENT—EMERGING TRENDS 45 (2011), *available at* http://www.fbi.gov/stats-services/pu blications/2011-national-gang-threat-assessment/2011-national-gang-threat-assessment-emerging-trends. Most notably, in March 2009, federal prosecutors in San Diego indicted 24 people in a massive mortgage fraud scheme that was led in part by Darnell Bell, a documented member of the Lincoln Park gang. *See* Indictment, *United States v. Darnell Bell*, 09-CR-1209 (S.D. Ca. 2009). The scheme, which ran from 2005 through 2008, involved more than 100 properties in San Diego. The properties were worth a total of $100 million and netted participants $11 million in profit. *See* Greg Moran, *Leader of huge SD mortgage fraud scam pleads guilty*, THE SAN DIEGO UNION-TRIBUNE (Mar. 5, 2010), *available at* http://www.utsandiego.com/news/2010/Mar/05/leader-of-fraud-ring-pleads-guilty/. Bell used his status as a long-standing member of the gang to recruit other members for the scheme, organizing a large network of fake buyers and sellers to defraud mortgage lenders. He was sentenced in early 2013 to 70 months' imprisonment.

Gangs have likewise targeted vulnerabilities in the banking and credit card industry, as illustrated by the ongoing Armenian Power Gang prosecution brought by the Central District of California. In July 2011, more than 70 individuals were charged in a 140-count indictment for criminal activities associated with the gang. In addition to charges for racketeering conspiracy, drug-trafficking, and unlawful possession of firearms, gang members were charged with sophisticated fraud schemes, including bank fraud, aggravated identity theft, credit card skimming, manufacturing counterfeit checks, and money laundering. *See* Press Release, Dep't of Justice, Office of Public Affairs, Eight Defendants Plead Guilty in Los Angeles in Armenian Power Gang Case (Sept. 11, 2013), *available at* http://www.justice.gov/opa/pr/2013/September/13-crm-1014.html. Notably, according to the indictment, the bank fraud and identity theft scheme victimized hundreds of customers of 99 Cents Only Stores throughout Southern California, causing more than $2 million in losses. The indictment further alleged that defendants secretly installed skimming devices at store cash registers to steal customer debit card account information, which was then used to manufacture counterfeit debit cards and steal funds from the victims' bank accounts. Thus far, 59 defendants have pleaded guilty for their roles in the charged conspiracy, with imposed sentences ranging up to 102 years in prison. *See id.*

Similarly, in July 2012, 40 members and associates of the Burn Out Family Mafia gang of Oakland, California, were indicted for drug trafficking, identity theft, and firearms possession charges. The defendants charged with identity theft are alleged to have purchased stolen credit card account numbers on the Internet, re-encoded the stolen credit card account numbers onto the magnetic strips of credit cards and gift cards, and distributed those cards to other members of the conspiracy. As U.S. Attorney Melinda Haag of the Northern District of California noted in the press release accompanying this indictment, "These indictments demonstrate that criminal street gangs are branching out beyond traditional drug-trafficking operations to other illegal enterprises such as identity theft." Press Release, U.S. Attorney's Office, Northern District of California, Forty Individuals Charged with Drug Trafficking, Identity Theft, and Firearms Possession in Oakland (July 13, 2012), *available at* http://www.justice.gov/usao/can/news/2012/2012_07_13_forty.charged.press.html.

More recently, gang members are reported to be orchestrating stolen identity refund fraud (SIRF) schemes, which have grown at an alarming rate during the past several years. According to the Department of the Treasury, the number of cases of tax identity theft detected by authorities was approximately 1.2 million in 2012. *See Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part IV: Hearing Before the Subcomm. on Gov't Organization, Efficiency, and Financial Management of the H. Comm. on Oversight and Gov't Reform*, 112th Cong. 1–2 (2012) (statement of the Hon. J. Russell George, Treasury Inspector General for Tax Administration), *available at* http://www.treasury.gov/tigta/congress/congress_11292012.pdf. This staggering figure can be attributed to SIRF's profitability as well as its simplicity. All that is needed is a victim's name, Social Security number, and birthdate; any other information necessary for completing a tax return (that is, employer or W-2 data, addresses, dependents) can be falsified. Armed with a victim's identifying information, the identity thief simply files multiple false tax returns and directs that the refunds be transferred to a bank account he controls (usually under a fake name) or, more commonly, sends the funds to prepaid cards. SIRF thieves count on the fact that the IRS processes refunds quickly. If they file their false returns early in the tax season, it will likely be months before the victims have any idea there is a problem.

Although SIRF crime has appeared in almost every state, nowhere is the impact of stolen identity refund fraud more prominent than in Florida. U.S. Attorney Wilfredo Ferrer of the Southern District of Florida has referred to SIRF as "a tsunami of fraud," and with good reason—Miami has 46 times the per-capita rate of false tax refund claims compared to the rest of the county, and 70 times the national average in dollar terms. *See* David Adams, *FEATURE-Florida hit by "tsunami" of tax identity fraud*, REUTERS, (Feb. 17, 2013), *available at* http://www.reuters.com/article/2013/02/17/usa-tax-fraud-idUSL1N0B7IYW20130217. Traffic stops in Florida are routinely resulting in the seizure of notebooks containing names and Social Security numbers, tax forms, and prepaid debit cards from Western Union or Turbo Tax. *See* David Wolman, *Beware of Gangsters Filing Tax Returns*, BLOOMBERGBUSINESSWEEK, (Jan. 9, 2014), *available at* http://www.businessweek.com/articles/2014-01-09/tax-refund-fraud-fake-returns-net-gangsters-millions.

One such traffic stop led to the prosecution and conviction of Frantz Pierre, a known member of the West Side Gang, for leading a stolen identity tax refund scheme that resulted in the payment of approximately $1.9 million in fraudulent refund claims by the IRS. *See* Press Release, U.S. Attorney's Office, Southern District of Florida, Three South Floridians Sentenced In $2.2 Million Identity Theft Tax Refund Scheme (Feb. 2, 2013), *available at* http://www.justice.gov/usao/fls/PressReleases/140206-02.html. During a pullover of Pierre and his brother, Terry, in June 2010, police recovered a handful of prepaid debit cards, marked with the name Tax Professors. The Pierres denied ownership of the cards, and the cards were, accordingly, confiscated. Further investigation revealed that Tax Professors was a tax preparation company run by the brothers, whose business was filing false tax returns using stolen identities. When law enforcement agents showed up to execute a search warrant and announced their presence at Frantz Pierre's seven-bedroom residence in Parkland, Florida, in July 2012, they saw a laptop

computer thrown out of the second floor window, apparently aimed for the pool. It missed. Law enforcement subsequently recovered over 70 pre-paid debit cards and a thumb drive in his bedside dresser with over 2,000 people's names, dates of birth, and Social Security numbers. A year later, on October 24, 2013, following a jury trial, both brothers and another coconspirator were convicted on 12 counts, including conspiracy to submit fraudulent claims, aggravated identity theft, and access device fraud. The evidence at trial demonstrated that the business, Tax Professors, filed over 338 false tax returns. Pierre was recently sentenced to 208 months' imprisonment for his role in the offense. Terry received 121 months' imprisonment.

To be sure, the above evidence of gang activity expanding into white collar crimes is anecdotal. But such evidence, which was almost unheard of 15 years ago, is more commonplace. So the next time ledgers are seized from a stash house, don't assume they'll only contain customer names and balances. They may also contain the personal information necessary for identity theft. ❖

ABOUT THE AUTHOR

❑ **Stephen Kubiatowski** is an Assistant U.S. Attorney from the Northern District of Illinois and is currently on detail as White Collar Crime Coordinator at the Executive Office for U.S. Attorneys. ✠

La Vida Loca Nationwide: Prosecuting Sureño Gangs Beyond Los Angeles

Seth Adam Meinero
National Violent-Crime Coordinator
Executive Office for United States Attorneys

Graffiti ominously reading "18th STREET" and "MS-13," "XVIII" and "XIII," "EL BARRIO" and "LA MARA." Spanglish slogans, devilish tattoos, and deft hand signs. Baby-faced teens ritually "jumped in" as they pledge allegiance to their gangs for the rest of their often truncated lives.

Once the hallmarks of Los Angeles gang culture, these signs of Sureño gang activity are now common across the United States. Over the past decade, two Sureño gangs—18th Street and MS-13—have left their marks in cities and suburbs and in all corners of the country. Still, these gangs and their culture remain unfamiliar to many communities outside southern California.

This article provides a brief history of Sureños, their culture, and their migration across the nation. It also surveys prosecutions of 18th Street and MS-13 outside Southern California and describes some recurring challenges in the unrelenting national effort to bring Sureños to justice.

I. Sureño origins, culture, and migration

Sureños, the Spanish word for "southerners," is an umbrella term for predominantly Latino gangs and their members that emerged in the 1960s–1980s in southern California.

The Sureños' birthplace is Los Angeles, where groups of Chicanos and immigrants of Mexican, Central-American, and other Latino descent struggled for identity and protection against whites and other

ethnic groups. As Sureños found themselves increasingly incarcerated, they allied with the Mexican Mafia—also known as *La eMe* (Spanish for the letter "M")—one of the most powerful prison gangs in southern California. Behind bars, Sureños are generally allied under *La eMe*'s leadership and protect themselves against prison gangs of other ethnicities. But on the street, Sureños can be vicious rivals of one another.

Scores of Sureño gangs exist in southern California. Some, like the gangs SUR-13, Clanton-14, and Florencia-13, have established cliques in other states. But 18th Street and MS-13 have become the largest and most powerful Sureño gangs in the nation.

A. 18th Street origins

The 18th Street gang—also known as *Dieciocho* ("18") or *Barrio Dieciocho* (the "Neighborhood [belongs to] 18")—emerged in the late 1960s and early 1970s. The gang's name derives from its original gathering place at the intersection of 18th and Arapahoe Streets in Los Angeles's Pico-Union neighborhood. Its original members—primarily American-born Latinos or immigrants from Central America or Mexico—were excluded from other established gangs because of their ethnic origin or because they were foreign-born. Surrounded by fierce rival gangs, 18th Street developed a reputation for tenaciously protecting its small turf through extreme violence. To increase its strength, the gang precipitously recruited members without regard to their ethnicity or immigration status, and recruited middle schoolers and even younger children. This policy was auspicious and farsighted. Within three decades, 18th Street became the largest street gang in Los Angeles County. ANDREW EWAYS AND GABRIEL MORALES, B.E.S.T.: BARRIO EIGHTEENTH STREET, MARA SALVATRUCHA, AND OTHER SUREÑO GANGS ACROSS AMERICA 11–14 (2012); *Gangland (Season Two): Murder by Numbers* (History Channel production 2008).

B. MS-13 origins

MS-13 is 18th Street's chief rival. Originally known as the *Mara Salvatrucha Stoners*, the once-social, nonviolent gang later shortened its name to *Mara Salvatrucha* when it became more focused on committing violent crime. Founded by immigrants who fled the Salvadoran civil war that erupted in 1979–80, the gang's name stems from the Salvadoran dialect for "gang" (*mara*) and a neologism for "Salvadoran" and "struggler" (*salvatrucha*). TOM DIAZ, NO BOUNDARIES: TRANSNATIONAL LATINO GANGS AND LAW ENFORCEMENT 23 (2009). An alternative interpretation is that *salvatrucha* means "guerilla fighter." *See Gangland (Season One): You Rat, You Die* (History Channel production 2007).

In the decade after the civil war began, tens of thousands of Salvadorans were killed, and many immigrated to Los Angeles. Like 18th Street's founders, the Salvadoran immigrants who formed *Mara Salvatrucha* eventually allied with *La eMe*. *Mara Salvatrucha* became better known by its nickname, an abbreviation of its original name (MS), coupled with an homage to *La eMe* (the number 13, representative of the letter M, the 13th letter of the alphabet). MS-13 eventually garnered a reputation for ferocious violence reminiscent of the civil war. One of its infamous slogans became, and still is, "*Mata, Controlla, Viola*" ("Kill, Control, Rape"). SAMUEL LOGAN, THIS IS FOR THE MARA SALVATRUCHA: INSIDE THE MS-13, AMERICA'S MOST VIOLENT GANG 134 (2009).

C. Organization, identity, and culture

The 18th Street and MS-13 gangs share similar leadership structure, rituals, and traditions. Clique leaders may report to higher-ranked shot callers in Los Angeles or Central America, or to a regional shot-caller located nearer to their clique. Generally, *paisas* (apprentices) must "do work" (commit crimes, recruit, generate money) to further the gang's purposes, such as extorting, selling drugs, robbing, and assaulting rival gang members. The culmination of this "walking in" (apprenticeship) is the commission of a serious crime, often a stabbing, shooting, or killing of a rival. After performing sufficient work, the

paisa endures a "jump in," a ritual pummeling, kicking, and stomping by fellow gang members. For 18th Street initiates, the beating lasts about 18 seconds; for MS-13 initiates, about 13 seconds. Female *paisas* have the option of being jumped in or "sexed in": literally gang raped by several members of the clique she aspires to join. The *paisa* emerges from the initiation rite as a full member of the gang, and pledges eternal fealty to the gang and animus to its rivals. Members who renege on this pledge often find themselves "green-lighted" for execution. EWAYS & MORALES, at 2–6.

Sureños often "tag" (identify) themselves by the numbers associated with their gangs. Members of 18th Street represent themselves with the number 18, expressed in either Arabic or Roman numerals, or a combination of both (for example, 18, 666 (whose sum equals 18), XVIII, or XV3). MS-13 members similarly represent themselves through the number 13 (for example, 13, XIII, or X3). NATIONAL GANG INTELLIGENCE CENTER, 2010 TATTOO HANDBOOK: CALIFORNIA HISPANIC GANGS 65, 67–72 (2010); EWAYS & MORALES, at 2–6.

Sureños uncannily share one value: their devotion to the *La Vida Loca*—"The Crazy Life"—a whirlwind of fast-living, partying, weapon-toting, and ruthless violence. *La Vida Loca* is often symbolized by a tattoo found on gang members' hands or faces: the *tres puntos* ("three points"). Displayed as three dots in a triangular pattern, this tattoo symbolizes—and glorifies —the three ultimate destinations of the Sureño lifestyle: the hospital, prison, or grave. EWAYS & MORALES, at 3–4.

D. Migration

With their numbers, power, and strong sense of culture and identity, 18th Street and MS-13 were destined to spread well beyond their native Los Angeles turf.

As foreign-born Sureños were increasingly arrested and deported to their native countries, cliques of 18th Street and MS-13 formed in El Salvador, Guatemala, Honduras, and elsewhere. These cliques became increasingly potent, and their members immigrated to other regions of the United States. Cliques formed in several east coast states. Today, members of these cliques often take marching orders directly from leaders in Central America. While according respect to the original leadership—the "Old Homies" and "Original Gs" of Los Angeles—these cliques often bear a tenuous connection to the founding Southern California cliques. DIAZ, at 164-65; GARLAND, at 71.

By the late 1990s and early 2000s, cliques of 18th Street and MS-13 were firmly established across the United States and continued to multiply. In its 2011 National Gang Threat Assessment, the National Gang Intelligence Center (NGIC) estimated that 18th Street was present in at least 16 states, plus Washington, D.C. Based on 2013 NGIC data, MS-13 is present in at least 31 jurisdictions: it has an "established" presence in 21 states and an "emerging" presence in 6 states and FBI field offices in Charlotte, North Carolina, New York, New York, Houston, Texas, and Washington, DC, report that MS-13 has a "significant organized presence" (the highest level of gang infiltration) in those metropolitan areas. Coordinated law-enforcement task forces are targeting both 18th Street and MS-13 in every region of the country.

II. Cases across the country

By the mid-2000s, Sureños had become among the most dangerous criminal threats in places far from Los Angeles. Cases across the country provide chilling examples of Sureño violence.

A. Washington, DC, suburbs

Two breathtaking cases from the Washington, D.C. suburbs of Arlington, Virginia, and Langley Park, Maryland, received nationwide attention.

The first case involved Brenda Paz, a pretty, round-faced girl whose nickname was "Smiley." Paz became a jumped-in member of MS-13 at age 15. She ran away from her family, embraced the criminal lifestyle, and began a habit of dating MS-13 clique leaders. After making her way to Arlington, Virginia, she was arrested for car theft. She made a fateful decision to break away from her destructive, contemptible way of life, and began cooperating with the local police. LOGAN, at 63, 73–75, 101–05.

Paz provided a treasure trove of intelligence about MS-13. Authorities realized she was a valuable informant. They made a risky decision to place this emancipated 17-year-old in federal witness protection in Kansas and Minnesota, far from her gang friends, the only family she had. Isolated and lonely, and recently pregnant, she began recontacting her Arlington MS-13 friends, and returned to Virginia. By then, Arlington clique leaders had figured out that Paz cooperated with the police. They green-lighted her for being a rat. *Id.* at 193, 205, 218; DIAZ, at 181.

On the night of July 12, 2003, Paz partied with her MS-13 friends. The next morning, her gang friends, Oscar Grande and Ismael Cisneros, lured her to the Shenandoah River Valley on the pretext of a fishing trip. As they walked to the rippling river, Grande and Cisneros strangled her with a rope and stabbed her 16 times. They dumped Paz's body—her head nearly severed, her unborn child still in her belly—in the cruelly ironic, placid setting. Grande and Cisneros and two others were federally tried in the Eastern District of Virginia for murdering Paz. On May 17, 2005, a jury found Grande and Cisneros guilty, and acquitted the others. Grande and Cisneros were sentenced to life in prison. LOGAN, at 230–33, 240–41.

The second case involved another teenaged victim. On the cold night of January 18, 2009, members of an 18th Street clique decided to hunt for a rival in Langley Park, Maryland, considered to be MS-13 turf. The 18th Street members drove there and encountered Dennys Guzman-Saenz, a fresh-faced 15-year-old standing at a bus stop. Guzman-Saenz had no known ties to any gang. But the 18th Street members quizzed Saenz and were convinced he was *Mierda Seca*—"Dried Shit," 18th Street's insulting term for MS-13. They kidnapped him, beat him in the car, and drove back to their home turf in Gaithersburg, Maryland. Dan Morse, *Final chapter in gang killing*, WASH. POST, at B3 (Aug. 6, 2012). After they arrived in Gaithersburg, Guzman-Saenz pleaded with the 18th Street members, telling them he was not an MS-13 member. The 18th Street members showed no mercy, brutally stabbing him over 60 times. Some of the wounds cut clear through the torso on his thin frame. His head nearly severed, the 18th Street members dumped Guzman-Saenz face-down in an icy creek—a final show of disrespect. *Id.*; Dan Morse, *Montgomery gang member pleads guilty in teen's slaying*, WASH. POST, at B1 (July 20, 2010); EWAYS & MORALES, at 5.

Eventually, 11 18th Street members were arrested and pleaded guilty in state court for their roles in Guzman-Saenz's murder. This single case yielded eight first-degree murder convictions, one of the largest murder cases in Maryland history. Dan Morse, *Final chapter in gang killing*, WASH. POST, at B3 July 20, 2010).

B. Long Island, NY

Communities in the New York City suburbs of Long Island, New York, began recognizing the threat of Sureños around 1999, when a college student was murdered by MS-13 near Hempstead, New York. SARAH GARLAND, GANGS IN GARDEN CITY: HOW IMMIGRATION, SEGREGATION, AND YOUTH VIOLENCE ARE CHANGING AMERICA'S SUBURBS 88 (2009).

Assistant U.S. Attorney (AUSA) John J. Durham (EDNY) has prosecuted hundreds of Sureño defendants operating on Long Island. Durham reports an interesting development: some MS-13 cliques in the area have become so well-established that members of those cliques have remigrated to Central America and established arms of the Long Island cliques there, including a "Hempstead" clique in El Salvador. He estimates that approximately 85 percent of the Sureños he has prosecuted are MS-13

members. The remaining gang members are with 18th Street and its allies, such as the gang Salvadorans with Pride. Telephone interview with John J. Durham (Feb. 14, 2014) (Durham Interview).

Three of Durham's most notorious cases involve MS-13 members Adalberto Ariel Guzman, Juan Garcia, and Heriberto Martinez. On February 5, 2010, Guzman and Garcia carried out the execution-style murders of Vanessa Argueta, 19, and her two-year-old son in Central Islip, New York. They were responsible for shooting Argueta once in the head and chest, and Guzman himself shot the infant in the head. They left the victims' bodies in a wooded area, and with Martinez's assistance, later fled to El Salvador.

Guzman was arrested in Miami, Florida, in May 2010, when he attempted to reenter the United States. Following a three-week federal trial, Guzman was found guilty on all counts, including the murders of Argueta and her son. He faces a sentence of life imprisonment. Sentencing is currently scheduled for June 5, 2014.

Martinez, an accessory-after-the-fact to the murders of Argueta and her son, was found guilty after a six-week federal trial of his role in those and other murders. On December 9, 2013, he was sentenced to life in prison.

Garcia had remained a fugitive during Guzman's and Martinez's trials. On March 26, 2014, the Federal Bureau of Investigation added Garcia to the "Ten Most Wanted" list. The following day, he voluntarily surrendered to the FBI in Nicaragua and agreed to return to the United States. He was returned on March 28, arraigned on March 31, and is pending trial. Email interview with John J. Durham (Apr. 14, 2014).

C. North Carolina

North Carolina has also become fertile ground for MS-13. In one prominent case spanning the state's Western and Middle Districts, gang leader Alejandro Enrique Ramirez Umaña illegally entered the United States and traveled to Charlotte, North Carolina, to assist in reorganizing an MS-13 clique there. On December 8, 2007, Umaña confronted two brothers in a family-run restaurant in Greensboro, North Carolina. When the brothers saw Umaña flash gang signs, they offended him by calling the signs "fake." Umaña killed both brothers, shooting one in the chest and the other in the head. Umaña fired three more shots in the restaurant, injuring another person with his gunfire. Umaña later fled to Charlotte with assistance from other MS-13 members. Authorities arrested him five days later. While incarcerated pending trial, Umaña coordinated attempts to execute witnesses and individuals cooperating with law enforcement. U.S. Marshals also discovered that Umaña had attempted to bring a knife to court proceedings.

A jury found Umaña guilty of the gang-related killings. On July 27, 2010, U.S. District Judge Robert J. Conrad, Jr., formally sentenced Umaña to death. Department of Justice (DOJ) officials announced that Umaña was the first MS-13 member to receive a federal death sentence.

Gretchen C.F. Shappert was the U.S. Attorney for the Western District of North Carolina during the investigation of Umaña's case. When she was the District's antigang AUSA in 2003, MS-13 graffiti was surfacing in Charlotte's public places. By the time of the Umaña prosecution, MS-13 had become well-established in the city. Shappert remembers Umaña as "a vicious, predatory gangster with a long history of spontaneous and indiscriminate violence and complete disregard for human life." Email interview with Gretchen C.F. Shappert (Mar. 6, 2014).

Umaña's case was part of a larger investigation that led to the federal prosecution of at least 25 MS-13 members. Besides Umaña, 6 defendants were convicted at trial in January 2010, and 18 other codefendants pleaded guilty to the racketeering charges related to MS-13 activities in North Carolina. Shappert credits the hard work of AUSAs Jill Rose and Kevin Zolot and Criminal Division trial attorney Sam Navarro for the successful prosecution. *Id.*

D. Other cases

Several other cases from the following areas show the breadth and depth of Sureño criminal activity across the United States:

Seattle, Washington: On October 4, 2004, MS-13 member Carlos Sorto shot and killed a victim, despite his pleas for mercy. Two weeks later, Immigration and Customs Enforcement (ICE) agents were conducting a document-fraud investigation and encountered Sorto, who had not been apprehended for the murder. When the ICE agents identified themselves to Sorto, he ran, pulled a gun, and fired at one of the agents. Sorto was caught and arrested. After receiving a 33-year state sentence for the prior murder, Sorto was sentenced on January 25, 2008, to an additional 166 months for shooting at a federal agent and for discharging a firearm during a crime of violence.

Hyattsville, Maryland: On May 5, 2007, 18th Street member Omar Villegas-Martinez, along with fellow gang members, struggled with Jose Carcamo in a car, shot Carcamo twice in the head, killing him. Villegas-Martinez eventually pleaded guilty. In November 2011, he was sentenced to 23 years in prison for RICO conspiracy, including his role in the murder.

Providence, Rhode Island: On December 5, 2013, federal authorities announced the results of "Operation Gas," a more than two-year investigation into heroin trafficking and firearms offenses by MS-13 and its associates. The operation resulted in the imprisonment of 24 individuals, including two local MS-13 leaders, Francisco Bonilla and Richard Ibanez, who respectively received sentences of 10 and 8 years in prison. In addition, the operation resulted in 12 other individuals facing deportation, and effectively dismantled MS-13 in Providence.

Washington, D.C.: On May 15, 2012, 18th Street member Victor Pineda and several associates surrounded a 16-year-old victim inside a carry-out restaurant. Pineda alleged the victim was talking negatively about 18th Street and accused him of being an MS-13 member. "You're either with us or against us," Pineda said, "and if you're against us, I'll call the guys from Los Angeles to come get you." Pineda pleaded guilty to a local felony of threatening to injure the victim. On November 7, 2012, a DC Superior Court judge sentenced him to six months' imprisonment.

Gwinnett and DeKalb Counties, Georgia: From October 2006 through October 2007, MS-13 members Ernesto Escobar, Miguel Alvarado-Linares, and Dimas Alfaro-Granados committed a series of shootings and murders of suspected adversaries. In October 2006, Alavarado-Linares and Alfaro-Granados killed a fellow MS-13 member they suspected of cooperating with police. In December 2006, when a fellow MS-13 member wanted to quit the gang, Alavarado-Linares and Alfaro-Granados ordered him to kill a rival gang member before they would allow him to quit. On Christmas Eve, the quitting member shot at a car he believed to contain rivals, hitting the driver and killing a passenger. In August 2007, Escobar got into a fracas with two teenagers at a gas station. He reported the incident to a clique leader, who gave Escobar a handgun to retaliate. Escobar returned to the gas station and shot and killed one of the teenagers, who was only 16 years old. Following a jury trial, all three MS-13 defendants were sentenced on December 19, 2013, to life in prison.

III. Challenging issues

As prosecutors build cases to dismantle these gangs in the neighborhoods they menace, they face recurring issues. Experts are often needed to educate uninitiated juries about Sureños' culture, their organizational structure, and the nature of their crimes. Authorities must take steps to assure the safety of cooperators and their families living in Central America. Sureños are often shockingly young, and

prosecutors must consider transferring juvenile Sureños for federal prosecution. Prosecutors must also convince juries to find these youthful, seemingly callow defendants guilty of their callous crimes.

A. Piercing the veil of Sureño culture for unfamiliar juries

Sureño culture is rife with symbols, Spanish and English slogans and mottos, rituals, traditions, and hierarchy. This evidence may help establish elements of a criminal enterprise, identity, intent, motive, or other key issues.

Former AUSA James M. Trusty, chief of the Criminal Division's Organized Crime and Gang Section (OCGS) in the Department of Justice, notes that cooperating gang members can provide "inside" lay-witness testimony about a gang's culture and structure. But because cooperators are often saddled with credibility issues and their own criminal liability, a favored method of presenting this evidence is through expert testimony from a law-enforcement expert, pursuant to Federal Rule of Evidence 702. *See* FED. R. EVID. 702 (describing when expert testimony can be used at trial).

Finding a law-enforcement expert may be a daunting task for prosecutors in regions where Sureños have only recently made inroads. Trusty encourages prosecutors to contact OCGS, which maintains numerous resources, such as GangLink, and a comprehensive database of available experts on scores of gangs, including Sureños.

One such expert is Sgt. Claudio Saa of the Herndon, Virginia, Police Department. As a police officer for over 12 years, and a gang investigator for the last 10, Saa has been involved in over 100 Sureño investigations. Most of Saa's cases have involved MS-13, which has been the dominant Sureño gang in the Northern Virginia suburbs of Washington, D.C. He also has extensive knowledge of 18th Street. He has been qualified as an expert on MS-13 approximately 12 times, and on 18th Street approximately 9 times, in state and federal courts in Maryland and Virginia.

"It's eye-opening," Saa says, "for the juries to hear about the levels of violence these gangs are committing in their backyard." While area jurors have heard about the emergence of MS-13, they know less about 18th Street. But for both gangs, "juries still think of gangs as being a product of the West Coast. Hearing that they're committing these crimes in this area hits close to home. It's a learning process for them." Telephone interview with Claudio Saa (Mar. 5, 2014).

Another expert, Sgt. H. George Norris, has spent 13 years as a gang investigator in the mid-Atlantic region. He is also the vice president of the International Latino Gang Investigators Association. Norris has participated in hundreds of investigations of Sureño gangs, the majority of which have involved MS-13, and to a lesser extent 18th Street and other Sureños. He has been qualified approximately 26 times as an expert on MS-13 operations, culture, history, and on other gang-related areas, in state and federal courts in Maryland, Virginia, and Washington, DC.

Like Saa, Norris has found that local public awareness of Sureños in the greater DC area has built with increased media attention over the past 10 years. Norris says that area jurors and other members of the public are "most interested by the fact that Sureño gangs actually exist in their area—many people do not believe or even know that these types of gangs exist in their area until they are involved as jurors in a case." Email interview with Henry G. Norris (Feb. 24, 2014).

Saa and Norris find that jurors are most interested in Sureño history, leadership structure, operations, the crimes Sureños commit, and how and why they commit them. Both agree that the symbology of Sureño culture—tattoos, graffiti, and hand signs—rivets jurors, and that jurors find it educational to look at photos or the actual tattoos on a person. "They love when these symbols are explained or deciphered for them," Norris says. *Id.*

Experts like Saa and Norris ensure that by the end of their trial testimony, they have demystified the clandestine criminal world of Sureños so that jurors clearly understand concepts such as doing work

and green-lighting, symbols such as the *tres puntos*, and the organized structure of the gang, from *paisas*, to clique leaders, to the Big Homies.

B. Protecting Sureño cooperators and their families in Central America

The international reach of Sureño gangs poses a host of difficulties for protecting Sureño cooperators and their families. Witnesses and family members in Central America may face lethal reprisals from local clique members once it becomes known—or even suspected—that they or their loved ones are cooperating with law-enforcement authorities in the United States.

S-visas: One way for prosecutors to better assure the safety of these witnesses and their families is to apply to admit them to the United States through the S-visa program, pursuant to 8 U.S.C. § 1101(a)(15)(S).

As the United States Attorneys' Manual (USAM) indicates, the S-visa classification

> "is available to a limited number of aliens who supply critical reliable information necessary to the successful investigation and/or prosecution of a criminal organization" or who supply critical, reliable information concerning a terrorist organization. The S-visa statute permits not only alien cooperators selected for the program, but also eligible family members "to be admitted to the United States in a temporary nonimmigrant status for up to three years, *see* 8 U.S.C. § 1184(k)[(2)], and authorizes the Secretary of the Department of Homeland Security [DHS] to waive most grounds of inadmissiblilty." USAM § 9-72.100. Applications to admit individuals under the S-Visa classification must be certified by the Assistant Attorney General for the Criminal Division and approved by DHS. *Id.* An alien's admission by S-visa is conditioned on the alien not committing any felony after obtaining the visa. 8 U.S.C. § 1184(k)(3)(B).

DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-72.100 (2014).

The S-visa program has limitations. By statute, only 200 alien witnesses or informants, per fiscal year, may be admitted into the United States by S-visa. *See* 8 U.S.C. § 1184(k)(1) (2014). That quota applies nationwide. *Id.* Spouses, parents, and children of these aliens are also eligible for admission into the United States in an S-nonimmigrant derivative status. *See id.* § 1101(a)(15)(S). Fortunately, the number of derivative admitted persons does not count against the numerical limit for witnesses or informants. *See* DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL § 1862 (2014).

As for the application process, a sponsoring law enforcement agency, such as a U.S. Attorney's office, must complete, in addition to supporting documentation, a Form I-854 and a worksheet prepared by the Criminal Division's Office of Enforcement Operations. Adult aliens must execute a certification that they have knowingly waived a number of immigration rights, including the right to a deportation hearing and, in many circumstances, to contest any deportation action instituted before they obtain lawful permanent resident status (a green card). In cases of federal prosecution, the Form I-854 must be signed by a high-level official in the headquarters of the sponsoring law-enforcement agency, and in all cases in which a U.S. Attorney's office is involved, by the U.S. Attorney. *Id*.

There is one tremendous benefit for an alien who complies with all terms of the S-visa requirements: the sponsoring law-enforcement agency may make an application, before the three-year expiration of the S-visa, for the alien to be permitted to apply for a green card. 8 U.S.C. § 1255(i) (2014). If the successful alien obtains the green card, agency supervision of the alien ceases. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL § 1865 (2014).

Parole: Another potential option for having endangered witnesses and their families brought to the United States is to have them paroled. Under DHS's regulations, implementing the Immigration and

Nationality Act, 8 U.S.C. § 1182–1198, parole—that is, permitted physical entry into the United States—may be granted for aliens "only on a case-by-case basis for 'significant humanitarian reasons' or 'significant public benefit,' " provided the aliens are neither a security nor flight risk. 8 C.F.R. § 212.5(b) (2014). An example of a "significant public benefit" is paroling aliens who "will be witnesses in proceedings being, or to be, conducted by judicial, administrative, or legislative bodies in the United States." *Id.* § 212.5(b)(4). Unlike the set quota of 200 S-visas, the number of paroles granted is not limited by statute. DHS may also consider paroling a cooperator's family members under the "significant public benefit" justification. *See id.* § 212.5(b)(5).

"This a matter of life and death," says AUSA Kim Dammers (NDGA) of the process for protecting foreign-national cooperators and their families in Central America. Telephone interview with Kim Dammers (Feb. 28, 2014). Dammers has prosecuted scores of Sureños in and around Atlanta, Georgia, for the past 10 years, including the case against MS-13 leaders Escobar, Alvarado-Linares, and Alfaro-Granados, summarized above.

In the case against Escobar and his cohorts, Dammers had a critical cooperating witness who was in the United States illegally and whose life was threatened. In addition, the lives of the cooperator's mother and three adolescent brothers living in El Salvador were in peril. The Justice Department's attaché in El Salvador confirmed that the threats against the family members were credible.

Dammers coordinated efforts with DHS law enforcement and immigration officials to parole the cooperator and his family. After the necessary approvals, the cooperator and his family were all paroled and allowed to remain physically present in the United States for the parole term. He testified successfully, Dammers and co-counsel Paul Jones received an outstanding result at trial, and the cooperator's family is resting considerably more assured within the United States.

Dammers notes that parole "is a short-term solution in the patchwork of available immigration-law tools." *Id.* Unlike the S-visa process, the parole process does not include a path to a green card. Unless DHS renews the term of the parole, the parolees must report for a removal hearing and may again face the danger of gang retaliation in their own country.

C. Prosecuting juvenile and youthful Sureños

Sureño defendants tend to be young—sometimes disturbingly so, considering the appalling, mature nature of their crimes. Murders and other violent crimes in aid of racketeering are frequently committed by 18- and 19-year-olds, and even juveniles. More frequently, federal prosecutors are moving to transfer juveniles to be federally tried for committing felony crimes of violence.

Juvenile transfer: The process for transferring a juvenile for federal prosecution is set forth in 18 U.S.C. § 5032, and incorporated in USAM § 9-8.130. Generally, juveniles—that is, individuals who before age 18 committed an eligible offense, such as a violent crime in aid of racketeering or other felony crime of violence—may be transferred under three conditions:

(1) upon the juvenile's written request, with advice of counsel, to be tried as an adult

(2) upon the Government's motion for a "discretionary transfer," if the juvenile has allegedly committed after his or her 15th birthday what would constitute a federal felony crime of violence (or other eligible offense), and if the district court finds after a hearing that such transfer would be "in the interest of justice," or

(3) upon the Government's motion for a "mandatory transfer," if the juvenile was previously adjudicated guilty after his or her 16th birthday for certain felony crimes of violence, certain weapons offenses, particular drug crimes, or a particularly dangerous crime.

See 18 U.S.C. § 5032 (2014); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-8.130 (2014).

In the case of a discretionary transfer, the district court considers the following factors to determine whether the transfer would be in the interest of justice: (1) the juvenile's age and social background, (2) the nature of the juvenile's alleged offense, (3) the extent and nature of the juvenile's prior delinquency record, (4) the juvenile's present intellectual development and psychological maturity, (5) the nature of past treatment efforts and the juvenile's response to those efforts, and (6) the availability of programs designed to treat the juvenile's behavioral problems. 18 U.S.C. § 5032 (2014). The federal courts of appeal have held that the district court is allowed broad discretion in weighing these factors, and need not weigh these factors equally. *See United States v. Sealed Appellant 1*, 591 F.3d 812, 820 (5th Cir. 2009); *United States v. Anthony Y.*, 172 F.3d 1249, 1252 (10th Cir. 1999); *United States v. Wellington*, 102 F.3d 499, 506 (11th Cir. 1996). Further, a district court does not abuse its discretion in placing primary emphasis on the gravity of the juvenile's offense. *See United States v. Smith*, 178 F.3d 22, 27 (1st Cir. 1999). Indeed, one circuit has recognized that in considering the § 5032 factors, "the nature of the crime clearly predominates." *United States v. Juvenile Male*, 554 F.3d 456, 460 (4th Cir. 2009) (quoting *United States v. Robinson*, 404 F.3d 850, 858 (4th Cir. 2005)) (case involving transfer of juvenile MS-13 member).

Although moving to transfer is an arduous administrative process requiring approval from the U.S. Attorney and consultation with the Criminal Division, satisfying the requirements of § 5032 is often not difficult, given the juvenile's background and history. By the time many juvenile Sureños face federal charges, they have already committed what would constitute felony crimes of violence under federal law. It is then a matter for prosecutors to decide whether moving for a mandatory transfer is appropriate, given the circumstances of the case.

As to discretionary transfers, AUSA Durham explains that he and his investigating agents engage in serious discussion before proceeding to federally try a juvenile Sureño. Once they and supervisory AUSAs decide that there is a strong federal interest to do so, they engage in ongoing consideration and substantiation of the § 5032 factors by drafting the charging document (which may charge a grave felony offense), a prosecution memorandum, and a juvenile certification (approved by the U.S. Attorney). By the end of this process, after obtaining all the necessary internal approvals, Durham maintains "we have articulated many reasons why a juvenile transfer is warranted in the 'interest of justice,' and have already made a compelling case for our motion to transfer." Durham Interview.

"That is not to say moving for a discretionary transfer is an easy process," says Laura Gwinn, a trial attorney with OCGS. Email interview with Laura Gwinn (Mar. 6, 2014). A veteran gang prosecutor specializing in MS-13, her investigations have taken her from the streets of Washington, DC to the jungle roads of El Salvador. Her recent prosecution of MS-13's Sailors clique in Washington involved the discretionary transfer of Yester Ayala, who had committed two murders when he was 17. Gwinn notes that the defense put up a vigorous fight through a flurry of pleadings and a drawn-out transfer hearing. Nevertheless, her motion to transfer was granted, and at trial, the jury found Ayala guilty of the murders. He faces life imprisonment at his sentencing.

Youthful, capable, and culpable: Whether juvenile or adult, Sureño defendants can be quite youthful-looking and diminutive, even childlike in appearance. This can present another challenge: convincing a jury that a seeming cherub could have committed—or even carefully planned—heinous crimes.

Gwinn recognizes this issue. Juries can be initially incredulous during her opening statement when she points her finger at a small, youthful Sureño defendant and describes his sophisticated, serious crimes. But "by the end of the trial—after the jury has heard *violence, violence, violence, violence*—it is convinced that he *was* capable of and *is* guilty of the crimes he's charged with." Interview with Laura

Gwinn, in D.C. (Feb. 11, 2014). Often, these crimes are among the most awful acts a human being can commit. The jury comes to understand that "it's not the size of the dog in the fight; it's the size of the fight in the dog."

When it comes to Sureños, the size of that fight can be immense.

IV. Conclusion

Sureños have spread far beyond the Los Angeles ganglands. They are deeply woven into the criminal subcultures of the DC suburbs, Long Island, Charlotte, and several communities across the country. Indeed, the "crazy life" is the vital norm in diverse regions. Prosecutors and law enforcement nationwide are meeting challenges to combat Sureños, but the struggle to vanquish these violent gangs will be enduring, expensive, and extensive. ❖

ABOUT THE AUTHOR

❑ **Seth Adam Meinero** is the National Violent-Crime Coordinator at the Executive Office for U.S. Attorneys. From 2007 to 2012, he was an AUSA for the District of Columbia. Mr. Meinero was also a civil rights attorney at the Environmental Protection Agency for eight years before becoming a prosecutor. He has lectured about the presence of Sureños in Washington, DC, and has previously contributed to the U.S. Attorneys' Bulletin. ✠

The author wishes to thank Diedre D. Butler, Kim Dammers, John J. Durham, Laura Gwinn, Robert Nieves, H. George Norris, Claudio Saa, Gretchen C.F. Shappert, and James M. Trusty for their generous assistance and input on this article. Unless otherwise cited, summaries of cases were culled from United States Attorneys' offices press releases. NGIC data were supplied directly from the agency.

DOJ International Resources: Advice and Assistance on Criminal Gang Issues and Capacity Building

Kevin L. Sundwall
Border and Immigration Legal Issues Coordinator
Indian, Violent and Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

I. Introduction

When prosecuting gangs and organized crime, the work of the Department of Justice (the Department) does not stop at the U.S. borders. Indeed, transnational gangs have become a major focus of the Department's gang interdiction efforts in recent years. Because of the international scope of so many criminal gangs, it is imperative that federal prosecutors familiarize themselves with the offices within the Department that focus on international concerns.

The Criminal Division of the Department's Office of International Affairs; the Office of Overseas Prosecutorial Development, Assistance and Training; and the Office of International Criminal Investigative Training Assistance Program are the main conduits for international case advice, investigative assistance, and capacity building. Additionally, the Department supports International Law Enforcement Academies (ILEAs), which enhance law enforcement agencies in other countries.

II. The Office of International Affairs (OIA)

When a gang or organized crime investigation involves international issues, prosecutors should consider consulting with OIA within the Criminal Division of the Department. For example, if the case involves locating financial records in foreign countries, interviewing a witness in another country, or extraditing a defendant back to the United States from a foreign country, the prosecutor will need to consult with OIA.

OIA provides advice and assistance on international criminal matters to federal prosecutors in the various Department Divisions and U.S. Attorneys' offices, and also to state and local prosecutors. It coordinates the extradition of international fugitives from foreign countries to the United States. The Office also provides advice and assistance on all international evidence gathering, adhering to Mutual Legal Assistance Treaties and other existing law enforcement agreements. *See* OFFICE OF INTERNATIONAL AFFAIRS, *available at* http://www.justice.gov/criminal/about/oia.html.

OIA ensures that the United States meets its reciprocal obligations to honor foreign requests by responding to requests for production of evidence located in the United States and by handling requests for extradition from the United States back to foreign countries. *Id.*

III. The Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT)

A. The mission

In April 2011, the U.S. Attorney General reiterated the Department's Priorities and Mission by explaining his four essential priorities: (1) to protect Americans from terrorism at home and abroad, (2) to fight violent crime, (3) to combat financial fraud, and (4) to protect the most vulnerable members of our society. *See* Dep't of Justice, *Attorney General Eric Holder Speaks About the Department of Justice's Priorities and Mission*, BRIEFING ROOM, JUSTICE NEWS (Apr. 25, 2011), *available at* http://www.justice.gov/iso/opa/ag/speeches/2011/ag-speech-110425.html. The work of OPDAT supports these four priorities by assuring that the United States has effective partners abroad.

Training foreign prosecutors and other law enforcement officials is particularly critical in combating international crime, including gang activity and the dismantling of the drug cartels. The Department has provided, and continues to provide, opportunities for Department personnel to cultivate relationships with foreign prosecutors and other law enforcement officials that support both parties in the pursuit of cross border criminal gang investigations and prosecutions.

The OPDAT mission is to "develop and administer technical assistance designed to enhance the capabilities of foreign justice sector institutions and their law enforcement personnel, so they can effectively partner with the Department of Justice in combating terrorism, trafficking in persons, organized crime, corruption, and financial crimes." OFFICE OF OVERSEAS PROSECUTORIAL DEVELOPMENT, ASSISTANCE AND TRAINING, OUR MISSION, *available at* http://www.justice.gov/criminal/opdat/about/mission.html.

OPDAT was established in 1991. It is uniquely situated to draw on Department resources and expertise in its overseas capacity-building efforts.

> OPDAT supports the United States and the Department's law enforcement objectives and priorities by preparing foreign counterparts to cooperate more fully and effectively with the United States in combating terrorism, trafficking in persons, organized crime, corruption, financial crimes, and other transnational crime. It does so by encouraging legislative and justice sector reform in countries with inadequate laws; by improving the skills of foreign prosecutors, investigators and judges; and by promoting the rule of law and regard for human rights.

Id. A few examples of this success include OPDAT programs that have helped draft and implement accusatory system criminal procedure codes in various countries, as well as supporting new legislation or amendments to existing anti-money laundering and terrorism financing legislation in the host countries. Strengthening the criminal justice system in foreign countries is critical to the destruction and dismantlement of transnational criminal gangs.

OPDAT places experienced federal or state prosecutors as advisors in foreign countries. Typically, an attorney advisor, designated a Resident Legal Advisor (RLA), works from and is assigned to the United States embassy in the foreign country. The Department's OPDAT Web site states that in fiscal year 2012, the Office had 48 RLAs in 32 countries. *See id.* "RLAs are experienced federal or state prosecutors stationed in a host country for at least one year where they provide full-time advice and technical assistance in establishing fair and professional justice sector institutions and practices." *Id.*

OPDAT also conducts discrete short and mid-term assistance programs, ranging from one week to six months. These programs focus on a specific aspect of criminal justice and are implemented by Intermittent Legal Advisors (ILAs), who like the RLAs, are experienced federal or state prosecutors. In fiscal year 2012, the Office conducted 588 assistance programs involving 92 countries, and it managed over $72.9 million in Department of State, U.S. Agency for International Development (USAID), and Department of Defense funding. *Id.*

B. DOJ/OPDAT programs in the Americas

Some of the most serious transnational gang activity is currently located to the south of America's borders. At the same time, many countries in Central and South America are undergoing transitions from inquisitorial judicial systems to accusatory systems. In the countries where OPDAT obtains funding from the Department of State, USAID, or the Department of Defense, OPDAT is able to provide technical assistance to prosecutors, investigators, and judges. In the Americas, OPDAT currently has an RLA or ILA presence in the Caribbean, Colombia, El Salvador, Honduras, Mexico, and Panama.

> Assistance often includes reform of criminal codes and criminal procedure codes. OPDAT also provides technical assistance in specialized areas, including terrorism, gangs and organized crime, witness protection, cybercrime, human trafficking, intellectual property rights, corruption, money laundering and asset forfeiture. In conducting these programs, OPDAT draws upon the expertise of the appropriate Criminal Division components (most notably the Office of International Affairs and the Asset Forfeiture & Money Laundering Section), federal law enforcement agencies (including FBI, DEA, and DHS), and the US. Attorney's Offices (in 94 districts around the country).

OFFICE OF OVERSEAS PROSECUTORIAL DEVELOPMENT, ASSISTANCE AND TRAINING, LATIN AMERICA AND THE CARIBBEAN, *available at* http://www.justice.gov/criminal/opdat/worldact-programs/latin-caribbean.html.

The government of Mexico has amended their constitution to allow for a transition from the written inquisitorial system to an accusatory system by 2016. The Merida Initiative in Mexico is one of OPDAT's fastest growing programs. Since 2009, OPDAT has been providing technical assistance to Mexican prosecutors and law enforcement officers in the investigation of complex crimes (including

gang-related violence and money-laundering). In Mexico, OPDAT has assisted "in criminal procedure code reform efforts, drafting of witness protection legislation, extradition and mutual legal assistance, human trafficking, intellectual property rights violations, and more. OPDAT conducts Trial Advocacy courses for Mexican prosecutors unfamiliar with the adversarial system in preparation for a transition to an adversarial system." *Id.*

OPDAT's longest running program in the Americas is in Colombia. Since 2000, OPDAT has been implementing in Colombia the Justice Sector Reform Program through the U.S. Embassy in Bogota. "It has assisted Colombian lawmakers, judges, prosecutors and police authorities in implementing a Colombian Criminal Procedure Code that mandated that country's transition from a written, inquisitorial criminal justice system, marked by delays and inefficiency, to an oral, accusatorial one." *Id.* Since 2008, OPDAT has continued to mentor Colombian counterparts in implementing the Criminal Procedure Code and providing training in specialized areas, such as human rights, witness protection, and victim/witness assistance. "The OPDAT RLAs in Colombia have also helped strengthen the Colombian judiciary and enhanced the courts' working relationships with other criminal justice sector institutions." *Id.*

Currently, OPDAT also lends technical assistance in the Americas in "Guatemala, Honduras, Costa Rica, the Caribbean and other countries" by providing capacity building efforts "relating to gang activity and other law enforcement or criminal justice system areas." *Id.* In the Americas in prior years, OPDAT has had RLAs stationed in Bolivia, Brazil, Haiti, Nicaragua, and Paraguay.

IV. International Criminal Investigative Training Assistance Program (ICITAP)

ICITAP is the Department's International Criminal Investigative Training Assistance Program. ICITAP was created in 1986 and "works in close partnership with and receives funding for its programs from the Department of State, the U.S. Agency for International Development, and the Department of Defense." INTERNATIONAL CRIMINAL INVESTIGATIVE TRAINING ASSISTANCE PROGRAM, *available at* http://www.justice.gov/criminal/icitap/.

Where OPDAT's focus is on prosecutors and the judiciary, ICITAP is the Department's international development organization that works with foreign governments "to develop strong law enforcement and corrections institutions through technical assistance and training." ICITAP FREQUENTLY ASKED QUESTIONS (FAQS), *available at* http://www.justice.gov/criminal/icitap/about/faq.html. It incorporates principles of human rights and transparency into all of its programs. Program areas include "organizational development, transnational crime, criminal investigations, public integrity and anticorruption, specialized and tactical skills, forensics, basic police skills, academy and instructor development, community policing, corrections, marine and border security, information systems, and criminal justice coordination." *Id.*

The work of ICITAP also supports the Attorney General's essential enforcement priorities by working with the United States' partners abroad. ICITAP, which is part of the Department's Criminal Division, "uses its technical assistance and training expertise to reinforce the DOJ's national security and law enforcement objectives. The equation is straightforward: by helping to strengthen the rule of law and law enforcement capacity in foreign countries, ICITAP helps strengthen the security of the United States." *Id.*

ICITAP often partners with other DOJ organizations in designing and executing international law enforcement development programs. These partners include the FBI, the Drug Enforcement Administration, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms and Explosives. ICITAP also frequently joins forces with OPDAT. ICITAP and OPDAT work together to help host countries build integrity, professionalism, and accountability in the three pillars of criminal justice: police, courts, and corrections. ICITAP currently has personnel in 34 countries, including Colombia, El Salvador, and Mexico, and has funding for capacity building in the Dominican Republic.

V. International Law Enforcement Academies (ILEAs)

A. Overview

ILEAs are international police academies administered by the Department of State. In these academies, U.S. law enforcement personnel instruct local police and prosecutors from participating countries in many law enforcement issues, including gangs and organized crime, counterterrorism, narcotics interdiction, detection of fraudulent documents, and border control practices. The ILEAs were established in 1995 by President Clinton as a means of bringing together international law enforcement authorities to reduce crime, combat terrorism, and share intelligence information and training.

Currently there are five ILEAs throughout the world: ILEA Budapest, Hungary; ILEA Bangkok, Thailand; ILEA Gaborone, Botswana; ILEA Roswell, New Mexico; and ILEA San Salvador, El Salvador. Additionally, there is an ILEA Regional Training Center in Lima, Peru, supervised by ILEA San Salvador. *See* ILEA SAN SALVADOR: HISTORY, *available at* http://www.ileass.org.sv/page.php?id=2.

The official ILEA Web site explains that "ILEA is the result of a philosophy that brings together the efforts of government agencies, institutions, instructors, and students to attain a common international law enforcement policy." *Id.*

> Since the beginning of 1997, the U.S. Government sought to establish the International Law Enforcement Academy in a host country of Latin America. Its establishment in San Salvador became a reality when the Salvadoran legislature ratified the bilateral agreement signed on September 20, 2005.
>
> ILEA San Salvador was created as a joint entity of El Salvador and the United States of America, after the signing of the "Agreement between the Government of El Salvador and the Government of the United States of America, on the Establishment of the International Law Enforcement Academy," ratified through Legislative Decree No. 880, of November 30, 2005, posted in the Official Gazette No. 239, Volume 369, of December 22, 2005.

Id.

Over the years, ILEA has trained scores of law enforcement officials who can put into practice the techniques learned and also help build capacity in their respective countries by sharing with others the information provided during the training courses.

B. ILEA's Advanced Anti-gang Course

The ILEA San Salvador routinely holds an Advanced Anti-gang Course. The course is designed to provide training on "techniques, and best practices to combat the illegal activities of gangs through prevention, investigation, prosecution, and incarceration." ILEA SAN SALVADOR: COURSE CONTENT SUMMARY, *available at* http://www.ileass.org.sv/page.php?id=21. The participants are taught forensic investigation techniques, interviewing techniques, and the management of gang members in the prison system. U.S. prosecutors and investigators explain how forensic evidence can be utilized to evaluate the truthfulness of statements to build a more persuasive criminal case, anticipate the defense, and challenge the testimony of the defendant. The participants engage in practical exercises and a field visit. The course also emphasizes the need for prosecutors, investigators, and forensic technicians to work together in all stages of the investigation and prosecution of the gang-related cases. *See id.* The DOJ supports this course by providing federal prosecutors and FBI agents to serve as instructors.

VI. Additional DOJ international resources

The DOJ has additional international resources beyond those already mentioned in this article. Within the Criminal Division, the Narcotics and Dangerous Drugs Section (NDDS) has attorney advisors stationed internationally. In the Americas, NDDS has advisors in both Mexico and Colombia. Finally, the DOJ law enforcement agencies, including the FBI, the Drug Enforcement Agency, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms and Explosives, all have an international presence. ❖

ABOUT THE AUTHOR

❑ **Kevin L. Sundwall** is the Border and Immigration Legal Issues Coordinator at the Executive Office for U.S. Attorneys (EOUSA). Mr. Sundwall served as the OPDAT Senior Resident Legal Advisor in Mexico from 2009 to 2013. Prior to his assignment in Mexico, he served as the OPDAT Resident Legal Advisor in Paraguay from 2007 to 2009, working regionally in Argentina, Bolivia, and Paraguay. Since 2002, Mr. Sundwall has been an Assistant U.S. Attorney for the District of Utah, and he is currently on detail assignment to EOUSA. ✠

Expert Codebreakers in Court

Jeanne Anderson
Cryptanalyst
Cryptanalysis and Racketeering Records Unit
Federal Bureau of Investigation

I. Introduction

While many people are familiar with famous codes and ciphers such as those written by the Zodiac Killer or the Unabomber, or even literary ciphers like those seen in Sir Arthur Conan Doyle's Sherlock Holmes stories and Edgar Allen Poe's works, few people realize how frequently codes and ciphers are actually used by everyday criminals. Gang members, terrorists, drug dealers, and organized crime members often use codes and ciphers to facilitate their criminal activities. Codes allow criminals to cloak the meaning of their records or messages, or even hide the message itself to avoid detection. If obtained and decoded, however, the information contained in criminal communications and records is valuable in both the investigative and prosecutorial phases of a case. Decoded messages can serve as evidence, and the cryptanalysts that break them can provide compelling expert witness testimony in court.

Coded records and messages are so prevalent and valuable that the Federal Bureau of Investigation (FBI) has devoted an entire unit to analyzing them: the Cryptanalysis and Racketeering Records Unit (CRRU). The official mission of the CRRU is to examine manually encrypted documents and records of illegal enterprises, as well as to provide expert testimony and other forensic assistance to further identify terrorism, foreign intelligence, and criminal activities in support of federal, state, local, and international law enforcement investigations and prosecutions.

The CRRU can analyze various types of cryptic writings, such as enciphered phrases tattooed on a prisoner or on an unidentified body, bags of records found in search warrants, or notebooks full of encoded material discovered in the possession of a lone wolf criminal. This cryptic material could in turn

be hiding past or planned criminal acts, the scope of a drug dealer's operations, or the form and extent of a gang or racketeer's criminal enterprise.

This article provides three case studies in which CRRU cryptanalysts broke criminal codes and provided expert testimony. In each of these cases, the CRRU's results were integral to the outcome of the case and sentencing. Also provided is contact information so that law enforcement agencies and attorneys can consult with CRRU on evidence submissions and expert testimony.

II. Case study I

In 2007, the CRRU received a letter that was intercepted between two inmates in the California Department of Corrections and Rehabilitation. The inmates were using a family member on the outside as a "three-way," a facilitator who would resend letters to other inmates from their address to bypass the regulations prohibiting inmate-to-inmate communications. The letter was being mailed to the founder of a white supremacist gang called the United Society of Aryan Skinheads (USAS). The letter was authored by another skinhead thought to be a USAS associate.

At first glance, the communication appeared harmless, but prison staff noticed a seemingly nonsensical jumble of letters intermixed in the conversation. The prison staff sent the letter to the CRRU with a request for decryption. The CRRU was able to provide a fast response to advise prison staff that this jumble of letters was actually an enciphered message that read, "Attempt murder on Donny McLachlan."

In 2009, the author of the coded letter was on trial, charged with the deliberate and premeditated attempted murder of Donald McLachlan, aggravated assault on McLachlan, and several other counts. The CRRU cryptanalyst forensic examiner walked the jury through the step-by-step process of decrypting the message. From the message, the expert witness, with no prior knowledge of Donny McLachlan, was able to provide specific details about the crime to the jurors. The testimony was integral in the defendant's conviction and sentence to life in prison without the possibility of parole.

III. Case study II

The CRRU also examines records from suspected illicit businesses. Records examinations can determine the size, scope, and nature of criminal activities documented within ledgers and notebooks. Record examinations and testimonies often influence federal Sentencing Guidelines by determining the type of drugs, as well as the roles of participants, prices, and quantities.

In 2006, the CRRU received a case from U.S. Immigration and Customs Enforcement (ICE). ICE agents had executed a search warrant at the home of a suspected drug trafficker and found no drugs. Their search would have left them empty-handed except that an agent discovered two pieces of paper behind a painting on the foyer wall. The papers contained cryptic letters and numbers. At first glance, the documents appeared to be records of small dollar purchases, but CRRU analysis revealed that these dollar amounts were actually marijuana weights. The subject had added decimal points to conceal their drug sales. For instance, a pound of marijuana that was valued at $350 was recorded on the paper as $3.50.

In 2007, a CRRU forensic examiner testified in federal court in Del Rio, Texas. This testimony revealed that the two pages contained records of the distribution of more than 1,900 pounds of marijuana to four coconspirators. The federal jury returned guilty verdicts and the defendants were convicted of smuggling more than 1,000 kilograms of marijuana, conspiracy to smuggle marijuana, and money laundering. The Government was also able to seize numerous vehicles and properties. While no drugs were seized, the huge quantities reflected in the records were able to be taken into account during sentencing. As the records were the sole source of quantities, the CRRU examiner's expert testimony was crucial to the conviction and sentencing in this case.

IV. Case study III

On Super Bowl Sunday in 2004, 11-year-old Carlie Brucia was abducted and murdered while walking home from a friend's house in Florida. Video footage from a nearby carwash helped law enforcement identify and arrest Joseph Smith for the murder. Smith eventually confessed, but he claimed that he was under the influence of cocaine and heroin, had no memory of the killing, and was terribly remorseful.

While awaiting trial, Smith sent a written message to his brother consisting only of math symbols and numbers. Law enforcement sent this letter to the CRRU, where cryptanalysts began work on these seemingly random symbols. Cryptanalysts determined that the symbols represented letters of the English alphabet, and the message began in the bottom right corner and read right to left, bottom to top. A full decryption was provided, and the decrypted message contained information about how Smith disposed of Carlie Brucia's clothes and backpack and how he dragged the body to where it was found. Smith also wrote that he wished "he had something juicy to say."

The decryption and the subsequent testimony highlighted Smith's lack of remorse, contradicting the penitent image he had attempted to paint of himself prior to his trial. Smith was convicted and sentenced to death for Carlie Brucia's murder, kidnapping, and sexual battery.

V. Tips for law enforcement and attorneys

While some cryptographic systems can be very obvious, others are more obscure and harder to recognize. Law enforcement and investigators should be mindful of recorded conversations or documents that contain what appear to be nonsensical jumbles of symbols, letters, words, numbers, or a combination thereof. Encrypted documents may appear to be shorthand writing systems and are often found with illicit businesses. They can be entire notebooks of enciphered messages or simple scribbles on a crumpled slip of paper in the pocket of a coat. If suspicious documents are found, they can be sent to the CRRU for analysis.

In addition to making sense of encrypted messages, the CRRU also provides expert witness testimony. Past CRRU testimonies have related to sports bookmaking, prostitution, drugs, loan sharking, human trafficking, murders, gang business, espionage, and numerous other crimes. Without cryptanalysis, there is no way to ascertain what encrypted documents may contain, and the contents of a decryption or an expert witness's testimony have the potential to make a huge impact on a case. Testimony support is an underused element that is freely available to law enforcement agencies and attorneys.

Attorneys and law enforcement agencies are welcome to submit encrypted documents to the CRRU. Email CODEBREAKERS@ic.fbi.gov or call (703) 632-7334 to request further submission instructions.

VI. Conclusion

Codes and ciphers are used by gangs, drug dealers, racketeers, and lone wolves alike. The CRRU provides decryption support that can bring cryptic secrets to light. The CRRU also provides expert testimony to these secrets that can also play a crucial role in conviction and sentencing. Past cases highlight the effectiveness of cryptanalysis in both the investigation and prosecution phases. While criminal use of encrypted messages and records may be a temporary hindrance to law enforcement, the CRRU's assistance can provide key pieces of evidence in the case.❖

ABOUT THE AUTHOR

❑**Jeanne Anderson** is a cryptanalyst in the Cryptanalysis and Racketeering Records Unit of the Federal Bureau of Investigation. Correspondence may be addressed to Jeanne Anderson, Federal Bureau of Investigation, CRRU, 2501 Investigation Parkway, Quantico, VA 22135. Email: Jeanne.Anderson@ic.fbi.gov. ✠

This is publication 14-04 of the Laboratory Division of the FBI. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the FBI or the U.S. Government. This work was prepared as part of their official duties. Title 17 U.S.C. § 105 provides that "copyright protection under this title is not available for any work of the United States Government." Title 17 U.S.C. § 101 defines a United States Government work as a work prepared by an employee of the United States Government as a part of that person's official duties.

Using "Digital Fingerprints" (or Hash Values) for Investigations and Cases Involving Electronic Evidence

Ovie Carroll
Director, Cybercrime Lab
Computer Crime and Intellectual Property Section
Criminal Division

Mark L. Krotoski
Assistant Chief
National Criminal Enforcement Section
Antitrust Division

Most federal cases now involve at least some electronic evidence. *Some* federal cases involve voluminous amounts of electronic evidence, including millions of records. For *any* case involving electronic evidence, hash values will be used in either the investigation, the forensic examination, or as evidence at trial.

Hash values provide a powerful and effective means to distinctly identify a particular electronic record. Illustratively, hash values can be obtained for a computer hard drive, a file or record (such as a PDF, email, image, Word document, or other comparable records), a string of text, or any other collection of data (collectively "data set"). For example, hash values can be used to review a voluminous amount of data set to determine how many copies of a particular document or image may be found. Based on the signature features of hash values, it is now common for courts, forensic experts, investigators, and practitioners to refer to a hash value as a "digital fingerprint" or "digital DNA." *See infra* Section III(A)(2) (collecting cases). Over the past several years, courts have considered and accepted the use and reliability of hash values as electronic evidence.

Consider a couple of examples:

- **Gang prosecutions:** In a gang or organized crime investigation, a leader may use texting to communicate commands with confederates. If any of the smart phones or devices used for texting are seized, a forensic examination will likely recover many of the text messages. Recovered smart phone images may also identify other confederates and contain pictures taken at past crime scene locations.

  Hash values may be used in imaging the seized devices as part of the forensic examination process and in locating key messages, images, and other records. At an organized crime trial, a forensic examiner authenticates the images and text messages based on the hash values and confirms how the same crime scene images were sent to several confederates shortly after specific crimes were committed. A timeline connects the date and time of key text messages and images with the offenses and helps the jury understand the unfolding events.

- **Trade secret misappropriations:** In a trade secret case, a former employee downloads critical files from the company network just before leaving to take another position with a competitor. The employee was a long-time, trusted supervisor, and no one anticipated any misappropriation until after his departure. As part of the theft, the employee used a thumb drive to transfer the company files and records. After transferring the files, the employee changed the names of the files as part of an effort to conceal them. Company network logs and an examination of his work computer provide the date and time of the download, transfer, and misappropriation of data.

  Hash values are used in the forensic examination of the media and to help identify the specific files that were downloaded and transferred. At the trade secret theft trial, the forensic examiner provides the dates and times that key trade secret files were downloaded from the company network to the defendant's work computer and transferred to the thumb drive. The examiner notes that the files were later transferred to another device and then emailed outside the country. The files were also deleted, but recovered from the thumb drive. Finally, the examiner testifies that matching hash values confirmed and located the misappropriated trade secret files, even though the names of the files were changed. The examiner explains to the jury that the hash value matched the content and that the change in the name of the file did not affect the hash value determination.

- **Company obstruction of justice:** After search warrants were executed at multiple company offices, some employees begin destroying records at a satellite office that was not the subject of the search warrants. As part of the destruction effort, one employee with some tech savvy slightly alters the content of some of the electronic records before deleting them. He anticipates that hash values may be used to find the original content and believes investigators will not find the altered content. After investigators learn about the destruction, network data and computers are seized.

  At an obstruction of justice trial, a forensic examiner testifies how hash values were used to locate a number of deleted records and assisted in recovering the deleted records that were not yet overwritten. Some of the deleted files were restored from backups. The examiner notes that by using "fuzzy hashing" (or context-triggered piecewise hashing), she was able to locate files with slightly altered content, as she was able to identify those files containing a high percentage of similarities.

In each of these examples, the collection and review of data requires the use of hash values. Hash values will be used, among other purposes, to authenticate electronic evidence, ensure the integrity of a forensic exam, provide investigative leads, efficiently review a voluminous amount of data to determine whether a particular document or email is on a seized computer or how many copies exist on seized media, and reduce the amount of data to be reviewed by eliminating unnecessary records or duplicates.

See generally infra Section IV (summarizing some common uses of hash values in investigations and cases).

Given the importance of hash values to electronic evidence, this article brings a forensics and courtroom perspective to using hash values effectively in investigations and at trial. It provides a comprehensive review of hash values and links to primary reference materials as a resource and aid to prosecutors and other practitioners seeking to address issues that may arise concerning the use of hash values involving electronic evidence in investigations and cases.

As an overview, the article surveys recent cases and legal issues that have been raised concerning the application and use of hash values. Section I(A) of this article compares hash values to alphanumeric serial numbers used to identify vehicles, firearms, currency, computers, and other devices. Hash values, however, are based on a mathematical algorithm and are much stronger and more reliable than these physical serial numbers. Common definitions of hash values are reviewed in Section I(B). In Section II, the two primary hash values used in the electronic evidence review process are highlighted—specifically, MD5 Message Digest Algorithm (MD5) and SHA-1 Secure Hash Algorithm (SHA-1). Examples using the Preamble to the U.S. Constitution are provided for these two common hash values.

Section III reviews cases and literature recognizing hash values as a "digital fingerprint" or "digital DNA." However, hash values are even more distinctive than common fingerprints or DNA because the likelihood of a random match for hash values is significantly less likely than for either fingerprints or DNA. Section IV highlights some common uses of hash values in investigations and cases. Section V considers the remote improbability of a random match for electronic evidence using hash values, explaining that it is actually one-in-340 undecillion for MD5 hash values and one-in-1.4 quindecillion for SHA-1 hash values. Section V(E) reviews the issue of a theoretical "collision" (the likelihood that two data sets will have the same hash value) and explains why the possibility (more likely the improbability) of a theoretical "collision" does not impact the use of hash values in computer forensics. In fact, in recent decisions, courts have considered and rejected the "collision" argument. The use of hash values in various legal contexts (for probable cause for a search warrant, to authenticate evidence, and at trial) is noted. The objective of this article is to provide practitioners with a better understanding of the vital role of hash values in the forensic process so that this tool can be effectively used in investigations, in cases, and at trial.

I. Overview: What are hash values?

A hash value is a unique result representing a specific data set (for example, a particular file, record, or hard drive). The result, which is generated by an algorithm, is a distinct alphanumeric string, using a combination of letters and numbers. The following is an example:

26a981554d7d761230bc7ef3a6645375

(This MD5 hash value is further discussed as an example in Section II(D)). The algorithm result is sometimes referred to as hash values, hash sums, checksums, or message digest. In this article, hash values refer to the hash function calculation for a data set, such as a file, record, or hard drive.

Hash values have a variety of uses and purposes and originally were important for cryptography (concerning secure or coded communications). *See generally* CRYPTOLOGY TIMELINE, *available at* http://www.math. cornell.edu/~morris/135/timeline.html. Today, they are used for network and information security, military communications, and digital certificates for secure Web sites, among other areas.

Hash values also provide a fundamental role in forensic examinations concerning the review and analysis of data. Years ago, "Brian Deering of the National Drug Intelligence Center introduced the paradigm of using cryptographic hashes, such as the MD5 Message Digest Algorithm ("MD5"), to uniquely identify files to the forensics community." WARREN HARRISON, THE DIGITAL DETECTIVE: AN

INTRODUCTION TO DIGITAL FORENSIC, ADVANCES IN COMPUTERS: INFORMATION SECURITY 101 (2004) (describing use of the Hashkeeper dataset) (footnote omitted). While hash values have been modified and enhanced over the years, and certainly will continue to be updated in the coming years, they provide a powerful tool in forensic examinations, investigations, and cases to authenticate, locate, and reduce the review of data. This article focuses on the use of hash values for forensic review of electronic evidence. It does not consider the use of hash values for cryptography or other security functions.

A. Contrasting other unique serial numbers used to identify particular evidence

There is an ongoing need to have an effective and efficient process to identify a specific record or item of evidence and to determine whether it is dissimilar from other evidence. Over the years, a variety of systems have been developed to identify or authenticate a particular piece of evidence or object. One common approach is based on the assignment of a unique alphanumeric string to a particular object. Hash values electronically follow this process, but are more reliable and distinctive. The following are some traditional examples.

Vehicle identification numbers: A vehicle may generally be identified by make, model, color, or other similar characteristics. However, a vehicle identification number (VIN) or license plate is used to identify a particular vehicle. *See, e.g.*, *United States v. Woods*, 321 F.3d 361, 362 (3d Cir. 2003) (in carjacking trial, admitting agent testimony that "he was able to trace the [stolen] minivan's unique vehicle identification number to a manufacturing plant located in Tarrytown, New York, using the database maintained by the National Insurance Crime Bureau"); *United States v. Shoffner*, 826 F.2d 619, 622 (7th Cir. 1987) (in "chop shop" conspiracy, "the victims authenticated certified title histories of their vehicles, which bore the VINs of the stolen vehicles").

Since 1954, VINs have been in use. In 1981, the National Highway Traffic Safety Administration "established a fixed VIN format" of 17 characters. The VIN is divided into four parts: (1) World Manufacturer's Identification, which is three numbers or letters, (2) Vehicle Description Section, which is five numbers or letters, (3) The VIN Accuracy Check Digit, which is one number, and (4) Vehicle Identification Section, which is eight numbers or letters. The following is a VIN example:

1ZVBP8CF5B5161451

This unique 17 character VIN identifies a particular 2011 Ford Mustang G, 2 door coupe with a V8, 5 OL engine, designated as a small passenger car with rear wheel drive, manufactured in Flat Rock, Michigan. *See* Ronald Montoya, *How To Quickly Decode Your VIN, What 17 Numbers Can Tell You About Your Car*, EDMONDS (Aug. 20, 2013) (providing example), *available at* http://www.edmunds.com/how-to/how-to-quickly-decode-your-vin.html; *see also* 49 C.F.R. §§ 565.1–.2 (2014) (VIN Requirements); *see generally* NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, VEHICLE IDENTIFICATION NUMBERS (VINS), *available at* http://www.nhtsa.gov/Vehicle+Safety/Vehicle-Related+Theft/Vehicle+Identification+Numbers+(VINs) (summarizing history and noting that "with model year (MY)1981, the National Highway Traffic Safety Administration required that all over-the-road-vehicles sold must contain a 17-character VIN"). A felony prosecution may result for knowingly altering or removing motor vehicle identification numbers under 18 U.S.C. § 511.

Firearm Serial Numbers: Similarly, a firearm may generally be identified by make, model, caliber, and type. However, a particular firearm is often identified by its serial number. *See, e.g.*, *United States v. Morales*, No. 95-16161996, 1996 WL 390466, at *3 (1st Cir. July 12, 1996) (unpublished) (firearm authenticated by serial number and detective testimony).

The Gun Control Act of 1968, Public Law 90-618, established a serial number requirement for firearms. *See* 18 U.S.C. § 923(i) (2014) ("Licensed importers and licensed manufacturers shall identify by means of a serial number engraved or cast on the receiver or frame of the weapon, in such manner as the

Attorney General shall by regulations prescribe, each firearm imported or manufactured by such importer or manufacturer."); *see generally* BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES, DEP'T OF JUSTICE, POLICE OFFICER'S GUIDE TO RECOVERED FIREARMS 8 (2009), *available at* https://www.atf.gov/files/publications/download/p/atf-p-3312-12.pdf; BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES, DEP'T OF JUSTICE, FIREARMS: TRACING & IDENTIFICATION (2007), *available at* http://www.atf.gov/files/publications/download/i/atf-i-3317-5.pdf. The following is a firearm serial number example:

510NN01001

This serial number identifies a particular Browning 9mm Hi-Power pistol, made in 1999, with the serial number 01001. *See* BROWNING HI-POWER PISTOL, *available at* http://www.browning.com/customerservice/categun/detail.asp?id=35. The removal or alteration of the serial number from a firearm may result in a felony prosecution under 18 U.S.C. § 922(k).

U.S. currency: Similar to a VIN and firearm serial number, since 1928 each U.S. currency note also has a unique serial number. *See* 12 U.S.C. § 413 (2014) ("Federal Reserve notes shall bear upon their faces a distinctive letter and serial number which shall be assigned by the Board of Governors of the Federal Reserve System to each Federal Reserve bank."). For example, U.S. currency produced since 1996 for $5 bills and higher notes has an eight-digit number supplemented with two capital letters before and one capital letter after the eight-digit number. The first prefix letter designates the series (A=1996, B=1999, C=2001, etc.) and the second letter designates which of the twelve Federal Reserve Banks (FRB) issued the note (A=Boston, B=New York, C=Philadelphia, etc.). The suffix letter designates the run of notes for that denomination for that FRB. Consider this hypothetical example:

BC12345678A

BC12345678B

The first note comes from the 1999 series from Philadelphia (BC12345678A), and the second note is the second run for that same denomination in 1999 (BC12345678B). A "star" or "replacement" note provides an exception to the numerically incremented serialized currency. The star note is used to replace an imperfect note, detected during production, and is also substituted for the 100 millionth note in a series. Star notes have their own special unique serial number followed by a star in place of the suffix letter.

> The Federal Reserve Bank of Atlanta has summarized the system used:
>
> The serial number appears twice on the front of the note. No two notes of the same kind, denomination, and series have the same serial number. This fact can be important in detecting counterfeit notes; many counterfeiters make large batches of a particular note with the same number. Notes are numbered in lots of 100 million. Each lot has a different suffix letter, beginning with A and following in alphabetical order through Z, omitting O because of its similarity to the numeral zero.
>
> Because serial numbers are limited to eight numerals, a "star" note is substituted for the 100 millionth note. Star notes also replace notes damaged in the printing process. Made up with independent runs of serial numbers, star notes are exactly like the notes they replace except that a star is substituted for one of the serial letters.

FEDERAL RESERVE BANK OF ATLANTA, DOLLARS AND CENTS: FUNDAMENTAL FACTS ABOUT U.S. MONEY 6 (2006), *available at* http://www.frbatlanta.org/filelegacydocs/DollarsCents.pdf; *see also* BUREAU OF ENGRAVING & PRINTING, CURRENCY NOTES 14, *available at* http://www.moneyfactory.gov/images/Currency_notes_508.pdf (describing serial number system); *see generally* Dave Undis, *How Rare are Fancy Serial Numbers?*, 274 PAPER MONEY 293, 293 (2011), *available at* http://coolserialnumbers.com/HowRareAreFancySerialNumbers.pdf. In addition to the serial number, other factors may be used to

identify counterfeit currency, such as the watermark, security thread, printing pattern, color-shifting ink, microprinting, and other established design features for each dollar. *See, e.g.*, U.S. SECRET SERVICE, KNOW YOUR MONEY, *available at* http://www.secretservice.gov/KnowYourMoneyApril08.pdf (summarizing distinctive features of currency).

Currency serial numbers may be used in criminal cases. As an example, in bank robbery cases, "bait" money (involving the use of known currency listed by serial numbers) may be provided to the robbers and later recovered as evidence. *See, e.g.*, *United States v. Brown*, 242 F. App'x 920, 921 (4th Cir. 2007) (per curiam) ("admitting testimony from a police detective that serial numbers on some of the currency found in Brown's home matched recorded serial numbers on the bank's 'bait money' list"); *United States v. Smith*, 10 F.3d 724, 726 n.1 (10th Cir. 1993) (trial stipulation noting that some of the bank robbery money included "$251 in bait money"). As the Tenth Circuit in *Smith* explained:

> Bait money is a packet of U.S. Currency which is placed in a bank teller's drawer and monitored by an alarm system. The individual bills and serial numbers in the bait money packet are also recorded and kept with one of the officers of the bank. The "bait money" purpose is to set off an alarm, inform police when money is taken from the drawer, and enable the money to be traced in the event of a theft. $50 of the bait money taken by the defendant was recovered from Mrs. Barbara Johnson who had received it from the defendant for the purchase of a car.

Smith, 10 F.3d at 726 n.1.

Other devices: The serial numbering system is a common means used to identify a variety of devices and equipment. For example, computer serial numbers may be used to authenticate the evidence or connect the defendant to the offense. *See, e.g.*, *United States v. Gavegnano*, 305 F. App'x 954, 958 (4th Cir. 2009) (computer was authenticated by "match[ing] the serial number for the computer subject to the forensic report with the computer and hard drive issued to" the defendant); *United States v. Robertson*, 493 F.3d 1322, 1331 (11th Cir. 2007) (computer serial numbers used to establish mail fraud scheme).

Seized computer equipment or devices are typically identified by serial numbers and other features. *See, e.g.*, *United States v. Espinal-Almeida*, 699 F.3d 588, 609–10 (1st Cir. 2012) (GPS device authenticated by serial number recorded on custody receipt form). In forfeiture proceedings, serial numbers are used to identify forfeited computer equipment obtained during a criminal case. *See, e.g.*, *United States v. Christensen*, No. 4:12CR3044, 2012 WL 5354745, at *5–6 (D. Neb. Oct. 29, 2012) (listing several hard drives by manufacturer, mode, and serial numbers).

In the forensics process, seized computer equipment is usually identified by serial numbers in the forensic or chain of custody report. These examples highlight the role of serial numbers as one means to identify computer equipment and property.

Compare hash values: In each of the prior examples, a unique alphanumeric string is assigned to a particular item (vehicle, firearm, U.S. currency, or device).

In a similar manner, for electronic data, hash values assign a unique alphanumeric string to a particular record, file, or other data set. This result confirms whether two electronic records are the same or different from another one.

The following is an example of an MD5 hash value for the Preamble of the Constitution:

26a981554d7d761230bc7ef3a6645375

The 32 characters of numbers and letters in this instance are assigned to one file (or data set), which in our example is the text for the first sentence in the Constitution. If this was an important email,

image, or record in a case, we may be able to find other copies by looking for the hash value. (More examples are considered below in Section II(D), along with the SHA-1 Secure Hash Algorithm (SHA-1).)

The following table compares the alphanumeric identifiers for our examples:

Type	Unique Alphanumeric Identifier	Specific Item
Vehicle Identification Number (VIN)	1ZVBP8CF5B5161451	• 2011 Ford Mustang G, 2 door coupe with a V8, 5 OL engine, designated as a small passenger car with rear wheel drive, manufactured in Flat Rock, Michigan • Alphanumeric string of 17 characters • Discussed in Section I(A)
Firearm Serial Number	510NN01001	• Browning 9mm Hi-Power pistol, made in 1999 with the serial number 01001 • Discussed in Section I(A)
U.S. Currency Note	BC12345678A	• 1999 currency note from the Federal Reserve Bank in Philadelphia • Alphanumeric string of 11 characters • Discussed in Section I(A)
MD5 Message Digest Algorithm (MD5)	26a981554d7d761230bc7ef3a6645375	• Text File of the Preamble to the U.S. Constitution (original text) • Alphanumeric string of 32 characters • Discussed in Sections I(A) and II(D)
SHA-1 Secure Hash Algorithm	f15b1ce9a37e7fb69086f25216617ae0a0e5706e	• Text File of the Preamble to the U.S. Constitution

(SHA-1)		(original text) • Alphanumeric string of 40 characters • Discussed in Section II(D)

In fact, hash values are *more* reliable than the serial number examples highlighted above for VINs, firearms, devices, or other objects that are physically applied or introduced to the object. Efforts may be made to tamper with, alter, or replace a physical serial number. Counterfeits might be used.

In contrast, the same hash value can be generated by an algorithm each time for a particular data set. If necessary, for further verification, different types of hash values (such as the MD5 or SHA-1) can be used to identify one particular data set. If a different hash value result occurs, then we know that the original data has been modified. Any attempt to alter the electronic data will be exposed by a different hash value.

B. Defining hash values

For computer forensics, one primary objective of a hash function is to verify the integrity of data. How are hash values defined? A hash function is a mathematical algorithm that produces a fixed size value or result (a hash value that is always the same length) from any size of data. The concept may generally be expressed and understood as follows:

Fixed-Size Hash Value = hash function algorithm (variable-length block of Data)

or

HV=hf(D)

There are numerous fixed-size hash values. Two common ones used in forensics are MD5 Message Digest Algorithm and SHA-1 Secure Hash Algorithm. Any change to the data set (or variable-length block of data) will change the hash value.

The National Institute of Standards and Technology (NIST) defines "Hashing" as "[t]he process of using a mathematical algorithm against data to produce a numeric value that is representative of that data." NAT'L INST. OF STANDARDS AND TECH., DEP'T OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 85 (2013) (citations omitted), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NISTIR.7298r2.pdf.

The following definitions of "hash function" and "message digest" are provided by NIST:

> Hash Function –
>
> A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
>
> 1) One-Way. It is computationally infeasible to find any input that maps to any prespecified output.
>
> 2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.
>
> ***
>
> A mathematical function that maps a string of arbitrary length (up to a predetermined maximum size) to a fixed length string.

Id. at 84.

> Message Digest –
>
> The result of applying a hash function to a message. Also known as a "hash value" or "hash output".
>
> A digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated.
>
> A cryptographic checksum, typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result.

Id. at 121–22.

II. Two common hash values used for the forensic review of electronic evidence

There are numerous types of hash values that are developed and used for different objectives. New hash values are being developed. *See infra* Section II(C). As mentioned above, for forensic examinations, two common hash values are typically used: MD5 and SHA-1.

The MD5 and SHA-1 hash values have been used for a variety of purposes over the years. For example, they have been used for cryptography and for network and information security. While these early hash values are being discontinued for cryptography or security purposes, they still serve a fundamental role in computer forensics. The forensic use involves the review of data and does not concern issues related to secure communications or security issues. In fact, many forensic tools will automatically generate both MD5 and SHA-1 hash value results as part of the forensic examination process.

A. MD5

MD5 was the fifth revision of a message digest algorithm developed by Professor Ronald Rivest of RSA Laboratories. He summarized this measure:

> The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. *It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.* The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

RONALD L. RIVEST, THE MD5 MESSAGE-DIGEST ALGORITHM (1992), *available at* http://people.csail.mit.edu/rivest/pubs/Riv92c.txt (emphasis added); *see generally* TIM BOLAND & GARY FISHER, SELECTION OF HASHING ALGORITHMS 8–10, 12 (2000), *available at* http://www.nsrl.nist.gov/Documents/hash-selection.pdf (summarizing hashing algorithms CRC32, MD4, MD5, and SHA-1). The MD5 creates an alphanumeric result consisting of 32 characters. (An example is provided in Section II(D) *infra*).

B. SHA–1

The SHA-1standards are published by NIST. SHA-1, published in 1995, was the first algorithm developed by the National Security Agency. It was based on the design principle of MD4. It applies the Merkle-Damgard paradigm to a dedicated compression function. It can produce a hash value of any input size smaller than 264 (or 2 billion gigabytes or 1.86264514 Exabyte's). *See generally* WILLIAM E. BURR, U.S. NAT'L INST. OF STANDARDS &TECH., CRYPTOGRAPHIC HASH STANDARDS: WHERE DO WE GO FROM HERE? 88 (2006), *available at* http://csee.wvu.edu/~katerina/Teaching/CS-465-Fall-2007/HashStandards.pdf ("The US National Security Agency (NSA) followed the Merkle-Damgaard principles in designing the SHA-1 hash function, which NIST adopted as a federal standard in 1995, and the SHA-2 functions (SHA-224, SHA-256, SHA-384, and SHA-512), adopted in 2002."); TIM BOLAND & GARY FISHER, SELECTION OF HASHING ALGORITHMS 10 (2000), *available at* http://www.nsrl.nist.gov/Documents/hash-selection.pdf ("NIST, along with the National Security Agency (NSA), designed the Secure Hash Algorithm Revision 1 (SHA-1) for use with the Digital Signature Standard (DSS) (REF12); this standard is the Secure Hash Standard; SHA-1 is the algorithm used in the standard.").

Generally, the SHA-1 works well for most forensic applications and can be used for historical, stored, or transferred records. *See generally* INFO. TECH. LAB., U.S. NAT'L INST. OF STANDARDS & TECH., SECURE HASH STANDARD (SHS) 3 (Mar. 2012), *available at* http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf; NIST: SECURE HASHING, *available at* http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html; NIST: POLICY ON HASH FUNCTIONS, *available at* http://csrc.nist.gov/groups/ST/hash/policy.html. In contrast to the shorter MD-5 hash value, the SHA-1 creates an alphanumeric result consisting of 40 characters. (An example is provided in Section II(D)).

C. New, emerging hash values

Given the important role for hash values and their wide application, new hash values have been and will continue to be developed over time. In 2001, the SHA-2 standard was published. *See, e.g.*, U.S. NAT'L INST. OF STANDARDS & TECH., SECURE HASH STANDARD, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 180–82 (2002) (archived copy), *available at* http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf; *see generally* BART VAN ROMPAY, ANALYSIS AND DESIGN OF CRYPTOGRAPHIC HASH FUNCTIONS, MAC ALGORITHMS AND BLOCK CIPHERS 44 (2004), *available at* https://www.cosic.esat.kuleuven.be/publications/thesis-16.pdf (summarizing the development of hash values).

In 2012, NIST announced the selection of a new a SHA-3 standard, which is not yet released. *See* SHU-JEN CHANG ET AL., U.S. NAT'L INST. OF STANDARDS & TECH., THIRD-ROUND REPORT OF THE SHA-3 CRYPTOGRAPHIC HASH ALGORITHM COMPETITION 1 (2012), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf; *see also* NIST: NIST SELECTS WINNER OF SECURE HASH ALGORITHM (SHA-3) COMPETITION, *available at* http://www.nist.gov/itl/csd/sha-100212.cfm; U.S. NAT'L INST. OF STANDARDS & TECH., SHA-3 SELECTION ANNOUNCEMENT, *available at* http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_selection_announcement.pdf; NIST: SHA-3 COMPETITION (2007-2012), *available at* http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

These newer standards are primarily designed and used for cryptography and information security purposes. Based on the past trend, it is expected that enhanced hash values will continue to be announced

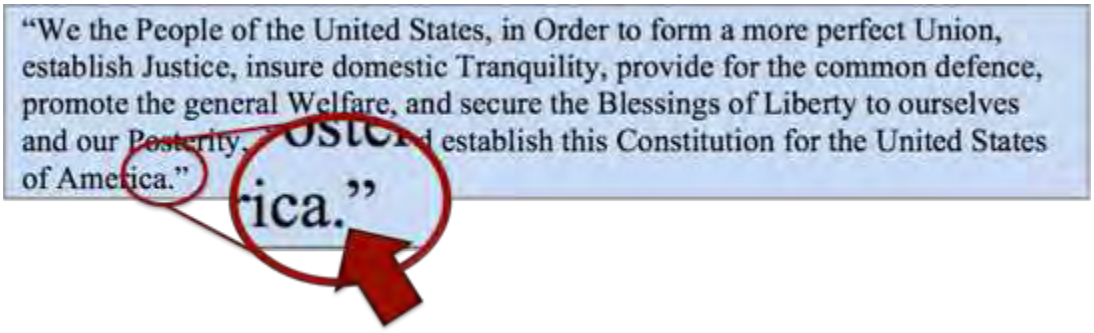
over time. As with the MD5 and SHA-1 hash values, these newer tools may have residual benefits for forensic applications.

D. MD5 and SHA-1 hash value examples

What does a hash value result look like for the commonly used MD5 and SHA-1? Consider the text for the Preamble to the U.S. Constitution (our data set). Let's assume a file named "Preamble" has the text for the Preamble. Then assume two minor alterations will be made to the text file, first by removing the period at the end of the sentence, and second by adding an extra space before the period at the end of the sentence. Observe what happens to the hash values:

Original and modified text example:

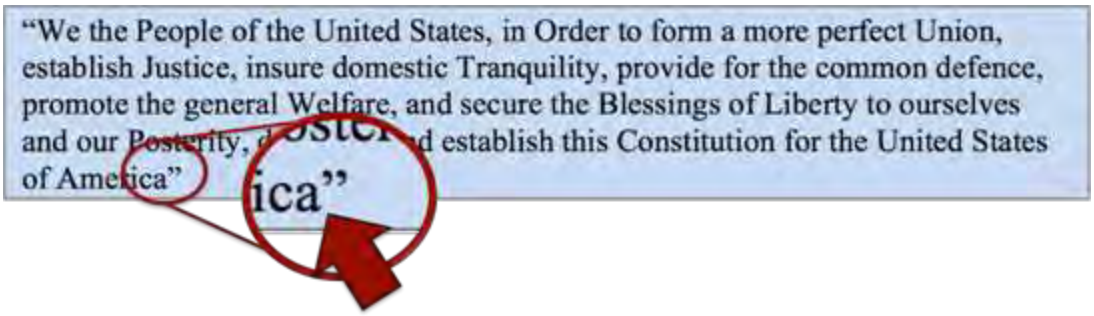
"Preamble" File (Original Preamble Text)



MD5: 26a981554d7d761230bc7ef3a6645375

SHA-1: f15b1ce9a37e7fb69086f25216617ae0a0e5706e

Now, using the same text, one slight change is made by merely removing the period at the end of the Preamble:

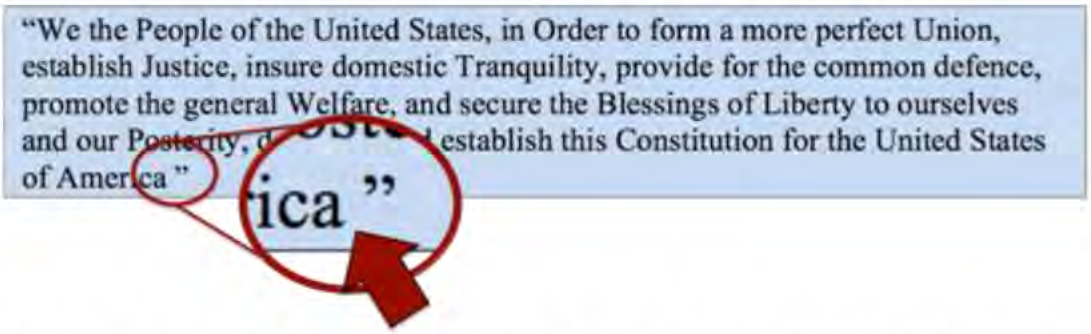


The hash value changes in the following manner:

MD5: 8ef46ff929b2b1af43f7bb326562ecc1

SHA-1: 37e8bbd169beb75c446db1ad844e82b7aea9b68f

In one final example, watch what happens to the hash value when a single "space" is added to the previous example in the place where the period was removed. This example demonstrates how any change to the content, even adding an extra space, significantly changes the hash value:



(Quotes are used above only to demonstrate to the reader where the extra space is located and were not part of the data content being hashed.)

MD5: 7d522bbe8c38a6da208acad47503419f

SHA-1: e8bf83af375a42581e30cb94d4c2773be9874c71

Here are the results summarized together:

File or Data Set	Hash Value	Result
Preamble (original text)	**MD5**	26a981554d7d761230bc7ef3a6645375
	SHA-1	f15b1ce9a37e7fb69086f25216617ae0a0e5706e
Preamble (period removed)	**MD5**	8ef46ff929b2b1af43f7bb326562ecc1
	SHA-1	37e8bbd169beb75c446db1ad844e82b7aea9b68f
Preamble (space added for removed period)	**MD5**	7d522bbe8c38a6da208acad47503419f
	SHA-1	e8bf83af375a42581e30cb94d4c2773be9874c71

As demonstrated in this illustration, the mathematical (or alphanumeric) result is unique to a particular file. Any alteration, regardless of size, will change the result. For each hash value, when a change was introduced to only one character (removing a period or adding a space), a different alphanumeric value resulted. There was no relationship between the first and later calculation (such as next number higher in sequence). The second hash value generated provides an entirely new and different result. No result was close in number to the original.

This illustration demonstrates the distinctive role of using hash values. Each hash value refers distinctly to a specific data set (here, version of the Preamble). *See generally* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 2.4 (2d ed. 1996), *available at* http://www.cse.iitk.ac.in/users/anuag/crypto.pdf ("A single bit change in the pre-image changes, on the average, half of the bits in the hash value. Given a hash value, it is computationally unfeasible to find a pre-image that hashes to that value."); NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 122 (2013), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (providing one definition of "Message Digest" as "[a] digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated.").

Now what would happen to each data set above if the name of the "Preamble" file was changed to "Preamble2"? Because the name of the file is not part of the "content" of the data being hashed, any file with the exact data content would have the same hash value, regardless of the file name. Thus, changing the file name does not impact the hash value at all.

So how do forensic examiners address the issue of locating data sets or files containing slight alterations? Other tools such as "fuzzy hashing" (or context-triggered piecewise hashing) permit the identification of data that contains a high percentage of similarities. *See infra* Section IV(D)(3).

Special features of hash values: These examples also highlight a few of the special features of hash values. First, the process can be readily replicated. A particular digital file can be measured using the hash function again and again. The fact that the same hash value results each time confirms that there is no change to the original digital file. Also, if needed, more than one hash value (such as MD5 and SHA-1) can be used to provide additional verification.

Hash values also operate "one-way." In other words, the hash value for a particular data set can be determined, but the content cannot be reassembled or determined by knowing the hash value. *See, e.g.*, BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 2.4 (2d ed. 1996), *available at* http://www.cse.iitk.ac.in/users/anuag/crypto.pdf ("A one-way hash function is a hash function that works in one direction: It is easy to compute a hash value from pre-image, but it is hard to generate a pre-image that hashes to a particular value. . . . A good one-way hash function is also collision-free: It is hard to generate two pre-images with the same hash value."); *see also* BRIAN DEERING, DATA VALIDATION USING THE MD5 HASH, *available at* http://www.woodmann.com/crackz/Tutorials/Md5info.htm ("This fingerprint is 'non-reversible', it is computationally infeasible to determine the file based on the fingerprint. This means someone cannot figure out your data based on its MD5 fingerprint.").

Consequently, it is also possible to generate a hash value without seeing or reviewing the content of the data. For example, if there is a privileged communication or contraband, a hash value may be obtained of the record that will uniquely identify it, without review of the content. *See, e.g.*, *United States v. Keith*, No. 11-10294-GAO, 2013 WL 5918524, at *8 (D. Mass. Nov. 5, 2013) ("In this regard it is worth noting that matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it.").

Finally, the risk of collision (the same hash value resulting for two different records) is immaterial or unlikely for forensic purposes. Professor Ronald Rivest described this feature as "computationally infeasible." RONALD L. RIVEST, THE MD5 MESSAGE-DIGEST ALGORITHM (1992), *available at* http://people.csail.mit.edu/rivest/pubs/Riv92c.txt ("It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest."); *see also* NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 84, 121–22 (May 2013) (defining "hash function" as "collision resistant" since it "is computationally infeasible to find any two distinct inputs that map to the same output"), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

III. Recognizing the signature characteristics of hash values

A. A "digital fingerprint" or "fingerprinting files"

For the past couple of decades, a hash value has been referred to as a "fingerprint" or "digital fingerprint." This label is used to capture the unique signature properties of a hash value. Only one data set is identified by this unique digital fingerprint. As noted below, the fingerprint attribute of hash values has been used by the developers of hash values in court proceedings and cases and by the legal community. However, as will be explained, this apt characterization actually understates the utility of hash values because the chance of a random match for a "digital fingerprint" is more unlikely than for standard fingerprints.

Early recognition of the "fingerprint" qualities of hash values: The early developers and users of hash values took note of the "fingerprint" qualities of hash values. More than 20 years ago,

Massachusetts Institute of Technology Professor Ronald Rivest originally described the MD5 algorithm as "produc[ing] as output a 128-bit '*fingerprint*' or 'message digest' of the input" which was "intended for digital signature applications." RONALD L. RIVEST, THE MD5 MESSAGE-DIGEST ALGORITHM (1992) (emphasis added), *available at* http://people.csail.mit.edu/rivest/pubs/Riv92c.txt.

Others have also referred to hashing as a "fingerprint." For example, a few years later, Bruce Schneier provided the following example:

> Think of it as a way of *fingerprinting files*. If you want to verify that someone has a particular file (that you also have), but you don't want him to send it to you, then ask him for the hash value. If he sends you the correct hash value, then it is almost certain that he has that file. This is particularly useful in financial transactions, where you don't want a withdrawal of $100 to turn into a withdrawal of $1000 somewhere in the network.

BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 2.4 (2d ed. 1996) (emphasis added), *available at* http://www.cse.iitk.ac.in/users/anuag/crypto.pdf (listing "fingerprint" as one of the names for "one-way hash function," and explaining that [t]he point . . . is to fingerprint the pre-image: to produce a value that indicates whether a candidate pre-image is likely to be the same as the real pre-image"); *see also* BRIAN DEERING, DATA VALIDATION USING THE MD5 HASH, *available at* http://www.woodmann.com/crackz/Tutorials/Md5info.htm (describing the "non-reversible" features of the MD5 "fingerprint" which "means someone cannot figure out your data based on its MD5 fingerprint").

Recent cases referring to hash values as a "digital fingerprint": Since the developers and users of hash values considered it to be a form of fingerprinting, it is not surprising that in cases and court proceedings, a hash value is commonly referred to as a "digital fingerprint." During the past few years, an increasing number of cases have referred to hash values as a "digital fingerprint." So far, this includes the following six federal courts of appeals:

- **First Circuit:** *United States v. Chiaradio*, 684 F.3d 265, 271 (1st Cir. 2012) (referring to hash values as "essentially, the digital fingerprint" used to compare files), *cert. denied*, 133 S. Ct. 589 (2012); *see also United States v. Farlow*, 681 F.3d 15, 19 (1st Cir. 2012) (describing "hash value" as "a sort of digital fingerprint" in denying motion to suppress, and rejecting defendant's claim that law enforcement should have limited the search for an image based solely on hash values), *cert. denied*, 133 S. Ct. 460 (2012).
- **Third Circuit:** *United States v. Miknevich*, 638 F.3d 178, 181 n.1 (3d Cir. 2011) (noting how a SHA-1 mathematical algorithm "can act like a fingerprint"), *cited in United States v. Beatty*, 437 F. App'x 185, 186 (3d Cir. 2011); *United States v. Sutton*, 350 F. App'x 780, 781 n.2 (3d Cir. 2009) (noting five images were identified "by matching the SHA 1 hash value, a kind of digital fingerprint"); *see also United States v. Cunningham*, 694 F.3d 372, 376 n.3 (3d Cir. 2012) ("Each hash value 'is an alphanumeric string that serves to identify an individual digital file as a kind of "digital fingerprint." ' ") (reversing trial conviction based on evidence error concerning child pornography video clips) (quoting *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011)).
- **Fourth Circuit:** *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011) (A hash value "is an alphanumeric string that serves to identify an individual digital file as a kind of digital fingerprint. Although it may be possible for two digital files to have hash values that collide, or overlap, it is unlikely that the values of two dissimilar images will do so.") (internal quotation marks omitted), *cert. denied*, 132 S. Ct. 1945 (2012); *see also United States v. Brown*, 701 F.3d 120, 122 n.2 (4th Cir. 2012) ("A hash value is a code that identifies an individual digital file as a kind of digital fingerprint.) (internal quotation marks omitted) (quoting *Wellman*, 663 F.3d at 226 n.2); *United States v. Richardson*, 607 F.3d 357, 362–63 (4th Cir. 2010) (The AOL's Image

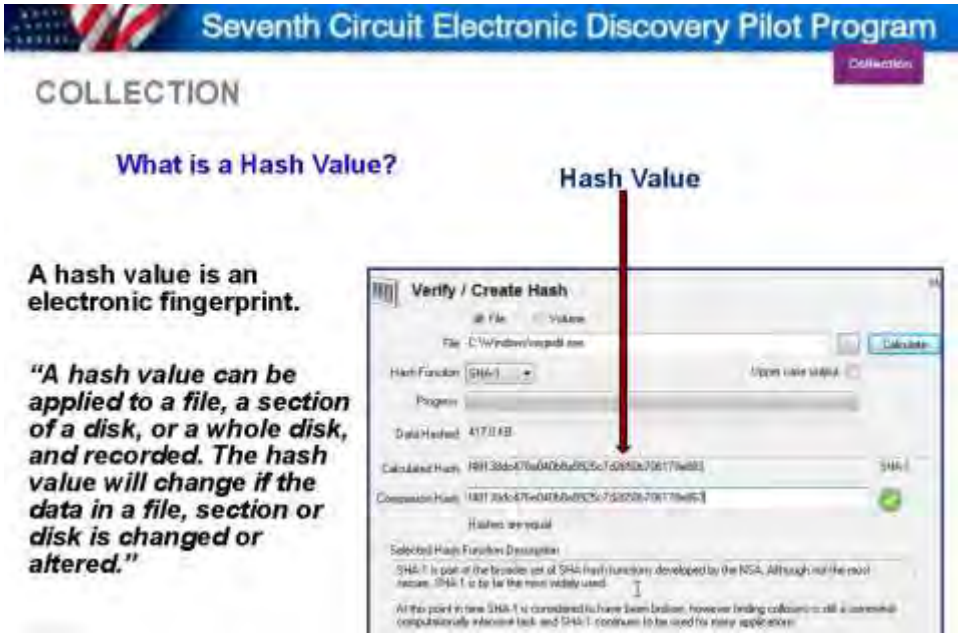
Detection and Filtering Program "recognizes and compares the digital 'fingerprint' (known as a 'hash value') of a given file attached to a subscriber's email with the digital 'fingerprint' of a file that AOL previously identified as containing an image depicting child pornography.").

- **Sixth Circuit:** *United States v. Schimley*, 467 F. App'x 482, 484 (6th Cir. 2012) (per curiam) (Trooper "used the 'SHA–1 hash value,' which is a unique signature or fingerprint for a file, to verify that the child-pornography video he had downloaded was the same file being shared by [the defendant]"); *see also United States v. Bradley*, 488 F. App'x 99, 100–01 (6th Cir. 2012) (quoting district court case summary explaining that an investigator "conducted an undercover investigation that targeted internet protocol ('IP') addresses that displayed hash values, commonly described as digital fingerprints, of known or suspected child pornography").
- **Eighth Circuit:** *United States v. Glassgow*, 682 F.3d 1107, 1110 n.2 (8th Cir. 2012) (describing the SHA-1 hash value as "a digital fingerprint of a computer file"), *cert. denied*, 133 S. Ct. 631 (2012); *United States v. Finley*, 612 F.3d 998, 1000 n.3 (8th Cir. 2010) ("The SHA is a mathematical algorithm that allows for unique identification of digital images and videos. SHA values are, in essence, unique digital fingerprints or signatures.") (citing *United States v. Klynsma*, No. CR. 08-50145-RHB, 2009 WL 3147790, at *6 (D.S.D. Sept. 29, 2009)).
- **Tenth Circuit:** *United States v. Stevahn*, 313 F. App'x 138, 139 (10th Cir. 2009) (" 'The United States has adopted the SHA-1 hash algorithm' for 'computing a condensed representation of a message or data file'; thus it can act 'like a fingerprint.' ") (quoting *United States v. Warren*, No. 4:08 CR 189 RWS, 2008 WL 3010156, at *1 n.4 (E.D. Mo. July 24, 2008)); *see also United States v. Henderson*, 595 F.3d 1198, 1199 n.2 (10th Cir. 2010) ("SHA value serves as a digital fingerprint . . . [and n]o two computer files with different content have ever had the same SHA value.").

Consistent with these appellate decisions, several district courts have also taken note of the "digital fingerprint" attribute of hash values. *See, e.g.*, *Malibu Media LLC v. Gilvin*, No. 3:13-CV-72 JVB, 2014 WL 1260110, at *1 (N.D. Ind. Mar. 26, 2014) ("Each bit of a file has a unique hash value ('bit hash') that is the bit's unique digital fingerprint. The entire digital file also has a unique hash value ('file hash')."); *United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at *9 (D. Vt. Nov. 8, 2013) ("The Gnutella Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the fingerprinting of files. Once you check a file with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file."); *United States v. Skow*, No. 1:11-CR-373-CAP, 2013 WL 5493308, at *2 (N.D. Ga. Oct. 2, 2013) (based on hearing testimony, summarizing an initial step in the forensic examination imaging process as "obtaining a digital signature, or fingerprint, of the computer and each document or file in it known as a 'hash value' "); *United States v. Dodson*, 960 F. Supp. 2d 689, 692 n.1 (W.D. Tex. 2013) ("A 'hash' value is a code that identifies an individual digital file as a kind of 'digital fingerprint.' ") (citing *United States v. Wellman*, 663 F.3d 224, 226 n.6 (4th Cir. 2011), *cert. denied*, 132 S. Ct. 1945 (2012)); *United States v. Broadhurst*, No. 3:11-cr-00121-MO-1, 2012 WL 5985615, at *1 n.1 (D. Or. Nov. 28, 2012) ("A SHA-1 value is best described as a digital fingerprint of a computer file.") (citing *United States v. Glassgow*, 682 F.3d 1107, 1110 n.2 (8th Cir. 2012), *cert. denied*, 133 S. Ct. 631 (2012)); *Patrick Collins, Inc. v. John Does 1-21*, 282 F.R.D. 161, 164 (E.D. Mich. 2012) ("The Unique Hash Identifier (also known as a hash tag, SHA1 hash, or a digital fingerprint) is a long string of letters and numbers that is used to compare a copy of a file with the original to ensure data integrity." (footnote omitted)), *report and recommendation adopted by* 286 F.R.D. 319 (E.D. Mich. 2012); *L-3 Commc'ns Westwood Corp. v. Robichaux*, No. 06-279, 2008 WL 577560, at *2 n.2 (E.D. La. Feb. 29, 2008) ("A 'hash value' is an electronic fingerprint. In order for two hash values to match, the files must be identical for every character and every line."); *United States v. Cartier*, No. 2:06-cr-73, 2007 WL 319648, at *1 (D.N.D. Jan. 30, 2007) ("Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value."); *see also United States v. Brooks*, No. 3:13-cr-58-J-34JRK, 2014

WL 292194, at *3 (M.D. Fla. Jan. 27, 2014) (noting that the search warrant affidavit described "[e]very file has a specific and unique SHA-1 value or signature that is similar to a fingerprint for the file" (internal quotation marks omitted)); *United States v. Hock Chee Koo*, 770 F. Supp. 2d 1115, 1123 (D. Or. 2011) ("The 'hash value' is a series of numbers that acts as a digital fingerprint; when the hash value changes it means the content of a file has changed."); *United States v. Collins*, 753 F. Supp. 2d 804, 806 n.3 (S.D. Iowa 2009) ("A mathematical algorithm assigns a unique SHA-1 value to computers files, including images and video content files. Special Agent Larsen testified that a SHA-1 value is akin to a digital fingerprint and that it is more than 99.9999% reliable.").

Legal community: The legal community also has accepted the role of hash values as "digital fingerprints." For example, the Seventh Circuit Electronic Discovery Pilot Program referred to the hash value as an "electronic fingerprint":



SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM, E-DISCOVERY PRACTICAL GUIDE, WHAT EVERYONE SHOULD KNOW ABOUT THE MECHANICS OF EDISCOVERY 64 (Apr. 6, 2011), *available at* http://www.discoverypilot.com/sites/default/files/MLS_7Circuit_Slides.pdf.

Some bar committees have also recognized the role of hash values as a "digital fingerprint." *See, e.g.*, E-DISCOVERY COMM., COMMERCIAL & FED. LITIG. SECTION OF THE N.Y. STATE BAR ASS'N, BEST PRACTICES IN E-DISCOVERY IN NEW YORK STATE AND FEDERAL COURTS VERSION 2.0 36 (Dec. 2012), *available at* http://www.nysba.org/Sections/Commercial_Federal_Litigation/ComFed_Display_Tabs/Reports/Edisc overy_Final5_2013_pdf.html (approved by the NYSBA Executive Committee April 5, 2013) (defining "Hash" as "[a] relatively small, unique number representing the unique digital 'fingerprint' of data, resulting from applying a mathematical algorithm to the set of data. The fingerprint may be called hash, hash sum, hash value, or hash code. Used to validate the authenticity and/or integrity of data.").

Legal articles also refer to hash values as a "digital fingerprint." *See, e.g.*, John Sammons, *Solid-State Drives Are a Game Changer for Deleted Files, Technology for the Litigator*, AM. BAR ASS'N (June 11, 2012), *available at* http://apps.americanbar.org/litigation/committees/technology/articles/summer2012-0612-solid-state-drives-deleted-files-discovery.html ("Traditionally, forensic examiners have relied on cryptographic hashing algorithms, such as MD5 or SHA1, to take the 'digital fingerprint' or 'digital DNA' of a hard drive. We can then take the 'fingerprint' of our evidentiary image at any time and compare it with the 'fingerprint' of the original. They should match exactly, verifying the integrity of the

evidence."); Sharon D. Nelson & John W. Simek, *Practical Guidance is an Antidote to Fear, Electronic Discovery in Everyday Cases*, OR. STATE BAR BULLETIN (Feb./Mar. 2009), *available at* http://www.osbar.org/publications/bulletin/09febmar/discovery.html (describing the "mathematical algorithm (normally an 'MD5 hash,' a sort of digital fingerprint)," which is used to confirm a match with "the MD5 fingerprint of the acquired computer hard drive"); *see also Hash Value Tool (Or "Digital Fingerprint") Increasingly Noted In Cases Involving Electronic Evidence*, FED. EVIDENCE REV. (Feb. 19, 2013),*available at* http://federalevidence.com/blog/2013/february/hash-value-tool-or-%E2%80%9Cdigital-fingerprint%E2%80%9D-increasingly-noted-cases-involving-elect ("[H]ash values are commonly referred to as 'digital fingerprints' or 'digital DNA' and have been described as having more than a 99 percent level of accuracy to confirm two files or records match.").

Random hash value matches are far less likely than random fingerprint matches: The "digital fingerprint" description represents an effort to capture the uniqueness of hash values, as one discrete hash value can be assigned to a particular data set. However, the likelihood of a random match for a "digital fingerprint" is more remote than a random match for traditional fingerprints. It is generally recognized that "the chances of two separate sets of data having matching MD5 hashes is far more unlikely than two individuals having matching fingerprints." *Hashing!*, VENDARI (Mar. 19, 2013), *available at* http://verndari.net/archives/tag/hash-collision. The statistical likelihood of a random match is difficult to obtain for traditional fingerprints given a variety of factors, including the role of expert opinion in making an identification and the quality of the print being considered. Nonetheless, consider these estimated ranges for the chance of a fingerprint match:

> Sir Francis Galton (1892), considered to be the father of Fingerprint Classification, estimated that there was a 1 in 64 billion chance that two fingerprints could match, and with 10 fingers each, the chance for two people to have matching fingerprints was 1 in 6.4 billion. . . .
>
> In following up on Galton's work, Osterburg (1980) estimated that the chances of two individuals having the same fingerprint was more in the range of 1 in 100,000,000,000,000,000,000 (or 100 billion, billion). . . .
>
> In this regard, the chances of two separate sets of data having matching MD5 hashes is far more unlikely than two individuals having matching fingerprints, and Fingerprint Classification has been widely used and upheld (under *Daubert*) in cases throughout the United States.

Id. (referencing FRANCIS GALTON AND FINGERPRINTS, *available at* http://galton.org/fingerprinter.html; James W. Osterburg, T. Parthasarathy, T. E. S. Raghavan & Stanley L. Sclove, *Development of a Mathematical Formula for the Calculation of Fingerprint Probabilities Based on Individual Characteristics*, 72 AMERICAN STATISTICAL ASSOCIATION 772, 777–78 (1977), *available at* http://cs.iupui.edu/~tuceryan/pdf-repository/Osterburg1977.pdf; *see also* Sharath Pankanti, Salil Prabhakar & Anil K. Jain, *On the Individuality of Fingerprints*, 24 IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 1010, 1010 (Aug. 2002), *available at* http://biometrics.cse.msu.edu/Publications/Fingerprint/PankantiPrabhakarJain_FpIndividuality_PAMI02.pdf (estimating the "probability that a fingerprint with 36 minutiae points will share 12 minutiae points with another arbitrarily chosen fingerprint with 36 minutiae points is 6.10×10^{-8}").

Additionally, fingerprint analysis entails some level of making judgments based on experience. Two examiners may use different approaches in their fingerprint analysis even if they arrive at the same conclusion. Instead, a hash value is based on a defined algorithm that can be calculated again and again on a particular dataset. The ability to make a fingerprint identification also depends on the sufficiency of the information about the fingerprint. So, while it is appropriate and useful to refer to hash values as "digital fingerprints," to be precise, hash values are actually more distinctive than fingerprints.

B. "Digital DNA" analogy

Recent cases: Recognizing the distinctive attributes of hash values, some cases have also described hash values as a form of "digital DNA." *See, e.g.*, *United States v. Crist*, 627 F. Supp. 2d 575, 578, 578 (M.D. Pa. 2008) ("An MD5 hash value is a unique alphanumeric representation of the data, a sort of 'fingerprint' or 'digital DNA.' "); *see also United States v. Wernick*, No. 03-CR-0189 (DRH), 2010 WL 415395, at *2 (E.D.N.Y. Jan. 29, 2010) (forensic copy of hard drive provided to the defense was based on "comparing the hash value of each original (equivalent to a DNA marker of the computer hard drive) to the forensic images" which provided "exact copies of the originals for evaluation"); *United States v. Wellman*, No. 1:08-cr-00043, 2009 WL 37184 (S.D. W. Va. 2009) ("[A] hash value or algorithm is '[a] digital fingerprint or a DNA of a file.' "), *aff'd*, 663 F.3d 224 (4th Cir. 2011), *cert. denied*, 132 S. Ct. 1945 (2012); *State v. Lyons*, 9 A.3d 596, 598 (N.J. Super. Ct. App. Div. 2010) ("The file was identifiable by its secure hash algorithm (SHA) value, a numerical value that acts as a data file's digital DNA.").

Hash values are far more accurate and unique than traditional DNA evidence: Hash values are described as "digital DNA" based on the distinctive attributes in identifying a particular file. However, in using this analogy, it is important to recognize that hash values (such as the MD5 or SHA-1) are more reliable and distinctive than DNA identification. *See, e.g.*, *United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at *3 (D. Vt. Nov. 8, 2013) (The SHA-1 value "is more reliable than DNA (in that the likelihood of two individuals coincidentally sharing the same DNA is greater than the likelihood that more than one file will have the same SHA-1 value) and a collision between two files with identical SHA-1 values but with non-identical content has never been shown to exist."); *see also United States v. Beatty*, No. 1:08-cr-51-SJM, 2009 WL 5220643, at *1 n.5, *7, *20 (W.D. Pa. 2009) (denying motion to suppress evidence seized from the defendant's computer and noting that agent's affidavit described "the SHA1 'digital fingerprint' as 'more unique to a data file than DNA is to the human body' "), *aff'd*, 437 F. App'x 185 (3d Cir. 2011); s*ee generally State v. Mahan*, No. 95696, 2011 WL 4600044, at *1 n.2 (Ohio Ct. App. Oct. 6, 2011) (referring to investigator's testimony "that SHA1 values are accurate in identifying a file to the 160th degree, which is 'better than DNA' ").

As the Supreme Court recently noted, generally, under current DNA procedures, "extreme accuracy in matching individual samples" is possible with a "random match probability of approximately 1 in 100 trillion (assuming unrelated individuals)." *Maryland v. King*, 133 S. Ct. 1958, 1968 (2013) (quoting JOHN M. BUTLER, FUNDAMENTALS OF FORENSIC DNA TYPING 270 (2009)). Some have suggested, depending on the circumstances, that the odds may be slightly larger. *See also Hirschfield a 1-in-240 trillion DNA match, criminalist says*, THE SACRAMENTO BEE (Oct. 9, 2012), *available at* http://blogs.sacbee.com/crime/archives/2012/10/hirschfield-a-1-in-340-trillion-dna-match-criminalist-says.html ("A state Department of Justice criminalist testified today that Richard Joseph Hirschfield's DNA profile is a one-in-240 trillion match to a semen stain linked to the killings of two UC Davis students 32 years ago.").

In comparison, there is a higher degree of accuracy in using hash values. For example, if a DNA profile has a random match probability of 1 in 100 trillion, the odds of a match (or collision) are significantly higher for hash values, as described below. *See infra* Section V. Specifically, the 100 trillion odds for DNA (100 followed by 12 zeros) is a substantially smaller number when compared with the 340 undecillion odds for MD5 (340 followed by 36 zeros) or 1.4 quindecillion for SHA-1 (1.4 followed by 48 zeros).

The fact that the probability of a random match is significantly higher with DNA than with hash values has been noted by others. *See, e.g.*, Loren D. Mercer, *Computer Forensics Characteristics and Preservation of Digital Evidence*, 73 FBI L. ENFORCEMENT BULL. 28, 30–31 (Mar. 2004), *available at* http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2004-pdfs/mar04leb.pdf (stating

that the likelihood that "two different data set values could prove identical" under MD5 hash values is "infinitely smaller" than for DNA results based on probability tables); *see also* Cindy McPherson, *Forensic Data Collection*, XACT DATA DISCOVERY (Jan. 29, 2014), *available at* http://www.xactdatadiscovery.com/digital-forensics-101/ ("The chance of two dissimilar files having the same MD5 hash is 2×10^{34}. The chance of two people having the same DNA is 6×10^{9}. There is more of a chance of two people having the same DNA than of an MD5 value matching a dissimilar file."); *see generally* George Ou, *Putting the cracking of SHA-1 in perspective*, ZDNET (Jan. 22, 2007), *available at* http://www.zdnet.com/blog/ou/putting-the-cracking-of-sha-1-in-perspective/409 ("The science of finger print forensics or even genetic DNA matching is far less reliable than SHA-1 hashing but perfectly legitimate in the courts."); JOHN PATZAKIS & VICTOR LIMONGELLI, EVIDENTIARY AUTHENTICATION WITHIN THE ENCASE ENTERPRISE PROCESS 2 (June 2003), *available at* http://faculty.usfsp.edu/gkearns/Articles_Fraud/EEEauthentication.pdf ("The odds of two computer files with different contents having the same MD5 hash value is more than 1 in 340 undecillion. This is a higher level of certainty than even DNA enjoys.").

DNA profiling is considered to be highly reliable for identification purposes and may be used as evidence to convict or acquit an individual. Hash values, such as SHA-1, have an even higher level of precision. In terms of courtroom evidence, it is difficult to imagine any other evidence that offers the same level of accuracy and an astronomically remote chance of a random collision than that offered by hash values. Given only the theoretical possibility of collision ("finding" two random items with the same SHA-1 hash value, much less manufacturing or orchestrating a duplicate image of a hard drive or dataset) so far exceeds the odds of finding two people with the same DNA and fingerprint, that law enforcement and the courts can reasonably rely on the integrity of digital evidence verification of hashed digital evidence.

C. High level of accuracy in confirming a match

One effective use of hash values is to confirm whether two electronic records are identical. Generally, it is well-recognized that a hash value has been used to produce a greater than 99 percent probability of a match between one file and a known file. There are few matching tools that can consistently produce the same high level of accuracy.

This high level of confirming a match has been noted in several cases. *See, e.g.*, *United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012) (relying on expert testimony that "there was a 99.9999% probability that exhibit 1 contained the same video clips that" the defendant possessed), *cert. denied*, 133 S. Ct. 631 (2012); *United States v. Wellman*, 663 F.3d 224, 225 n.2 (4th Cir. 2011) ("[T]he district court found that files with the same hash value have a 99.99 percent probability of being identical."); *see also United States v. Gozola*, No. 12-130, 2012 WL 3052911, at *2 (D. Minn. July 10, 2012) (quoting officer's affidavit as noting that the "hash value can identify identical files with a certainty 'exceeding 99.99 percent,' regardless of the name given to the file by a user"); *United States v. Driver*, No. 11-20219, 2012 WL 1605975, at *1 (E.D. Mich. May 8, 2012) ("A hash value is an alphanumeric algorithm that functions like a file's DNA or fingerprint-they are essentially unique, up to 99.99%. The name of a file can change, but the hash value remains the same as long as the content is unchanged."); *United States v. Willard*, No. 3:10-CR-154, 2010 WL 3784944, at *1 n.1, *5 (E.D. Va. Sept. 20, 2010) (stating that "[b]y comparing the SHA1 values of two files, investigators can determine whether the files are identical with precision greater than 99.9999 percent certainty" and, in denying motion to suppress, rejecting request for *Franks* hearing based upon a claim "that the officers making the affidavit made false statements regarding the accuracy of SHA1"); *United States v. Collins*, 753 F. Supp. 2d 804, 808 n.6 (S.D. Iowa 2009) ("Defendant's forensic computer expert agreed . . . that SHA-1 values are in excess of 99.9999 percent accurate and that if a collision of values ever did occur, it would make P2P networks entirely obsolete."); *United States v. Wellman*, No. 1:08-cr-00043, 2009 WL 37184, at *1 n.2 (S.D. W. Va. Jan. 7, 2009) (special agent's affividavit noting, "Because each hash value is unique, an algorithm, the Secure Hash Algorithm-1 (SHA-1), can be used to show to a 99.99 percent certainty that a file with the same hash

value is an identical copy of the same file."); *see generally United States v. Bershchansky*, 958 F. Supp. 2d 354, 357 n.3 (E.D.N.Y. 2013) (Special agent's affidavit noted that "[b]y comparing the SHA1 values of two files, one can conclude that two files are or are not the same with a precision of 99.9999 percent certainty. I am aware of no documented occurrences of two different files being found on the Internet having different content while sharing the same SHA1 value. The use of SHA1 values to match movies and images has proven to be extremely reliable."); *United States v. Righter*, No. 4:11CR3019, 2011 WL 2489949, at *3 (D. Neb. May 19, 2011) (denying motion to suppress and rejecting challenge to investigator's affidavit using the 99.9999 percent accuracy figure, because the affidavit explained that, inter alia, "the origin of SHA1 values, and explains how law enforcement uses these values to create a master list for digital images known to depict child pornography" and "that based on this officer's experience and training, SHA1 values are 99.999% reliable in identifying illegal pornographic images"), *report and recommendation adopted by United States v. Righter*, No. 4:11CR3019, 2011 WL 2470673 (D. Neb. June 21, 2011).

IV. What are some common uses of hash values in investigations and cases?

Hash values have a variety of uses in investigations and at trial. As described below, hash values may be used during an investigation: (1) to support a search warrant application, (2) to comb a voluminous amount of data to determine whether particular or similar files are located on computer media, (3) to facilitate discovery (by Bates Stamping records, for de-duplication, and managing voluminous records), (4) to authenticate, locate, and reduce the amount of electronic records in a forensic examination, and (5) to authenticate and admit records at trial. While there are many ways in which hash values can be used in forensics, a few are highlighted below.

A. Investigative phase

During the investigative phase of the case, hash values may be used to identify leads and confirm the use or distribution of contraband. For example, for some crimes committed over the Internet, investigators have identified contraband by matching known files. *See, e.g.*, *United States v. Bradley*, 488 F. App'x 99, 101 (6th Cir. 2012) (affirming denial of motion to suppress and stating that during an investigation, a "specific IP address in Fayette County had been observed displaying file names and hash values consistent with known or suspected child pornography, and that this IP address was assigned to a fire station located . . . in Lexington, Kentucky"); *see also United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013) (affirming denial of motion to suppress and quashing of subpoena where an Internet service provider identified certain hash values associated with suspected child pornography and reported it to the National Center for Missing and Exploited Children).

Hash values may be used along with other information in applying for a search warrant. For example, in considering the totality of the circumstances, a hash value match or confirmation may verify the presence of an infringing item or contraband. *See, e.g.*, *infra* Section V(F)(4) (citing case examples).

During the execution of a search warrant, hash values may be used to identify electronic evidence. For example, in a copyright infringement investigation, if the infringing works have known hash values, investigators may be able to scan a large number of hard drives and identify those with hits for the infringing hash values consistent with the terms of the search warrant. While this process would take considerably less time than examining every drive manually, two factors should be considered: (1) Hashing every file on a hard drive can take a significant amount of time, and (2) because hash values are specific to only an exact duplicate, a file with any modification to the content will have a significantly different hash and would not be identified. This process can confirm whether exact duplicates of infringed copyrighted works are present on computer media, thus assisting in the decision on whether to limit the number of seized items.

B. Identifying known records

The hash of known images or files can be used to search and identify matching records. In particular, hash values are effective in reviewing a voluminous amount of data to determine whether a file or data set resides on a computer, or to determine how many copies of the file reside on the media. For this reason, the use of hash values has proven to be an effective means to identify the possession or distribution of child pornography because there is a large known set of images. *See, e.g.*, *United States v. Schimley*, 467 F. App'x 482, 484 (6th Cir. 2012) (per curiam) (Trooper "used the 'SHA-1 hash value' . . . to verify that the child-pornography video he had downloaded was the same file being shared by" the defendant); *United States v. Richardson*, 607 F.3d 357, 362–63 (4th Cir. 2010) (AOL's Image Detection and Filtering Program identified possible child pornography based on a hash value match).

The National Center for Missing and Exploited Children maintains a database of child pornography "elements." Congress has directed that the elements may include "hash values, relating to any apparent child pornography image of an identified child reported to the National Center for Missing and Exploited Children." 18 U.S.C. § 2258C (2014).

The same principle of matching hash values to contraband can be used in other areas. All that is required is a known data set for comparison. For example, in copyright infringement cases, if a known hash value is obtained for a copyrighted work, a match of the hash value may reinforce concerns about infringement. *See, e.g.*, *Breaking Glass Pictures v. John Does 1-32*, No. 2:13-cv-849, 2014 WL 467137, at *2 (S.D. Ohio Feb. 5, 2014) (alleging copyright infringement based on "the exact same unique copy of Plaintiff's movie as evidenced by the cryptographic hash value") (footnote omitted); *TCYK, LLC v. Does 1-47*, No. 2:13-cv-539, 2013 WL 4805022, at *2 (S.D. Ohio Sept. 9, 2013) ("Plaintiff also alleges that 'all of the infringements alleged in this lawsuit arise from the exact same unique copy of Plaintiff's movie as evidenced by the cryptographic hash value.' ") (footnote omitted); *Bicycle Peddler, LLC v. John Does 1-177*, No. 13-cv-0671-WJM-KLM, 2013 WL 1103473, at *1 (D. Colo. Mar. 15, 2013) (In considering joinder of multiple defendants in a copyright infringement action, the court stated that "[d]uring the course of this investigation, the company identified 177 IP addresses in the District of Colorado that had downloaded a file with one of the following hash values: 354A7CFDE35B396C4F2130CEA73CA71 DO or 5E813482FACE3941 F09D3FBB7AA1 F98327 ('Hash Numbers'), which have been associated with the Work.") (footnote omitted).

C. Discovery

In cases involving voluminous amounts of electronic records, hash values may be used during discovery for civil and criminal cases. Hash values are being used in a number of ways in the discovery process.

A new substitute for Bates stamping: Traditionally, discovery has followed a Bates Numbering process to identify each page or document. Based on the increasing use of electronic evidence, hash values are beginning to be substituted for the number role served by the Bates Stamp. *See, e.g.*, BARBARA J. ROTHSTEIN, RONALD J. HEDGES & ELIZABETH C. WIGGINS, FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 38 (2d ed. 2012), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt2d_eb.pdf/$file/eldscpkt2d_eb.pdf (" 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production."); *see also* Ralph C. Losey, *HASH: The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1, 12–13 (2007), *available at* http://ralphlosey.files.wordpress.com/2007/09/hasharticlelosey.pdf (proposing a process for using hash values to mark discovery).

In fact, some courts have formally suggested that parties use hash values for electronic records:

> Because identifying information may not be placed on ESI as easily as bates-stamping paper documents, methods of identifying pages or segments of ESI produced in discovery

> should be discussed, and, specifically, and without limitation, the following alternatives may be considered by the parties: electronically paginating Native File ESI pursuant to a stipulated agreement that the alteration does not affect admissibility; renaming Native Files using bates-type numbering systems, *e.g.*, ABC0001, ABC0002, ABC0003, with some method of referring to unnumbered "pages" within each file; using software that produces "hash marks" or "hash values" for each Native File; placing pagination on Static Images; or any other practicable method. The parties are encouraged to discuss the use of a digital notary for producing Native Files.

U.S. DIST. COURT FOR THE DIST. OF MD., SUGGESTED PROTOCOL FOR DISCOVERY OF ELECTRONICALLY STORED INFORMATION ("ESI") 20–21 (2009), *available at* http://federalevidence.com/pdf/2008/09-Sept/DMd_Protocol%20for%20ESI%20Discovery.pdf; *see also* U.S. DIST. COURT FOR THE DIST. OF KAN., GUIDELINES FOR CASES INVOLVING ELECTRONICALLY STORED INFORMATION [ESI] 7 (2013), *available at* http://www.ksd.uscourts.gov/guidelines-for-esi ("Because identifying information may not be placed on ESI as easily as bates stamping paper documents, methods of identifying pages or segments of ESI produced in discovery should be discussed. Counsel are encouraged to discuss the use of either a digital notary, hash value indices or other similar methods for producing native files.") (footnotes omitted).

De-duplication: Given the voluminous amount of discovery of electronic records, hash values can be used to reduce the amount of production in discovery. Some courts have specifically suggested the use of hash values or a hash database to remove duplicate data or unnecessary information. One example from the District Court of Kansas provided:

> Counsel should discuss the elimination of duplicative ESI and whether such elimination will occur only within each particular custodian's data set or whether it will occur across all custodians, also known as vertical and horizontal views of ESI.
>
> In addition, counsel should discuss the de-NISTing of files which is the use of an automated filter program that screens files against the NIST list of computer file types to separate those generated by a system and those generated by a user. [NIST (National Institute of Standards and Technology) is a federal agency that works with industry to develop technology measurements and standards.] NIST developed a hash database of computer files to identify files that are system generated and generally accepted to have no substantive value in most cases.

U.S. DIST. COURT FOR THE DIST. OF KAN., GUIDELINES FOR CASES INVOLVING ELECTRONICALLY STORED INFORMATION [ESI] 6 (2013) (footnote omitted), *available at* http://www.ksd.uscourts.gov/guidelines-for-esi.

Discovery orders may contain stipulations to use hash values for de-duplicating discovery. *See, e.g.*, *North Carolina State Conference Of The NAACP v. McCrory*, Nos. 1:13-CV-658, 1:13-CV-660, 1:13-CV-861, at 8 (M.D.N.C. Jan. 17, 2014), *available at* http://moritzlaw.osu.edu/electionlaw/litigation/documents/NAACP_000.pdf (revised consent order regarding discovery of documents and electronically stored information) ("The parties agree to use MD-5 hash values to deduplicate exact duplicate documents for individual custodians.").

In large cases, discovery management procedures will use hash values as part of the de-duplication process. *See, e.g.*, *United States v. eBay, Inc.*, No. 12-cv-05869-EJD, 4, 10 (Doc. No. 34-2) (N.D. Cal. May 31, 2013), *available at* http://www.justice.gov/atr/cases/f297500/297578.pdf (attachment B to joint case management statement and [proposed] order: DOJ standard specifications for production of ESI) (providing metadata table listing hash values for MD5 and SHA-1 "used for deduplication or other processing," and stating, "Before doing any de-duplication, provide the Division with a written description of the method used to de-duplicate (including which elements are compared and what hash

codes are used), and what is considered a duplicate."); *In re Elec. Books Antitrust Litig.*, No. 12-cv-03394-DLC, 16, 19 (Doc. No. 111) (S.D.N.Y. July 6, 2012), *available at* http://www.justice.gov/atr/cases/f285000/285031.pdf (joint initial report revised) ("Apple will use a document hosting vendor to apply non-manual techniques to cull duplicates and material previously produced to the DOJ, including but not limited to the MD5 Hash standard within custodians. Apple will then manually review documents for attorney-client privilege, work-product, and responsiveness as well as to prepare documents for production. . . . ESI will be subject to date restrictions, as agreed by counsel, and will be de-duped by custodian using a MD5 Hash standard.").

Discovery management of privileged communications: In managing discovery, hash values may be useful in marking or locating particular records. Since hash values do not reveal the content of the record but only identify a particular data set, hash values have proven useful in addressing attorney-client privilege issues.

For example, where privileged communications may be involved, the parties may obtain a log of privileged communications. The hash value and any relevant metadata may establish the existence of the communication. If a court needs the list for *in camera* review, the list of hash values will be useful. (In the same way, contraband may be identified by hash values without viewing the contraband, such as child pornography.)

D. Computer forensic examinations

Hash values have numerous uses in forensic examinations, in fact, too many to list. As a general overview, hash values may assist in three primary areas of forensic examinations: (1) authenticating electronic records, (2) identifying or finding records, and (3) reducing the amount of data for review. In criminal cases, a forensic examination will normally be conducted pursuant to the terms of a search warrant, unless some other legal basis for the examination is authorized (such as consent).

Authenticating electronic records: One primary function for hash values is to authenticate electronic records. A common means occurs during the imaging and examination process of a computer hard drive.

Prior to a forensic examination, three hash values are normally obtained for seized media (such as a computer hard drive). Consider this example:

> Agents seize a computer hard drive pursuant to a search warrant. Initially, a decision may be made on whether to image the hard drive on site or to seize it and book it into evidence. Due to a host of factors, let's assume the original is booked into evidence. Back at the lab, a bit by bit mirror image of the original will be made. In this process, a *first* hash value will be obtained of the original computer hard drive. After the imaging, a *second* hash value will be made of the mirror image copy. A match in the two hash values confirms that the copy is identical to the original. A mismatch would alert the examiner to determine what caused the discrepancy.
>
> Consistent with best practices, the forensic examination is conducted on the copy. The original is therefore returned to evidence control. After the forensic examination is completed, a *third* hash value will be made of the mirror image copy. A third match will confirm the integrity of the examination, that is, no alterations were made during the examination process. This final hash verification helps document that none of the processes or tools used in the examination made any modifications to the forensic image. Similar to this final hash verification, a hash value is generated for any file extracted from the original forensic image. This hash is compared to the file inside

the original forensic image to ensure the extracted copy is an exact duplicate and no changes/modifications occurred during the extraction.

A copy of the original forensic image file may also be copied to a forensic server. A study of 100,000 different types of hard disk drives, conducted by researchers at Carnegie Mellon University, found that the actual reported failure rate of hard disk drives is much higher than stated in manufacturers' data sheets. BIANCA SCHROEDER & GARTH A. GIBSON, COMPUTER SCIENCE DEP'T, CARNEGIE MELON UNIV., DISK FAILURES IN THE REAL WORLD: WHAT DOES AN MTTF OF 1,000,000 HOURS MEAN TO YOU?, FAST07, 5TH USENIX CONFERENCE ON FILE AND STORAGE TECHNOLOGIES (2007), *available at* http://www.pdl.cmu.edu/ftp/Failure/failure-fast07.pdf. Although the observed real world failure rates were between approximately 2 to 4 percent (with some as high as 13 percent), which are relatively low, frequent handling and transportation of hard disk drives inevitably jostles the sensitive mechanical parts in the drives and can only increase the potential for drive failure. A more advanced and safer method of maintaining forensic images is to upload, or copy, the forensic image to a fault tolerant Redundant Array of Independent (or Inexpensive) Disks (RAID) system. The entire purpose of RAID storage is redundancy—if one disk in the array fails, the data remains secure on one of the other redundant disks. Also, unlike a powered-down hard disk drive, a running RAID system can be configured to conduct routine backups to tape archives, which can be stored off-site. This is a useful data recovery backstop in the event of a disaster, such as a flood or fire at an evidence storage location. Indeed, the implementation of secure RAID evidence storage appears to adhere to the National Institute of Justice, Office of Justice Programs' recommendation that investigators preserve evidence "in a manner designed to diminish degradation or loss." NAT' INST. OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, DEP'T OF JUSTICE, CRIME SCENE INVESTIGATION: A GUIDE FOR LAW ENFORCEMENT 28 (2000), *available at* http://www.ncjrs.gov/pdffiles1/nij/178280.pdf. After transferring a copy of the forensic image file to a forensic server, the hash value is verified again to ensure no changes or damage occurred during the transfer.

Other files may be authenticated as part of the examination. For example, the computer forensic expert may use a hash value comparison to explain how the hash of a known file matched other files during the forensic examination.

Data reduction: Hash values can provide efficiencies by reducing the amount of data to be reviewed and, therefore, can save time spent reviewing relevant records. *See generally* Dan Mares, *Using File Hashes to Reduce Forensic Analysis*, SC MAGAZINE (May 1, 2002), *available at* http://www.scmagazine.com/using-file-hashes-to-reduce-forensic-analysis/article/30472 (highlighting the role of hash values in data reduction for forensic review). At the onset of a forensic examination, examiners often use Known File Filters (KFFs) to eliminate certain files and highlight others. Typically, there are at least two types of KFFs: (1) Known Ignorable, and (2) Known Alerts. Known ignorable files generally are operating system and application files. By eliminating known operating system and application files that contain no user information, examiners can sometimes reduce the amount of files to examine in a case by nearly 50 percent. In corporate or other structured environments, examiners can often obtain what is known as the corporate "Gold Standard." This gold standard includes data for new fully configured computer systems that are provided to new employees. By eliminating all files that come standard on a system, examiners can focus on only those files that have been created or changed by user actions.

There are several kinds of known alert files. The National Center for Missing and Exploited Children maintains a list of hashes of known child pornography. The National Software Reference Library (NSRL) provides the collection of hashes of software from various sources that are incorporated into a Reference Data Set (RDS) of information. The NSRL RDS contains known ignorable hash sets for various operating systems and applications, as well as known alerts for files that may be considered malicious (for example, keyloggers, steganography tools, and hacking scripts), but do not contain any hash values of any illicit data. Other organizations (both private and governmental) often create and maintain their own set of hash libraries. The purpose of these hash libraries ranges from known

intellectual property to classified documents. Depending on the situations, investigative agencies may create or use case specific hash libraries to quickly identify and categorize known files (either as ignorable or alert for further review).

Identifying and locating matching or similar records: During a forensic examination, hash values also provide a valuable tool to identify records. One value of using known file filter alerts (hash value libraries) is that they allow the rapid identification of very specific files, without exposing the digital investigative analyst to the content of the file. If an alert hash library identifies a file, even without human examination, the file is known to be an exact copy of a known file. Because identifying files via their hash does not require or expose any human to the content of the file, this technique provides the least amount of invasion of privacy. In classified environments, this technique would allow an analyst to detect the existence of highly classified documents, to know what classification level the documents are, and to alert the authority with the proper clearance level, all without being exposed to information. Some Internet or mail service providers also employ hash libraries to detect malware, viruses, and contraband. *See, e.g.*, *United States v. Richardson*, 607 F.3d 357, 362–63 (4th Cir. 2010) (noting operation of AOL's Image Detection and Filtering Program).

During forensic examinations, hash values are often used to identify duplicate copies of files, regardless of their file name. It is not uncommon to find identical files with different file names. This occurs both unwittingly when a user downloads the same file to the same location twice and when the operating system automatically modifies the file name (in many cases appending the word "copy" or "(1)" to the file name). Other instances have occurred when the user renames a file in an attempt to hide it. (For example, a user renames a trade secret Word document to look like a picture file.). As previously discussed, the file name is not part of the file content that is hashed and, as such, has no impact on the hash value of the file. *See* Section II(D), *supra*.

What if the user intentionally alters the data set to avoid a match with hash values? With "fuzzy hashing" (or context triggered piecewise hashing), files that have been slightly modified may be identified. The "fuzzy hashing" tool is able to locate data that contains a high percentage of similarities. *See generally* Jesse Kornblum, *Identifying almost identical files using context triggered piecewise hashing*, *in* DIGITAL INVESTIGATION S91–97, S91 (2006), *available at* http://dfrws.org/2006/proceedings/12-Kornblum.pdf ("describ[ing] a method for using a context triggered rolling hash in combination with a traditional hashing algorithm to identify known files that have had data inserted, modified, or deleted"). Consequently, if slight alterations are made to a record, these records may be found using the "fuzzy hashing" tool. "Fuzzy hashing" may be particularly useful to locate intellectual property documents that have been slightly modified.

E. Trial evidence

At trial, hash values may be used to admit forensic evidence or electronic records. A recent child pornography prosecution in the Eleventh Circuit demonstrates how hash values were used to authenticate and admit videos and images obtained from the defendant's computer.

> [Defendant] challenges his convictions on the ground that the District Court abused its discretion in admitting into evidence Government's Exhibit 11, a CD containing videos and still images of child pornography. [Investigator] Wilkins testified that the videos and images on the exhibit had SHA-1 values matching the SHA-1 values for the files he found on [Defendant's] computers. "SHA" stands for Secured Hash Algorithm, which is "used to compute a condensed representation of a message or date file." *United States v. Miknevich*, 638 F.3d 178, 181 n.1 (3d Cir. 2011). A SHA-1 value "can act like a fingerprint." *Id. See also United States v. Sutton*, 350 F. App'x. 780, 781 n.1 (3d Cir. 2009) (a SHA-1 value is "a kind of digital fingerprint") (unpublished). A national data base contains a listing of SHA-1 values for known images of child

> pornography. Thus, when Wilkins identified file names on [Defendant's] computers indicative of child pornography, he checked the national database for the SHA-1 values for those files. When he found a match, he concluded that a specific file saved on [Defendant's] computer contained an image of child pornography.
>
> The district court, pursuant to Federal Rule Evidence 104, found that Exhibit 11 contained videos and images that matched videos and images stored on [Defendant's] computer. The evidence was obviously relevant and thus admissible, *see* Federal Rule of Evidence 402, unless the District Court's threshold findings—that the videos and images on the computers matched what Wilkins found in the national database—were clearly erroneous. We conclude that they were not. To the extent that [Defendant] contends that the evidence should have been excluded under Federal Rule of Evidence 403, his contention is meritless. Exclusion of relevant evidence under Rule 403 is an extraordinary remedy, a discretionary call. We find no abuse of discretion in the call the court made, to admit Exhibit 11 into evidence.

United States v. Cobb, 479 F. App'x 210, 211–12 (11th Cir. 2012). In *Cobb*, the SHA-1 hash values confirmed a match of files obtained from the defendant's computer with a known database. The trial court was able to make an admissibility ruling under Federal Rule of Evidence 104. The files were relevant to issues at trial and not unfairly prejudicial. *Id.* at 212.

In another trial, a forensic expert authenticated images found on the defendant's computer with known images by comparing the hash values:

> A government expert, however, verified that the images in exhibits 3 through 17 were the actual enlarged images from [Defendant's] computer. To the extent [Defendant] is challenging the government's exhibit 1 (a DVD compilation of three video clips from a law enforcement database), the SHA-1 values of these videos matched the SHA-1 values of the files offered for distribution from [Defendant's] computer.

United States v. Glassgow, 682 F.3d 1107, 1110 (8th Cir. 2012) (footnote omitted), *cert. denied*, 133 S. Ct. 631 (2012). These cases provide a few recent examples of how hash values have been used to admit electronic evidence at trial.

V. How likely is one-in-340 undecillion or even one-in-1.4 quindecillion?

The likelihood of a random match for electronic evidence using hash values is *extremely* remote. The probability is unparalleled when compared with other evidence typically admitted in court. In fact, the numbers are astronomical and daunting. To grasp the remoteness, some uncommon numbers must be considered.

A. An undecillion and other large numbers

An undecillion is a very large number. It is 10^{36} or 1 followed by 36 zeros:

1,000,000,000,000,000,000,000,000,000,000,000,000

Alternatively, it is 1 billion, billion, billion, billion. To place this number in context, undecillion follows some other very large numbers:

- billion, 1 followed by 9 zeroes
- trillion, 12 zeroes
- quadrillion, 15 zeroes
- quintillion, 18 zeroes

- sextillion, 21 zeroes
- septillion, 24 zeroes
- octillion, 27 zeroes
- nonillion, 30 zeroes
- decillion, 33 zeroes

Next is undecillion, 1 followed by 36 zeroes. Yet it is still smaller than:

- duodecillion, 39 zeroes
- tredecillion, 42 zeroes
- quattuordecillion, 45 zeroes
- quindecillion, 48 zeroes
- or even googol, 100 zeroes

See generally RUSS ROWLETT, HOW MANY? A DICTIONARY OF UNITS OF MEASUREMENT, NAMES FOR LARGE NUMBERS, *available at* http://www.unc.edu/~rowlett/units/large.html.

B. MD5 remote improbability of a random match

What is the significance of an undecillion for hash values? Actually, the likelihood of two different files randomly having the same MD5 hash value is 2^128, or more than 1 in 340 undecillion (or more than 1 in 340 billion, billion, billion, billion chance). The exact number is:

1 in 340,282,366,920,938,463,463,374,607,431,768,211,456

Brian Deering explained the remoteness of this number by stating, "There are actually 3.402 x 10^38 or 340 billion billion billion billion or a little more than 1/3 of a googol possibilities. When you consider that most people have never seen a million of anything the actual number becomes really difficult to conceptualize." BRIAN DEERING, DATA VALIDATION USING THE MD5 HASH, *available at* http://www.woodmann.com/crackz/Tutorials/Md5info.htm; *see also Hashing!*, VENDARI (Mar. 19, 2013), *available at* http://verndari.net/archives/tag/hash-collision (reviewing the probabilities); STEVE MEAD, UNIQUE FILE IDENTIFICATION IN THE NATIONAL SOFTWARE REFERENCE LIBRARY 2 n.1 (2005), *available at* http://www.nsrl.nist.gov/Documents/analysis/draft-060530.pdf ("The probability of a collision between hashes in either MD5 or SHA1 is so small that it is effectively zero.").

C. SHA-1 remote improbability of a random match

For SHA-1, the chance of two different files randomly having the same hash value is even more remote: 2^160, or a 1.46 trillion, trillion, trillion, trillion. *See* WOLFRAMALPHA, *available at* http://www.wolframalpha.com/. To date, the authors can find nothing beyond the theoretical documentation of random collisions (the likelihood of two items randomly having the same SHA-1 hash value).

Furthermore, attempts at calculating even theoretical collision resistance of SHA-1 range from 2^69 to 2^160. *See* XIAOYUN WANG, YIQUN LISA YIN & HONGBO YU, FINDING COLLISIONS IN THE FULL SHA-1 2 (2005), *available at* http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf; *see generally* T. POLK ET AL., SECURITY CONSIDERATIONS FOR THE SHA-0 AND SHA-1 MESSAGE-DIGEST ALGORITHMS 4 (Internet RFCs, ISSN 2070-1721, RFC 6194, 2011), *available at* http://www.rfc-editor.org/pdfrfc/rfc6194.txt.pdf ("[I]t will take 2^106 computations to find a second pre-image in a 60-byte message."); QUYNH DANG, COMPUTER SEC. DIV., INFO. TECH. LAB., RECOMMENDATION FOR APPLICATIONS USING APPROVED HASH ALGORITHMS 8 (2012), *available at* http://csrc.nist.gov/publications/nistpubs/800-107-rev1/sp800-107-rev1.pdf (discussing strengths of the approved hash algorithms);

Richard P. Salgado, *Fourth Amendment Search And The Power Of The Hash*, 119 HARV. L. REV. F. 38, 39 n.6 (2006) ("[T]he prolific algorithm MD-5 can generate more than 340,000,000,000,000,000,000,000,000,000, (that's 340 billion, billion, billion, billion) possible values. The widely used SHA-1 algorithm generates a range of values over four billion times larger than that. Thus, although there is a finite number of possible hash values and an infinite number of possible data inputs, the odds of a collision are infinitesimally small.").

To put these numbers in context, 2^69 equals approximately 590 quintillion (590,295,810,358,705,651,712 or 5.90295810358705651712 × 10^20). In contrast, 2^160 equals approximately 1 quindecillion. The odds of two different files having the same SHA-1 hash value is:

1 in 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976

or 1.46150163733090291820368483271628301965593254297 6 × 10^48

or 1.461 trillion, trillion, trillion, trillion

These numbers demonstrate the extreme improbability of a random collision (or a random match in hash values for two different data sets). The remote "possibility" of a random hash value collision is discussed in Section IV(E) below.

D. Comparing the odds

The extremely remote "possibility" (actually, improbability) of a random collision for hash values is difficult to comprehend. It is exceedingly rare to find other evidence involving a comparable infinitesimally remote unlikelihood.

To put these numbers in context, it helps to compare the odds with some other occurrences:

Event	Odds	Source/Notes
Struck by lightening	1 in 750,000	• LIGHTNING—FREQUENTLY ASKED QUESTIONS, NATIONAL WEATHER SERVICE, *available at* http://www.srh.noaa.gov/jetstream/lightning/lightning_faq.htm.
Killed by a shark	1 in 3,700,000	• Meg Gleason, *Nat Geo WILD: What Are the Odds? Some Surprising Shark Attack Stats*, NAT GEO WILD (Nov. 22, 2011), *available at* http://newswatch.nationalgeographic.com/2011/11/22/nat-geo-wild-what-are-the-odds-some-surprising-shark-attack-stats/.
Odds of a ladder U.S. currency note	1 in 16,666,667	• A ladder currency note results when each digit in a serial number is one number higher than the prior digit (for example, 01234567). • Odds are based on a "randomly selected note from a run of 99,999,999 consecutive notes." Dave Undis, *How Rare are Fancy Serial Numbers?*, 274 PAPER MONEY 293, 297 (2011), *available at* http://coolserialnumbers.c

		om/HowRareAreFancySerialNumbers.pdf.
Winning the Mega Millions lottery	1 in 259 million or more	• *See* Tanya Basu, *Feeling Lucky? How Lotto Odds Compare to Shark Attacks and Lightning Strikes*, NATIONAL GEOGRAPHIC (Dec. 19, 2013), *available at* http://news.nationalgeographic.com/news/2013/12/131219-lottery-odds-winning-mega-million-lotto/ (noting it is "more likely to get killed by an asteroid or injured by a toilet than win the lottery"). • *See also* Matt Stevens, *$400-million Powerball: Odds of winning are 1 in 175 million*, L.A. TIMES (Feb. 19, 2014, 4:30 AM), *available at* http://www.latimes.com/local/lanow/la-me-ln-400-million-powerball-jackpot-numbers-20140218,0,7635405.story#ixzz2vT1qlIEC.
Selecting a perfect March Madness basketball bracket	1 in 128 billion	• Derek Thompson, *Warren Buffett and Quicken Loans Will Pay You $1 Billion for the Perfect March Madness Bracket*, THE ATLANTIC (Jan. 21, 2014), *available at* http://www.theatlantic.com/business/archive/2014/01/warren-buffett-and-quicken-loans-will-pay-you-1-billion-for-the-perfect-march-madness-bracket/283228/ ("Those odds are 1 in 128 billion, according to DePaul math professor Jeff Bergen. (Some outlets are quoting 1 in 9.2 quintillion, but that assumes that all 63 games are 50-50 toss-ups, which they're not. For example, Number 1 seeds just about always advance to the second round.) If everyone in the United States filled out a bracket, Chris Chase calculated, we'd get a $1 billion winner every 400 years."). • *See also Warren Buffett Wants to Pay You $1 Billion for the Perfect March Madness Bracket*, REUTERS (Jan. 29, 2014, 3:51 PM), *available at* http://www.reuters.com/article/2014/01/29/idUS35781187820140129 ("The chances of someone predicting the correct outcome of all 63 games is around 1 in 9.2 quintillion (that's 18 zeroes).") (assuming each team has an equal change to win).
DNA random	1 in 100 trillion	• 100 trillion is 1 followed by 14 zeroes.

match probability		• JOHN M. BUTLER, FUNDAMENTALS OF FORENSIC DNA TYPING 270 (2009) ("Since they were selected in November 1997, the 13 CODIS core STR loci have been required for data entry into the national level of the U.S. DNA database. These 13 STR markers provide a random match probability of approximately 1 in 100 trillion (assuming unrelated individuals)."), *cited in Maryland v. King*, 133 S. Ct. 1958, 1968 (2013).
Lottery: Selecting the 20 random winning numbers between 1 and 80	1 in 1 quintillion	• 1 quintillion is 1 followed by 18 zeroes. • Mike Orkin, WHAT ARE THE ODDS? CHANCE IN EVERYDAY LIFE 13–14 (2000) ("If there is one drawing per week and everyone on earth (6 billion people) always buys a ticket, it will take an average of about 5 million years to produce a winner.").
Coin Toss: Chance of 100 consecutive heads in 100 coin tosses	1 in 1 nonillion	• 1 nonillion is 1 followed by 30 zeroes. • Mike Orkin, WHAT ARE THE ODDS? CHANCE IN EVERYDAY LIFE 14 (2000) ("If every person on earth (6 billion people) starts tossing coins 24 hours per day, with each person tossing at the rate of 100 tosses every 5 minutes, it will take an average of about a million billion (1,000,000,000,000,000) years until somebody gets 100 heads in 100 tosses.").
Possible values generated by an MD-5 hash	1 in 340 undecillion	• Precisely: 340,282,366,920,938,463,463,374,607,431,768,211,456 • Or 340 followed by 36 zeroes • Or 340 billion, billion, billion, billion • *See* WOLFRAMALPHA, *available at* http://www.wolframalpha.com/. • *See also* BRIAN DEERING, DATA VALIDATION USING THE MD5 HASH, *available at* http://www.woodmann.com/crackz/Tutorials/Md5info.htm.

Possible values generated by a SHA-1 hash	1 in 1.46 quindecillion	• Precisely: 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 • Or 1.46 followed by 48 zeroes • Or 1.46 trillion, trillion, trillion, trillion • Or 4 billion times larger than the possible values generated by an MD-5 hash • *See* WOLFRAMALPHA, *available at* http://www.wolframalpha.com/.

When it comes to hash values, the likelihood of a match for two different data sets are infinitesimally small and remote, particularly when compared to many daily events. *See generally* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 30 (2d ed. 1996), *available at* http://www.cse.iitk.ac.in/users/anuag/crypto.pdf.

Specifically, if someone claims that hash values are unreliable for forensic purposes, based on theoretical collisions, the astronomical improbability of a collision must be understood in context. No other evidence provides the same remote probabilities, including DNA or fingerprint evidence, which are often considered to be highly reliable.

As noted in Section V(F) below, it is also relevant to consider the legal context for which the hash value is being considered. For example, authentication normally requires a "prima facie" or "some evidence" showing of genuineness under Federal Rule of Evidence 901(a). After this threshold showing, the judicial process will be used to test and assess the strengths and weaknesses of any evidence.

E. Theoretical "collision possibility"

Occasionally, the argument is advanced that it is theoretically "possible" for two different records to have a matching hash value. This is often referred to as a "collision." *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 36 (2013) (a "collision" occurs when "[t]wo or more distinct inputs produce the same output"), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Theoretical developments: Some recent papers have provided *theoretical* collisions for some hash values. *See, e.g.*, XIAOYUN WANG, DENGGUO FENG, XUEJIA LAI & HONGBO YU, COLLISIONS FOR HASH FUNCTIONS MD4, MD5, HAVAL-128 AND RIPEMD (2004), *available at* http://eprint.iacr.org/2004/199.pdf; XIAOYUN WANG, YIQUN LISA YIN & HONGBO YU, COLLISION SEARCH ATTACKS ON SHA1 (2005), *available at* http://www.c4i.org/erehwon/shanote.pdf; *see generally* Bruce Schneier, *Cryptanalysis of SHA-1*, SCHNEIER ON SECURITY (Feb. 18, 2005), *available at* https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html ("Earlier this week, three Chinese cryptographers showed that SHA-1 is not collision-free. That is, they developed an algorithm for finding collisions faster than brute force.").

Assessing the theoretical significance for reviewing electronic evidence: To what extent should a theoretical "collision" matter in using hash values for computer forensics purposes? While a collision is certainly important for cryptography, military communications, digital certificates for secure

Web sites, and network and information security, it does not undermine the role of hash values for forensic purposes.

First, the role in using hash values must be considered. In information security, any vulnerability must be identified, assessed, and analyzed. Remote possibilities may be too risky for national or information security purposes. *See, e.g.*, QUYNH DANG, COMPUTER SEC. DIV., INFO. TECH. LAB., RANDOMIZED HASHING FOR DIGITAL SIGNATURES 2 (2009) (NIST Special Publication 800-106), *available at* http://csrc.nist.gov/publications/nistpubs/800-106/NIST-SP-800-106.pdf ("Collision resistance is a required property for the cryptographic hash functions used in Digital Signature Applications."); WILLIAM E. BURR, U.S. NAT'L INST. OF STANDARDS & TECH., CRYPTOGRAPHIC HASH STANDARDS: WHERE DO WE GO FROM HERE? 88 (2006), *available at* http://csee.wvu.edu/~katerina/Teaching/CS-465-Fall-2007/HashStandards.pdf ("[R]esearchers have successfully attacked MD5 and SHA-1, the two most commonly used cryptographic hash functions. It's no longer advisable to use them in applications such as digital signatures, although some other applications, such as hashed message authentication codes, aren't affected.").

In contrast, for forensic examinations, hash values are used as a tool to review and authenticate existing data. A collision has not been shown to impact the use of hash values for forensics. The context in which the hash values are being used must be taken into account. The security concerns over collision for cryptography do not bear on the use of hash values for forensic purposes.

Second, a random collision has never been observed in an actual case. What may be *possible* in a laboratory environment remains *improbable* in an actual case. In the lab, the theory can be considered by *manipulating* or *controlling* certain variables. For example, matching hash values can theoretically be constructed. The two data sets (or inputs) are manufactured to test the collision theory. In contrast, the *random* collision for hash values has *never* been observed in *any* case.

Consequently, the possibility of a collision is confined to theory, not to the real world. *See, e.g.*, *United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at *3 (D. Vt. Nov. 8, 2013) (noting "a collision between two files with identical SHA1 values but with non-identical content has never been shown to exist") (footnote omitted); *see also* Richard P. Salgado, *Fourth Amendment Search And The Power Of The Hash*, 119 HARV. L. REV. F. 38, 40 n.8 (2006) ("Research shows that, under controlled and artificial circumstances, it is possible to engineer two different files with the same hash value. Some effort has been made to design a tool that can create collisions. It is extremely unlikely that collisions would happen in the wild, much less in the context of digital media imaging and forensics.").

Third, in an examination, one hash value result is never considered in isolation. Other circumstances and factors concerning any record can be considered. In fact, most forensic tools generate multiple hashes. For example, by default, Access Data's Forensic Tool Kit (FTK), the most widely used digital investigative analysis software, generates three different hash values for every file (MD5, SHA-1 and SHA-256). Furthermore, FTK Imager, one of the most popular software applications to create forensic images, by default, generates two different hash values when creating forensic images MD5 and SHA-1.

Other forensic tools are used to authenticate extracted data. The theoretical "collision" argument focuses on one narrow issue and fails to consider the variety of tools used in a forensic examination.

Fourth, questions about the identity of any record can be considered in conjunction with the surrounding circumstances. For example, the electronic evidence usually will consist of much more than the mere confirmation of a match in hash values. Other circumstances, such as the time and location of the file, corroborated with external information (witness interviews and events), will be considered. In this manner, hash values provide a powerful tool to confirm an event. The surrounding case circumstances may explain or provide further insight into any discrepancy. The hash value result provides

only one piece of information that is considered along with other facts uncovered in the forensic examination or case investigation.

Fifth, it is unlikely that any case will focus only on one matching hash value for two records. For example, if there was one match for one copyright infringed work, there likely are many others in the case. Consequently, there likely will be multiple hash value matches for each different record. It is simply infeasible to anticipate that multiple "collisions" will result in any one case. If the odds of a random match are remote for one file, they are significantly more remote where multiple files may be involved. For this additional reason, the theoretical possibility of a collision is unlikely to impact the forensic review in any single case.

Finally, as noted below, the judicial process has time-tested avenues to assess the strengths and weaknesses of any evidence. All evidence remains subject to challenge and review under established standards and processes. Electronic evidence is not treated any differently under the Federal Rules of Evidence and judicial processes. *See infra* Section IV(F).

For these reasons, the theoretical remote possibility of a collision is immaterial when it comes to the use of hash values in forensics. When viewed in proper context, the collision issue does not undermine the role of hash values for forensic purposes.

Judicial rejection of "collision" arguments: Not surprisingly, the mere theoretical possibility of a collision has been raised in challenges to electronic evidence presented in court. When this issue has been advanced, the courts have rejected it.

Consider a case where this argument was considered through expert testimony. The district court summarized the following:

> Each party presented an expert who testified regarding the reliability of hash values in file identification. Cartier's expert testified hash values are not a reliable means of determining what a file contains. He testified an investigator cannot evaluate a file's content based on the hash value alone. He also testified two files could have duplicate hash values but completely different content, known as a "collision" of hash values. The Government's expert testified that hash values were a reliable means of investigating child pornography because in practical application, a file's hash value is unique to that file. He testified that if this premise were not true, P2P networks would not work because the searcher could not reliably search for a known file, which is what P2P networks are designed to do. He also testified that as long as the investigator starts with an image with known content and a known hash value, an investigator can use the hash value to search for duplicates of that file. Both experts testified that in their professional knowledge, the only collision of hash values ever encountered were in studies designed to prove that hash values can be duplicated in different files. The Government's expert testified that had two hash values ever collided in "real-world" application, the event would be well publicized because it would be significant in their field.

United States v. Cartier, No. 2:06-cr-73, 2007 WL 319648, at *2 (D.N.D. Jan. 30, 2007). The Eighth Circuit affirmed the district court's denial of the motion to suppress and noted that the trial court heard both experts. It also rejected the defense's expert testimony "that hash values could collide and that in laboratory settings these values had done just that" after crediting government expert testimony "that no two dissimilar files will have the same hash value." *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008).

Relying on *Cartier*, the Fourth Circuit arrived at the same conclusion when the argument was presented:

> A "hash value" is an alphanumeric string that serves to identify an individual digital file as a kind of "digital fingerprint." Although it may be *possible* for two digital files to have hash values that "collide," or overlap, it is *unlikely* that the values of two dissimilar images will do so. *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008). In the present case, the district court found that files with the same hash value have a 99.99 percent probability of being identical.

United States v. Wellman, 663 F.3d 224, 226 n.2 (4th Cir. 2011) (emphasis added) (suspected child pornography identified by hash values), *cert. denied*, 132 S. Ct. 1945 (2012).

In another case, the theoretical argument was made and then withdrawn in light of "real world experience." *United States v. Collins*, 753 F. Supp. 2d 804, 808 n.6 (S.D. Iowa 2009). In denying a motion to suppress a search warrant, the district court noted:

> Defendant argued in his brief that using SHA-1 values to compare files was an inaccurate method of confirming the presence of contraband content because of the theoretical possibility that two SHA-1 values could collide. In the wake of evidence that, in actual real world experience, two SHA-1 values have never collided, the Defendant withdrew this argument. In fact, Defendant's forensic computer expert agreed with Special Agent Larsen that SHA-1 values are in excess of 99.9999 percent accurate and that if a collision of values ever did occur, it would make P2P networks entirely obsolete.

Id.

Several other cases have reached the same result. *See, e.g.*, *United States v. Stewart*, 839 F. Supp. 2d 914, 931 (E.D. Mich. 2012) ("The likelihood of two data collections having the same hash value is extremely remote, so hash values can be used to verify that a forensic image or clone was captured successfully."); *see also United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at *13 (D. Vt. Nov. 8, 2013) (Defense expert initially "opined that a SHA1 value is not a reliable indicator of a file's contents and that more than one file may have the same SHA1 value. She later clarified her testimony to acknowledge that she had personally never seen or heard of a SHA1 value colliding, and she acknowledged that two files with the same SHA1 value cannot have different content. (Tr. 7/30/13 at 86, 87.) She asserted a similar opinion with regard to the MD4 hash value, but did not cite to any specific instances of collisions or any research that has found an MD4 hash value cannot reliably be used to identify a file's contents."); *United States. v. Klynsma*, No. CR. 08-50145-RHB, 2009 WL 3147790, at *6 (D.S.D. Sept. 29, 2009) ("A SHA value of a computer file is, so far as science can ascertain presently, unique. No two computer files with different content have ever had the same SHA value."); *United States v. Schmidt*, No. 4:09CR00265 ERW, 2009 WL 2836460, at *10 (E.D. Mo. Aug. 27, 2009) ("The chances of a 'collision,' which is when two digital video files, with some significant difference in the video characteristics, share the same SHA1 value, are not mathematically significant.") (footnote omitted); *see also United States v. Cunningham*, 694 F.3d 372, 376 n.3 (3d Cir. 2012) ("Although it may be possible for two digital files to have hash values that collide, or overlap, it is unlikely that the values of two dissimilar images will do so.") (reversing trial conviction based on evidence error concerning child pornography video clips) (quoting *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011)).

F. Considering hash values in context

Context matters, particularly in considering hash values. For cryptography, military communications, and network and information security, the theoretical possibilities of a collision remain important. The possibility of any vulnerability must be determined and assessed.

However, for electronic evidence, the use of hash values concerns the review of data. This role for hash values is distinct from the security of communications or a network (the classic "apples vs.

oranges" distinction). Consequently, for electronic evidence, the remote improbability of a random hash collision is not material. Additionally, questions about the identity of any record can be considered in conjunction with other evidence. For example, the evidence will consist of much more than the mere confirmation of a match in hash values. Other circumstances such as the time and location of the file, corroborated with external information (witness interviews and events) will be considered. In this manner, hash values provide a powerful tool to confirm an event.

The judicial process has established avenues to assess the weight of the evidence. In the courtroom, the rules of evidence do not require that any other evidence satisfies the lofty standards provided under hash values (for example, 1 in more than 340 undecillion for the MD5 hash value). Hash value results substantially exceed the "prima facie" or "some evidence" standard to authenticate evidence in court. At trial, other time-tested avenues are available to assess the admissibility and weight of the electronic evidence based on hash values. All evidence is subject to the same scrutiny and process. A few examples of the use of hash values in these contexts are reviewed below.

Authentication—"prima facie" or "some evidence" threshold showing for admissibility: One legal context in using hash values concerns the authentication of electronic evidence. While hash values are not the only means to authenticate electronic evidence, they are generally an effective and proven way to do so.

Generally, a high standard is not required to establish the genuineness of particular evidence. Most courts apply a "prima facie" or "some evidence" standard to satisfy the threshold authentication requirement. *See, e.g.*, *United States v. Vidacak*, 553 F.3d 344, 349 (4th Cir. 2009) ("The burden to authenticate under Rule 901 is not high—only a *prima facie* showing is required."); *In re McLain*, 516 F.3d 301, 308 (5th Cir. 2008) ("[T]his Court does not require conclusive proof of authenticity before allowing the admission of disputed evidence [as] Rule 901 merely requires *some evidence* which is sufficient to support a finding that the evidence in question is what its proponent claims it to be.") (emphasis added) (quoting *United States v. Jimenez-Lopez*, 873 F.2d 769, 772 (5th Cir. 1989)); *United States v. Dhinsa*, 243 F.3d 635, 658–59 (2d Cir. 2001) (noting that "Rule 901 does not erect a particularly high hurdle" and that hurdle may be cleared by "circumstantial evidence") (citation omitted); *United States v. Holmquist*, 36 F.3d 154, 168 (1st Cir. 1994) ("[T]he burden of authentication does not require the proponent of the evidence to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood."); *United States v. Ortiz*, 966 F.2d 707, 716 (1st Cir. 1992) ("The rule does not erect a particularly high hurdle."); *United States v. Goichman*, 547 F.2d 778, 784 (3d Cir. 1976) ("[T]here need be only a *prima facie showing*, to the court, of authenticity, not a full argument on admissibility.") (emphasis added).

Initially, the trial court, serving as a gatekeeper, determines whether the evidence is admissible. *See generally* FED. R. EVID. 104. After a threshold showing of admissibility, the jury (or factfinder) ultimately decides the authenticity and weight of any evidence. *See, e.g.*, *United States v. Fluker*, 698 F.3d 988, 999 (7th Cir. 2012) ("Only a prima facie showing of genuineness is required; the task of deciding the evidence's true authenticity and probative value is left to the jury."); *United States v. Isiwele*, 635 F.3d 196, 200 (5th Cir. 2011) ("Once the proponent has made the requisite showing, the trial court should admit the exhibit . . . in spite of any issues the opponent has raised about flaws in the authentication. Such flaws go to the weight of the evidence instead of its admissibility.") (citation and internal quotation marks omitted); *Orr v. Bank of America*, 285 F.3d 764, 773 n.6 (9th Cir. 2002) ("Once the trial judge determines that there is prima facie evidence of genuineness, the evidence is admitted, and the trier of fact makes its own determination of the evidence's authenticity and weight."); *United States v. Caldwell*, 776 F.2d 989, 1002 (11th Cir. 1985) ("Once that prima facie showing has been made, the evidence should be admitted, although it remains for the trier of fact to appraise whether the proffered evidence is in fact what it purports to be.").

As already noted, hash values generally have a 99.99 percent probability of confirming a match. *See supra* Section III(C). Additionally, there is an incredibly improbable likelihood of a collision (at least 1 in 340 undecillion for an MD5 hash, and even more remote for a SHA-1 hash). *See supra* Section V. Consequently, evidence that is authenticated by hash values substantially surpasses the "prima facie" or "some evidence" showing or the low bar normally used to authenticate evidence. The jury is often allowed to consider evidence despite questions raised about flaws or defects in authentication or chain of custody. In the end, the jury determines the final weight given to the evidence.

Hash values provide one effective means to authenticate evidence at trial. In particular, authentication may be made by distinctive characteristics. The features of the record may include "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." FED. R. EVID. 901(b)(4). Hash values are one way to authenticate electronic evidence under this Rule. *See, e.g.*, *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 547 (D. Md. 2007) ("Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4)."). Any alternation in the record (such as adding or removing one character) would result in a different hash value, confirming that two records do not match. *United States v. Keith*, No. 11-10294-GAO, 2013 WL 5918524, at *1 (D. Mass. Nov. 5, 2013) (noting "any alteration of the file, including even a change of one or two pixels, would result in a different hash value" and "once a file has been 'hashed,' a suspected copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value").

Consequently, hash values provide a powerful and significant avenue to authenticate electronic evidence. If courts will authenticate physical evidence that may have defects in the chain of custody, certainly hash values with a greater degree of reliability may be admitted and subjected to the time-tested means of scrutinizing the evidence. Given the high level of accuracy of hash values, they readily exceed the authentication standards under Rule 901.

Distinguishing "possible" from "probable" alterations: For electronic evidence, the opposing party may argue that the evidence is subject to alteration. When it comes to electronic evidence, the courts have also demonstrated the ability to distinguish between probable or possible alterations. Remote possibilities have not posed a bar to admitting otherwise relevant evidence.

As with other forms of evidence, most electronic evidence can be modified. For example, an email can be readily modified. One district court explained the following in dismissing a challenge to admit emails on the bare claim that they are subject to possible alteration:

> The defendant argues that the trustworthiness of these e-mails cannot be demonstrated, particularly those e-mails that are embedded within e-mails as having been forwarded to or by others or as the previous e-mail to which a reply was sent. The Court rejects this as an argument against authentication of the e-mails. The defendant's argument is more appropriately directed to the weight the jury should give the evidence, not to its authenticity. While the defendant is correct that earlier e-mails that are included in a chain—either as ones that have been forwarded or to which another has replied—may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. Indeed, fraud trials frequently center on altered paper documentation, which, through the use of techniques such as photocopies, white-out, or wholesale forgery, easily can be altered. The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance

> in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done.

United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) (emphasis in original).

Courts have repeatedly rejected efforts to exclude otherwise admissible evidence on the grounds of some possible or theoretical claim that the evidence could be altered. *See, e.g.*, *id.* at 41; *see also United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) ("[A] reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable."); *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility.").

In the same vein, the extraordinarily remote theoretical possibility of a collision for hash values should not prevent relevant hash value evidence from being admitted. Generally, the jury, as the finder of fact, should hear all relevant evidence. Most importantly, as noted below, the judicial process has a variety of avenues to take when considering challenges to evidence.

Trial measures to test the evidence: Once evidence has been authenticated and admitted for the factfinder's consideration, there are a number of other issues to consider. When questions about the reliability of evidence have been raised, the Supreme Court has continually noted the ability of the judicial process to highlight any merits and deficiencies of the evidence. For example, with regard to expert testimony, the Court noted the following in a landmark ruling:

> [R]espondent seems to us to be overly pessimistic about the capabilities of the jury and of the adversary system generally. Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence. Additionally, in the event the trial court concludes that the scintilla of evidence presented supporting a position is insufficient to allow a reasonable juror to conclude that the position more likely than not is true, the court remains free to direct a judgment, Fed. Rule Civ. Proc. 50(a), and likewise to grant summary judgment, Fed. Rule Civ. Proc. 56. These conventional devices, rather than wholesale exclusion under an uncompromising "general acceptance" test, are the appropriate safeguards where the basis of scientific testimony meets the standards of Rule 702.

Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 596 (1993) (citations omitted).

More importantly, evidence at trial is rarely viewed in isolation, as the surrounding circumstances and facts are taken into account. The jury may consider whether any evidence is corroborated or makes sense in the context of all the other evidence, including any challenges to the weight of the evidence. These long-established judicial processes provide an adequate test to highlight the strengths and weaknesses of any evidence, whether it is a fingerprint, firearm, or electronic record.

Probable cause: Another important legal context concerns establishing probable cause to obtain a search warrant. Hash values may be useful in considering the totality of the circumstances to determine whether there is probable cause to search a particular place under the Fourth Amendment. As the Supreme Court explained, under this standard, the judge must "make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

One district court noted the following in denying a motion to suppress a search warrant in which hash values were used in an investigation to identify child pornography images:

> When considered in proper context however, the cited language merely establishes that use of SHA1 values provides an extremely high level of precision in identifying specific file content—a level of precision which, according to the affidavit, is more unique than DNA matching. Such precision likely exceeds the exactitude necessary to establish proof beyond a reasonable doubt; certainly, it exceeds what is necessary under general probable cause standards. Thus, the affidavit may be fairly read as implying a fairly obvious principle—that SHA1 values provide a more reliable means of identifying actual file content than is possible by virtue of file names alone. This principle, however, does not lead ineluctably to the conclusion that file names thereby always constitute meaningless information.

United States v. Beatty, No. 1:08-cr-51-SJM, 2009 WL 5220643, at *7 (W.D. Pa. Dec. 31, 2009), *aff'd*, 437 F. App'x 185, 186–88 (3d Cir. 2011) (affirming denial of motion to suppress and describing how files were matched using a SHA1 value to known child pornography files contained in a database maintained by the Wyoming Internet Crimes Against Children Task Force); *see also United States v. Bershchansky*, 958 F. Supp. 2d 354, 376 (E.D.N.Y. 2013) (on motion to suppress, rejecting defendant's "meritless" argument questioning the reliability of a SHA1 value match and explaining that "[a]s numerous courts have found, SHA1 values are sufficiently accurate as to form a reliable basis on which a court may find that there is probable cause to believe that contraband or evidence of a crime will be found in a particular place").

The final assessment of probable cause will be based on a totality of the circumstances. Hash values are typically considered along with other evidence obtained during the investigation.

VI. Conclusion

Hash values remain a valuable and powerful tool to identify electronic evidence in a reliable, effective, and efficient manner.

This article has surveyed the recent use of hash values for electronic evidence in investigations and cases. Hash values are somewhat akin to serial numbers that may be used to uniquely identify particular items such as a Vehicle Identification Number, firearm serial number, U.S. currency serial number, or device serial numbers. However, hash values—compared to these other examples—are stronger, more distinctive, and cannot be altered.

Hash values are commonly referred to as "digital fingerprints" or "digital DNA." The "fingerprinting" qualities have been noted by early developers of hash values, by recent cases, and by those in the legal community. However, the likelihood of a random match for hash values is significantly more remote than for either fingerprints or DNA. Generally, hash values produce a greater than 99 percent probability of a match between one file and a known file. In fact, the probability of a random match is *significantly* higher with DNA than it is for the MD5 or SHA-1 hash values.

This article considered the recent issue of a theoretical "collision" (the likelihood that two data sets will have the same hash value) and demonstrated that while this issue may be important for cryptography and other fields, it does not affect the use of hash values for forensic purposes. When the "collision" argument has been raised concerning the forensic use of hash values, courts have, so far, rejected it. Among several reasons noted, this remote possibility has yet to be observed in an actual case. Most importantly, the judicial process has effective avenues to consider and weigh the strength of any evidence, electronic or otherwise. As the Supreme Court noted, "Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence," among other steps. *Daubert v. Merrell*

Dow Pharm., Inc., 509 U.S. 579, 596 (1993) (citations omitted). These time-tested judicial processes can be effectively used to consider any challenges or issues concerning hash values in any case. Electronic evidence and hash values are scrutinized under the same judicial process that applies to all forms of evidence.

In the past, a number of improvements have been made to hash values. This trend will continue. While current tools may be updated or replaced, the hash value has proven to be an essential and invaluable tool for electronic evidence in investigations and cases. ❖

ABOUT THE AUTHORS

❑ **Ovie Carroll** is the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS). He has more than 28 years of experience in law enforcement. Mr. Carroll is an adjunct professor at George Washington University in the Masters of Forensic Science program, where he teaches Internet Investigations. He is also a certified SANS Instructor and co-author of SANS Forensic 408-Windows in Depth course. Prior to joining the Department of Justice, Mr. Carroll was the Special Agent in Charge of the Technical Crimes Unit at the United States Postal Service (USPS), Office of Inspector General (OIG), responsible for all computer intrusion investigations within the USPS network infrastructure and for providing all computer forensic analysis in support of OIG investigations and audits, as well as the deployment, installation, and monitoring of technical computer surveillance equipment in support of criminal investigations. Mr. Carroll was also a special agent with the Air Force Office of Special Investigations, where he led and assisted in the planning and conducting of computer intrusion investigations into Department of Defense networks and conducted investigations into a variety of offenses, including murder, fraud, bribery, theft, counterintelligence matters, and gangs and narcotics. Mr. Carroll regularly has instructed at the National Advocacy Center on electronic evidence and other forensic issues. ✠

❑ **Mark L. Krotoski**, a federal prosecutor since 1995, previously served as National Computer Hacking and Intellectual Property (CHIP) Program Coordinator at CCIPS in the Criminal Division for nearly four years, and as a CHIP prosecutor in the Northern and Eastern Districts of California for about eight years, among other positions. Mr. Krotoski has prosecuted a variety of cases and trials involving electronic evidence. He has regularly served as an instructor at the National Advocacy Center on electronic evidence and other issues. Presently, he is an Assistant Chief in the Antitrust Division. ✠

The views expressed in this article do not necessarily reflect those of the Department of Justice.

Snitches Get Stitches: Combating Witness Intimidation in Gang-Related Prosecutions

Linda A. Seabrook
Program Attorney
Indian, Violent and Cyber Crime Staff
Executive Office for United States Attorneys

Jelahn Stewart
Assistant United States Attorney
Chief of the Victim Witness Assistance Unit
District of Columbia

It plays out like an episode of Law & Order: a repeat, unfortunately. Gang members stand accused of assault, murder, and drug trafficking. A witness—an ex-girlfriend of a gang member or a member of the community plagued by gang violence finally takes a stand by taking the stand—a hero to many, an enemy to the gang. The snitch has to be silenced. The Bloods, the Crips, MS-13, and the remaining 33,000 gangs that the FBI identified as active in the United States today employ similar tactics of intimidation, harassment, and often violence to discourage or prevent witnesses from cooperating with the authorities. In fact, one of the mottos of the renowned gang, MS-13, is "kill, rape, and control," their modus operandi. *United States v. Machado-Erazo*, No. 10-256-08, 2013 WL 5434709, at *7 (D.D.C. Oct. 1, 2013).

Intimidation can either be community-specific or case-specific. Residents of communities located within gang territory know that cooperating with law enforcement places them at risk. In fact, many residents will not open their doors when police are investigating crimes in their neighborhoods out of fear that they will be identified as "snitches." In case-specific intimidation, looks or gestures in the courtroom, threats or assaults to a witness or the witness's family, damage to a witness's property, and murder are readily-used weapons in the gang's arsenal to protect one of their own. Loyalty among gang members is the ammunition—all for one, one for all. Witness intimidation, whether in the community or in a particular case, can prevent a case from going forward by depriving the prosecution of crucial evidence or a critical witness.

I. Pretrial strategies to combat witness intimidation

The Attorney General Guidelines for Victim and Witness Assistance directs Department of Justice (the Department) employees to "take reasonable measures to address the security concerns of witnesses." ATTORNEY GENERAL GUIDELINES FOR VICTIM AND WITNESS ASSISTANCE, art. VI, pt. B. 51 (2012). While "reasonable measures" may be a vague mandate, witnesses who agree to participate in the criminal justice process at great risk to the safety and well-being of themselves and their family should receive the benefit of the Department's available resources and assistance. Prosecutors should use great care to consider the risks to witnesses in gang-related cases and create a comprehensive plan to account for such risks.

A. Initial appearance

Witness intimidation can be direct or implicit. While it may be perpetrated by the defendant in gang-related prosecutions, often other gang members, as well as the defendant's family, may intimidate witnesses in the hopes of preventing the witness from testifying or from testifying truthfully. Therefore, it is important that prosecutors demonstrate from the initial appearance that the Government will aggressively combat witness intimidation, no matter the form and no matter the perpetrator. Detaining or significantly restricting the freedom of the defendant while on release reduces the opportunities for the defendant to intimidate or connect with cohorts to intimidate witnesses, thus enhancing witness security. In order to make the case for detention, prosecutors may want to ensure that the Pre-Trial Services Report or the court record details the defendant's gang affiliation, documenting all indicia that the defendant subscribes to the gang lifestyle, such as tattoos, social media postings, other gang-related arrests, monikers, wiretap admissions of gang membership, and known associates.

B. Engaging the witness

In order to foster witness participation and trust, prosecutors should make early contact with witnesses, encouraging witnesses to take an active role in their safety and security. Prosecutors or Victim-Witness personnel should recommend that the witness reduce visibility by taking actions, such as deleting or suspending social media accounts, altering routines, and avoiding areas associated with the crime or with a gang presence, whenever possible. Witnesses should also be provided with information about available Department resources to enhance their security, and with specifics regarding what conduct to report and to what agency or individual any reports of threats or harassment should be made. Any such threats or harassment should be taken seriously and aggressively prosecuted or used to argue for bond revocation and detention. Charges can be brought for witness tampering pursuant to 18 U.S.C. § 1512, witness retaliation under 18 U.S.C. § 1513, and prosecutors can obtain protective orders to restrain the harassment of a witness pursuant to 18 U.S.C. § 1514.

C. Witness security and discovery obligations

On January 4, 2010, then-Deputy Attorney General David Ogden issued several memoranda addressing discovery issues in criminal cases. While the memoranda directs Department prosecutors to provide broad and early discovery, the guidance clarifies that prosecutors should also be mindful of any "countervailing considerations," such as protecting witnesses from harassment and intimidation. *See* Memorandum from former Deputy Attorney General David Ogden to Department of Justice Prosecutors (Jan. 4, 2010), *available at* http://www.justice.gov/dag/discovery-guidance.html. Prosecutors should note that unless it is a capital case, defendants do not have a right, as a matter of course, to pretrial disclosure of the identity of the Government's witnesses. *See United States v. Lewis*, 594 F.3d 1270, 1280 (10th Cir. 2010); *United States v. Grace*, 526 F.3d 499, 508–13 (9th Cir. 2008) (en banc); *United States v. DeCoteau*, 186 F.3d 1008, 1009 n.2 (8th Cir. 1999); *United States v. White*, 116 F.3d 903, 918 (D.C. Cir. 1997); *see also* CRIMINAL DISCOVERY WORKING GROUP, DEP'T OF JUSTICE, FEDERAL CRIMINAL DISCOVERY 160–64 (2011). However, courts may compel disclosure of pretrial witness lists. In gang-related prosecutions, witness names, addresses, and other identifying information should be redacted from this discovery material prior to its production to the defense. Further, any disclosure of this information should be made subject to a protective order restraining the defense attorney from providing this information to anyone other than an investigator for the defense. Finally, delaying disclosure of any witness information until directly before trial can provide a measure of enhanced security for witnesses, curtailing the opportunities for intimidation and harassment.

II. Strategies to use during trial to address witness intimidation

Witness intimidation occurs in many venues, including right in the courthouse during the prosecution of the case. Government witnesses waiting in the courthouse to be called to testify have been threatened or harassed by the defendant's family or gang family. Prosecutors may use several different strategies to prevent such intimidation in the courthouse. In addition to being able to charge those who threaten government witnesses with witness tampering or retaliation, the prosecutor can ask the court to designate a separate waiting area specifically for prosecution victims and witnesses in the courthouse. In fact, federal law requires prosecutors to ensure that a victim-witness is provided a waiting area removed from, and out of the sight and hearing of, the defendant and defense witnesses. *See* 42 U.S.C. § 10607(c)(4) (2014). This strategy allows prosecution victim-witnesses to wait for their testimony in an area where they do not have to encounter the defendant or endure harassment by the defendant, his or her family members, or other gang members.

Unfortunately, there are times when the intimidation of witnesses occurs right inside the courtroom. This can happen when friends or relatives of the defendant sit in the courtroom during the trial and use threatening gestures, or give the government witness threatening looks in order to prevent the witness from testifying or from testifying truthfully. In gang cases, it is not uncommon for fellow gang members to attend court proceedings and attempt to intimidate witnesses through the use of threatening looks or intimidating hand signs. If prosecutors are made aware of this threatening behavior, the prosecutor can alert the court and seek the removal of those attempting to intimidate the witness.

Prosecutors should work with bailiffs, the court, and the marshals, to prevent and address intimidation within the courtroom. A useful strategy to hamper courtroom intimidation is to have the marshals or other court personnel to check the identification of anyone entering the courtroom. The marshals can then check for outstanding warrants, identify possible truants, or alert probation to the presence of those on supervised release. Another strategy prosecutors can use is to request that the court reserve the first row of seats in the courtroom for attorneys or police officers so that the witness may not have a clear view of anyone in the courtroom trying to intimidate the witness during the witness's testimony.

A. Closing the courtroom

If the prosecutor can provide evidence that an individual poses a danger to a witness or compromises the court's ability to elicit truthful testimony from the witness, the prosecutor can seek partial or complete closure of the courtroom or exclusion of specific individuals. Complete closure of the courtroom implicates a defendant's Sixth Amendment right to a public trial and is a rare occurrence. *See Pressley v. Georgia*, 558 U.S. 209, 213–14 (2010). Those seeking to close court proceedings over the objection of the accused must adhere to a strict test. *See Waller v. Georgia*, 467 U.S. 39, 45–46 (1984). Under this test "(1) the party seeking to close the hearing must advance an overriding interest that is likely to be prejudiced, (2) the closure must be no broader than necessary to protect that interest, (3) the trial court must consider reasonable alternatives to closing the proceeding, and (4) it must make findings adequate to support the closure." *Drummond v. Houk*, 728 F.3d 520, 527 (6th Cir. 2013) (citing *Waller*, 467 U.S. at 48); *see also* 28 C.F.R. § 50.9(c)(1)–(6) (2014) (listing several requirements a prosecutor must adhere to before moving to or consenting to closure of a proceeding). A strong presumption exists against closing proceedings, and prosecutors may not move for or consent to the closure of any criminal proceeding without the express prior authorization of the Deputy Attorney General. *See* 28 C.F.R. § 50.9 (2014); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-5.150 (2012). The presumption can be overcome, however, and closure can be permitted if the prosecutor can establish that failure to close the proceedings will produce "[a] substantial likelihood of imminent danger to the safety of parties, witnesses, or other persons[.]" 28 C.F.R. § 50.9(c)(6)(ii) (2014).

Partial or limited closure of the courtroom is more common and is subject to the lower "substantial reason" standard. *See United States v. Thompson*, 713 F.3d 388, 395 (8th Cir. 2013);

United States v. Addison, 708 F.3d 1181, 1184, 1187 (10th Cir. 2013) ("Where . . . there is only a partial closure of the trial, the defendant's right gives way if there is a 'substantial' reason for the partial closure."); *United States v. Cervantes*, 706 F.3d 603, 611–12 (5th Cir. 2013) ("Whereas the Supreme Court has enumerated a four-part test for determining whether closed proceedings are warranted, the requisite analysis varies when, as here, the challenged closure was partial rather than complete."). Ordering some individuals out of the courtroom because of the witness's fear of retaliation can be considered a partial closure of the courtroom. *See Thompson*, 713 F.32 at 396 ("The government's interest in protecting its witness and the witness's concern for his own safety justify the partial closing in this case."); *Addison*, 708 F.3d at 1187. (Witness intimidation alone was a substantial reason for excluding an individual from courtroom).

If prosecutors cannot partially or fully close the courtroom, there are other strategies to promote the security of witnesses during the course of the trial. For example, in *United States v. Ramos-Cruz*, 667 F.3d 487 (4th Cir. 2012), the Fourth Circuit upheld the district court's decision to allow two witnesses, El Salvadoran police officers, to testify under pseudonyms. *Id.* at 499–501. The prosecution moved for permission to have the police officers testify under aliases and without revealing any identifying information, due to concern for the officers' safety and the safety of their families. The Government submitted affidavits from the officers *in camera*, explaining the credible threat to their safety and the safety of their families as a result of their agreeing to testify against MS-13 gang members in a U.S. court, and provided a synopsis of the proposed testimony to the defense. The district court questioned the witnesses and determined that the Government had no disclosure obligations under *Giglio v. United States*, 405 U.S. 150, 154–55 (1972), and therefore allowed the witnesses to testify using pseudonyms and without revealing any identifying information. *Ramos-Cruz*, 667 F.3d at 492.

B. Forfeiture by Wrongdoing

No prosecutor ever wants to hear that his or her witness has been harmed, or even killed, as a result of the witness's participation in a prosecution. Unfortunately, in a small percentage of cases, witnesses are murdered or harmed so badly that they are unavailable to testify at trial. In such instances, prosecutors are not without recourse, and the trial is not necessarily doomed. If the prosecutor can establish, by a preponderance of the evidence, that the accused caused the witness's unavailability for trial in order to prevent the witness from attending or testifying in the trial, the prosecutor may be able to admit the statements made by the witness under a legal doctrine and hearsay exception known as Forfeiture by Wrongdoing. *See Giles v. California*, 554 U.S. 353, 367 (2008). Forfeiture by Wrongdoing can be a powerful tool for the prosecution because it allows admission of evidence that would typically be barred by the Confrontation Clause. As the name of the doctrine indicates, the accused actually forfeits his or her Sixth Amendment right to be confronted by witnesses against him or her, as well as any hearsay objection to the introduction of such evidence, if he or she "wrongfully procured the unavailability of that witness with the purpose of preventing the witness from testifying." *Zanders v. United States*, 999 A.2d 149, 155 (D.C. Cir. 2010) (citing *Giles*, 554 U.S at 360–61).

The Forfeiture by Wrongdoing doctrine was recognized in the common law as early as 1666, *see Giles*, 554 U.S at 359, but was used more frequently during the 1980s and 1990s when witness intimidation was on the rise in the United States. Courts across the country were routinely admitting unsworn, out-of-court statements offered against defendants when it could be shown that the defendants, or someone acting on his or her behalf, murdered or harmed witnesses to procure their unavailability at trial. *See United States v. Houlihan*, 92 F.3d 1271, 1279 (1st Cir. 1996); *United States v. Aguiar*, 975 F.2d 45, 47 (2d Cir. 1992); *United States v. Rouco*, 765 F.2d 983, 995 (11th Cir. 1985); *Steele v. Taylor*, 684 F.2d 1193, 1202 (6th Cir. 1982); *United States v. Balano*, 618 F.2d 624, 628 (10th Cir. 1979); *United States v. Carlson*, 547 F.2d 1346, 1360 (8th Cir. 1976). In *United States v. White*, 116 F.3d 903 (D.C. Cir. 1997), for example, the trial court allowed the Government to introduce unsworn incriminating

statements made by a police informant, who was murdered by a drug gang. The D.C. Circuit affirmed the admission of the statements, reasoning:

> It is hard to imagine a form of misconduct more extreme than the murder of a potential witness. Simple equity supports a forfeiture principle, as does a common sense attention to the need for fit incentives. The defendant who has removed an adverse witness is in a weak position to complain about losing the chance to cross-examine him. And where a defendant has silenced a witness through the use of threats, violence or murder, admission of the victim's prior statements at least partially offsets the perpetrator's rewards for his misconduct. We have no hesitation in finding, in league with all circuits to have considered the matter, that a defendant who wrongfully procures the absence of a witness or potential witness may not assert confrontation rights as to that witness.

Id. at 911.

On December 1, 1997, the common law Forfeiture by Wrongdoing doctrine was codified as an evidentiary hearsay exception, titled, "Statement Offered Against a Party That Wrongfully Caused the Declarant's Unavailability." The Rule prohibits the exclusion of an unavailable declarant's statement as hearsay if it is:

> [a] statement offered against a party that wrongfully caused--or acquiesced in wrongfully causing--the declarant's unavailability as a witness, and did so intending that result.

FED. R. EVID. 804(b)(6).

Forfeiture by Wrongdoing is an effective tool against a defendant who directly procures the unavailability of a government witness. In addition, a coconspirator can also cause the forfeiture of another defendant's confrontation rights, if the unavailability of the witness was rendered as part of the conspiracy and was reasonably foreseeable. *See United States v. Carson*, 455 F.3d 336, 363–65 (D.C. Cir. 2006). In *Carson*, the statements of a murdered witness, who had been part of the conspiracy, were admissible not only against the individual charged with murdering the witness, but also against other coconspirators. *Id.* at 365. The coconspirators challenged the Government's theory that a defendant could forfeit his confrontation rights based on the misconduct committed by a coconspirator. *Id.* at 362. The court made clear, however, that such statements could be used against coconspirators and ruled:

> [T]he reasons why a defendant forfeits his confrontation rights apply with equal force to a defendant whose coconspirators render the witness unavailable, so long as their misconduct was within the scope of the conspiracy and reasonably foreseeable to the defendant . . . .

Id. at 365.

Practically, evidence under the doctrine of Forfeiture by Wrongdoing can be introduced in a number of ways by prosecutors. In a recent case, *United States v. Pray*, No. 10-cr-51 (RMC), 2012 U.S. Dist. LEXIS 86294, at *1 (D.D.C. June 21, 2012), a government cooperator was killed after testifying in the grand jury and participating in a debriefing with prosecutors about the drug activities of the defendant. The witness was killed by a coconspirator, and the Government, after establishing that the killing was done to render the witness unavailable for trial and in furtherance of the conspiracy, was able to introduce the witness's grand jury testimony at trial. Additionally, the prosecutors with whom the government witness had debriefed were able to testify at trial about the conversations they had with the witness.

C. EWAP and WITSEC

There is no greater alarm for a prosecutor than receiving a call from a witness who has been threatened or harmed as a result of his or her participation in the prosecution of a case. Prosecutors often feel responsible for the safety of those victims and witnesses who are brave enough to come forward and

tell the truth about criminal activity. It is therefore essential to have tools in place for prosecutors to help ensure the safety and well-being of their victims and witnesses.

An important resource of use in combating witness intimidation is the Emergency Witness Assistance Program (EWAP), a program designed to provide relocation and other services to victims and witnesses who have fears about testifying or participating in prosecutions.

EWAP came into existence in the 1990s, a time when witness retaliation was at an all-time high. In fact, in the early 1990s, the District of Columbia, which led the nation in murders and was recognized as the "murder capital of the country," had an extremely high witness retaliation rate. Other U.S. cities claimed that title as well throughout the 1990s, primarily as a result of gang and drug-related violence. High witness retaliation rates meant that witnesses were threatened, assaulted, or even murdered, merely for their participation in prosecutions.

EWAP was instituted to provide resources for the immediate relocation of victims and witnesses who have concerns about their safety. The program is available to victims and witnesses who are participating in a pending prosecution or investigation, if the victims or witnesses have been threatened or perceive that they are in danger as a result of their participation in the prosecution. The program is also available to their family members, if necessary. EWAP can be used to provide assistance with both emergency and permanent relocations. Emergency relocation assistance can include the costs of transportation to a safe location and emergency lodging, temporary placement with a friend, relative, or emergency placement in a hotel. Permanent relocation assistance can include assistance with securing a Section 8 voucher or a public housing transfer, moving expenses, and expenses associated with moving, such as security deposits and utility activation fees. In addition, EWAP can be used to assist with security measures for making homes more secure, such as installing alarm systems or window locks. While EWAP services are intended as short-term emergency services for victims and witnesses, EWAP can be a useful resource in providing immediate services to address the fears of victims and witnesses who are involved in the prosecution.

Another important resource to address the security concerns of witnesses is the Federal Witness Security Program (WITSEC), often referred to as the Federal Witness Protection Program. WITSEC, which is administered by the Office of Enforcement Operations (OEO) within the Department and operated by the U.S. Marshals Service, "provides for the security, safety and health of government witnesses and their authorized family members, whose lives are in danger as a result of their cooperation with the U.S. government." OFFICE OF PUBLIC AFFAIRS, DEP'T OF JUSTICE, U.S. MARSHALS SERVICE FACT SHEET: WITNESS SECURITY 1 (2014). This long-term witness relocation program was created by the Organized Crime Control Act of 1970 and was revised by the Witness Security Reform Act of 1984. *See* 18 U.S.C. §§ 3521–3528 (2014). WITSEC is typically used in the most serious cases, including federal organized crime and racketeering offenses, federal drug trafficking offenses, and other serious violent crimes. *See id.* § 3521(a).

Designed to protect endangered witnesses before, during, and after trial, WITSEC provides 24-hour protection to all witnesses while they are in dangerous environments. OFFICE OF PUBLIC AFFAIRS, DEP'T OF JUSTICE, U.S. MARSHALS SERVICE FACT SHEET: WITNESS SECURITY 1 (2014). Witnesses and their family members are typically assigned new identities with authentic documentation, and are permanently relocated for their safety. Witnesses are provided with housing, transportation, subsistence for basic living expenses, and assistance with obtaining employment. *See* 18 U.S.C. § 3521(b)(1) (2014). OEO determines whether witnesses will be admitted to WITSEC. Some of the factors considered in assessing the suitability of a witness for the program include the witness's criminal history, psychological evaluation, and the seriousness of the investigation or case in which the witness participates. *See id.* § 3521(c). The possible risk of danger to the community where the witness is to be relocated is another important consideration. *Id.*

WITSEC has very strict rules for its participants. For example, Program participants are prohibited from returning to the neighborhood where the criminal activity took place, and are similarly prohibited from disclosing any facts regarding their protection. *See id.* § 3521(d)(1)(C). Although the rules are strict, no WITSEC participant who followed the security guidelines has been harmed while under the active protection of the U.S. Marshals. OFFICE OF PUBLIC AFFAIRS, DEP'T OF JUSTICE, U.S. MARSHALS SERVICE FACT SHEET: WITNESS SECURITY 1 (2014). The U.S. Marshals have protected, relocated, and given new identities to more than 8,500 witnesses and 9,900 of their family members since the program began in 1971. OFFICE OF PUBLIC AFFAIRS, DEP'T OF JUSTICE, U.S. MARSHALS SERVICE FACT SHEET: FACTS AND FIGURES 2 (2014).

III. Conclusion

Witness intimidation presents a significant stumbling block to the successful prosecution of gang-related cases and to the fair administration of justice. Prosecutors trying a gang-related case should expect that witness intimidation will be a factor and should prepare their case to account for this reality from the outset. Familiarity with the resources and strategies available to address and foster witness security is the prosecutor's best weapon to combat witness intimidation and promote the successful prosecution of gang-related crime. ❖

ABOUT THE AUTHORS

❑ **Linda A. Seabrook** is the Program Attorney for the Indian, Violent and Cyber Crime Staff (IVCC) of the Executive Office for U.S. Attorneys. In this role, she provides project-based assistance and support for the IVCC program areas. Prior to joining the Department of Justice, Linda was a *Project Ceasefire* prosecutor on a cooperative gun and drug task force in Charleston, South Carolina. ✠

❑ **Jelahn Stewart** is an Assistant U.S. Attorney and Chief of the Victim Witness Assistance Unit in the U.S. Attorney's Office for the District of Columbia. As Chief, Ms. Stewart manages the largest prosecution-based victim assistance program in the federal system and coordinates services for victims of, and witnesses to, crime in cases before the District of Columbia and the Superior Court for the District of Columbia. In her role as Chief, Ms. Stewart also oversees the Witness Security Section of the Unit, which processes hundreds of witness security requests each year. ✠

Developing a Step-by-Step Application of the New Orleans Strategy to Combat Violent Street Crews in a Focused Deterrence Strategy

K. Tate Chambers
OCDETF Lead Task Force Attorney
Central District of Illinois

Peoria was experiencing a surge in violent crime. Street crews had divided up the city into territories and were protecting their turf and drug trade with gun violence. As the shootings, retaliation shootings, and further retaliation shootings mounted along with the drive-bys, house shootings, and numbers of dead and wounded, the community searched for an answer. A team, led by the mayor and including the sheriff, the police chief, the State's Attorney, the U.S. Attorney's Office (USAO) for the Central District of Illinois, and community leaders, came together and chose the focused deterrence strategies designed by David Kennedy of John Jay College in New York City to attack the problem. Modeling their efforts after those outlined in Kennedy's book, Don't Shoot, One Man, A Street Fellowship, and the End of Violence in Inner-City America, the team designed and implemented a comprehensive and aggressive focused deterrence strategy to address Peoria's gang gun violence.

Don't Shoot Peoria started with an intense public education and awareness program. Kennedy's book, Don't Shoot, was chosen as the Peoria Reads book for that year. Hundreds of copies of the book were distributed throughout the community and the schools. As the community read Don't Shoot, the Don't Shoot Peoria team hosted a series of four radio shows where they discussed portions of the book and interviewed local and national guests about the focused deterrence strategy. David Kennedy traveled to Peoria and made a series of public appearances, answering questions about the strategy and how it would be implemented in Peoria. The mayor and his team also hosted a series of community forums and roundtables where members of the community could meet and discuss the violence problems and the focused deterrence strategy. Assistant U.S. Attorney (AUSA) Rob Lang—the father of one of the most successful and longest running focused deterrence strategies in the nation in High Point, North Carolina—came to Peoria, spoke to the community, and mentored the Don't Shoot Peoria team.

Don't Shoot Peoria billboards and bus stop signs were placed all over Peoria. A Web site, http://www.dontshootpeoria.com/, was put in place. Jim Lewis, the U.S. Attorney, hosted a state-wide conference to explore ways to fight the violence created by street crews. Don't Shoot Peoria partnered with existing pre-entry diversion and re-entry programs in the city. Members of the team designed and implemented focused deterrence strategies in the middle and high schools.

Nevertheless, as the team moved forward with the implementation of the focused deterrence strategy, one deficiency became obvious. One of the basic elements of focused deterrence is that during a "call-in," gang members are given the option of putting down their guns and stopping the violence or facing swift, severe, and certain consequences. If after being given the option, a gang member shoots, the strategy calls for a comprehensive law enforcement response against all of the members of that gang. The required response from the Peoria police and sheriff's departments was clear: increased, constant enforcement that would result in numerous state charges. The local and state response was well-planned in the strategy. But what was the swift, certain, and severe federal law enforcement response? Any federal

response to address the street crew as a whole was likely to use conspiracy theories. But developing a conspiracy case from scratch leading to a RICO or CCE charge usually takes a long time—several months at least. And that negated the threat of a swift sanction for gang gun violence promised when the gang members were called in and warned to put down their guns. What was needed was a federal response that addressed the leaders and shooters of the gang, contained severe potential penalties, and, at the very longest, took no more than 90 days (preferably 40 days) to indict. Nothing in the federal toolbox appeared to fit the bill until the team turned to a strategy developed by the USAO in New Orleans and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

This article will address that strategy, now known as the New Orleans Strategy, and how it was employed in Don't Shoot Peoria's focused deterrence game plan. This article will outline the fourteen steps developed by Don't Shoot Peoria to implement the strategy and discuss some of the practical applications of those steps.

I. The New Orleans Strategy

In the 2000s, New Orleans had one of the highest per capita murder rates of any major city in America. The state and local criminal justice system was overburdened, and the system was clogged. To address the problems created by the violence, the men and women of the USAO in New Orleans and the ATF developed what is now known as the New Orleans Strategy for addressing violent crime by street gangs or crews. The effort was spearheaded by ATF Special Agent Michael Eberhardt and AUSA Maurice Landrieu. It is their work that serves as the basis for the following summary.

The New Orleans strategy is a historical conspiracy approach to combating street gang violence. It is based on the belief that most members of violent street gangs have committed criminal acts in their past and that these actions have the potential to be charged today. The goals of the strategy are to learn what those acts are and to produce the evidence necessary to charge them either as stand-alone substantive charges or as overt acts of a RICO conspiracy or a drug conspiracy.

The strategy is premised on the conspiracy theory that street gang members (1) control a specific area, (2) maintain the right to deal drugs and commit other crimes in that area, (3) use violence to maintain control of that area, and (4) those actions are overt acts of a conspiracy between the members of the gang. Every act committed in furtherance of the agreement becomes an overt act of the conspiracy between the members. Focusing on gang members' existing criminal exposure, the New Orleans strategy looks for those past crimes where (1) all of the elements necessary to constitute the criminal violation are complete, (2) no additional act of the part on the perpetrator is necessary, and (3) the perpetrator cannot undo or cause the violation to be incomplete.

The New Orleans strategy is driven by the witnesses and the existing physical evidence that corroborates them. The emphasis is on locating existing evidence such as ballistic evidence and DNA, and not on creating new pro-active evidence through TIIIs, surveillance, drug buys, search warrants, or the use of confidential sources or undercover operations. The New Orleans strategy is premised on the belief that a suspect can derail a proactive investigation by moving from the area or changing his behavior, but he cannot thwart an investigation using the New Orleans strategy because the evidence already exists. The existing criminal exposure is independent of present day actions by the suspect and is only limited by the investigators' resources and the statute of limitations. Special Agent Eberhardt coined the phrases "target independent" and "target dependent" to illustrate the difference between the New Orleans strategy and the standard proactive investigative techniques. Proactive techniques are "target dependent." The target can impact their success. Evidence of crimes already committed is "target independent." The evidence already exists, and the target cannot change it.

To implement the New Orleans strategy, the law enforcement team comes together to form a working team. Investigators and prosecutors work together from the beginning. Next, the team researches

and pulls all of the police reports for violent crime in a given target area. Crime mapping is an essential part of this step. Reviewing these reports helps identify potential targets, charges, and witnesses. The investigation at this early stage casts a wide net and narrows it as the investigation progresses. Once the target list is established, each target's criminal history is researched for potential new charges and evidence that can be used in the RICO conspiracy.

The team then looks for witnesses to the target's crimes. Finding witnesses in the historical case relies on the common sources, such as victims, victims' family members, rival drug dealers, drug addicts, former gang members, and jailhouse informants.

After the target list is established, the police events are determined, and the witnesses identified, the prosecutor begins the grand jury investigation. The witnesses are brought to the grand jury as soon as possible to establish their testimony. Without wasting the grand jury's time, anyone who may have usable information is brought before the grand jury and every witness is examined carefully about all aspects of the street crew's violence and drug business. In order to conduct this type of aggressive grand jury work it is important that the AUSA be involved in the investigation from the beginning and be as familiar with the facts of the case as the agents.

Again, the goal of the New Orleans Strategy is to produce, at the most, a chargeable RICO, CCE, or drug conspiracy case and, at the least, chargeable stand-alone substantive crimes such as 18 U.S.C. §§ 922(g) and 924(c). AUSA Landrieu emphasized that conspiracy charges are preferred because they (1) allow for the prosecution of multiple defendants in one case, (2) allow for the introduction of evidence of multiple crimes over an extended period of time, (3) result in convictions with substantial sentences, and (4) promote the development of intelligence from cooperating defendants to use in the next case.

The New Orleans strategy was successful. After the USAO and ATF implemented the strategy, they began to see results. Violent street crews were prosecuted using its techniques. Violent crime went down in the areas where those crews once controlled.

II. Don't Shoot Peoria—the 14-step application of the New Orleans Strategy

When members of the Don't Shoot Peoria team looked for a law enforcement strategy to bring their federal resources to bear against street gangs that failed to put down their guns, they were looking not only for a severe and certain consequence, but also a strategy they could implement in a short time—two to three months. They also wanted a strategy they could standardize because many of the law enforcement resources that were part of the Don't Shoot team were state and local officers who were not familiar with federal conspiracy investigations. They wanted a strategy that would, in short, order produce a prosecutable federal conspiracy case against the leaders and the most violent members of the offending street crew and that could be replicated time and time again against other street crews. To achieve those goals, they took the New Orleans Strategy and developed a 14-step method to implement the strategy in Peoria.

A. Step 1: Identify the target group—who shot?

The first step is to identify which group shot. Who committed the act of violence that is being sanctioned? Many of today's violent street crews are not like the street gangs of the past. There is no hierarchical structure. There is no role differentiation. There are no regular meetings, dues, or written rules. The chain of command is not as rigorous and changes frequently, depending on who is in jail and what type of crimes the crew is committing. But today's crews still think as a group. They claim ownership of a specific geographical area. They commit crimes in that area. They maintain the exclusive right to sell drugs in that area. They use violence to protect that area. They use violence to protect each other. In their social media and with their tattoos, they identify to the crew. In sum, they act and think as a group. Consequently, they can be investigated and prosecuted as a group. But, even with that said, they

often are split into several factions and each faction operates as a separate group within the larger group. Under the focused deterrence strategy, it is important to sanction the actual group that committed the violence. If other subgroups of the larger crew have put down their guns and stopped shooting, it sends the wrong message to punish everyone in the larger group. That is why it is important to identify the actual group that shot and that is being targeted for sanctions.

B. Step 2: Identify the members of the target group

Once the targeted group is selected, the next step is to identify the members of that target group. Police gang intelligence and criminal history information are good sources for this information. Jail and prison records and social media are also often helpful in identifying the members of a specific crew.

C. Step 3: First cut—select the crew leaders and the most violent members

Once the members of the targeted group are identified, it is time to make the first cut. Depending on the size of the crew, it may be necessary to focus on the crew leaders and the most violent members of the crew. The strategy requires that at this point the team cast a wide net, but that the net be manageable. Trying to work with dozens of names will make the next steps in the process overly burdensome and time-consuming. Police intelligence can help identify the crew leaders and most violent members. It is also important at this step to focus on the date of birth of the members. It is not unusual to learn that several members of the crew have not reached the age of federal majority or that their crimes were committed when they were minors.

D. Step 4: Run criminal histories on first cut targets

Next, run complete criminal histories on the first cut targets. This task is one of the most important steps in the process. Failure to do it correctly will result in numerous problems analyzing the case in the steps to come. The agents should run the criminal histories and then summarize them in the following format:

1. Date of conviction
2. Court number
3. Jurisdiction of conviction
4. Crime of conviction
5. Sentence received

First, a complete criminal history is essential for determining whether a target has the priors for Armed Career Offender, Felon in Possession, 851 enhancements for prior felony drug convictions, or Career Offender status. The date of conviction is very important because, among other reasons, it determines which overt acts were committed by the targets after they became adults. The court number is important because, with a large number of prior convictions, it will allow the investigators to track the convictions and identify them by number. The actual crime of conviction is also important. Many times a defendant will be charged with a much more serious charge, such as drug distribution, but will plead down to a less serious charge, such as possession. The sentence the defendant received is important to establish when he was out of custody and available to commit overt acts of the conspiracy. Taking the time to carefully pull the entire criminal history and place it into the proper format will prevent numerous problems as the investigation proceeds.

E. Step 5: Pull all police incidents for first cut targets

Pull every police incident involving the first cut targets, whether they are listed as suspects, witnesses, or victims. No exceptions. It is important to remember to run all of the indices from the federal

agencies, other state and local agencies, as well as from the principal police agencies files. There is no limit on the types of incidents that should be pulled. Convictions, acquittals, dismissals, no charges—they all should be pulled. Next, the agents should prepare a one-line summary of each incident, including the date of the incident, the police report number, and a characterization of the incident, such as car stop, search warrant, etc. They should also indicate which of the first cut targets are named in the reports. The summaries should then be placed in chronological order and charted on a spreadsheet.

F. Step 6: Collect talker interviews and identify additional potential talkers

The next step is to ask all law enforcement agencies (federal, state, and local) to run their indices and provide all reports of interviews where the talker mentions one of the first cut targets or discusses the targeted group. A thumbnail summary of what each talker provides should be written and organized by target. Remember to mine all of the common sources for talkers, such as former group members, rival group members, ex-wives and girlfriends, cell mates, and current group members serving time.

G. Step 7: Second cut—select crew leaders and most violent members

Bring the team together again and, using the summaries of criminal histories, the police incident spreadsheets, and the talker summaries, select the most active leaders and the most dangerous members of the targeted group from the original first cut list. As you tighten the net, remember that there will be yet a third opportunity to tighten it more, so the agents should err on the side of including additional targets at this stage. However, because the next few steps are very labor intensive, it is important to reduce the second cut to a manageable number of names.

H. Step 8: Prepare affidavit quality summary of police incidents for second cut targets

Now that the team has a list of second cut targets, it is time to go back to the police incident list and select every incident that (1) involves one of the second cut targets, and (2) shows either criminal activity or a relationship between the targets and the street crew. For example, a car stop where four members of the crew, including one of the second cut targets, are found with one pistol in the car should be included. A barking dog call at a second cut target's home should not be included. Once the incidents are selected, the agents should prepare an affidavit quality summary of each incident. That means answering the questions they would have to answer for a criminal complaint affidavit. Examples of questions to be answered include: Are the witnesses still alive? Has the physical evidence been destroyed? Are the squad car tapes still in existence? These summaries will serve as the basis for any later prosecution memorandum and will be used to charge stand-alone substantive counts and establish overt acts of any charged conspiracy.

I. Step 9: Do grand jury work on second cut targets

The ability to conduct extensive grand jury work on an investigation is one of the benefits of federal prosecution. That is especially true in executing the New Orleans Strategy. The prosecutor and investigators must be willing to spend the hours necessary to develop the witnesses, prepare them for the grand jury, and commit them to their testimony before the grand jury. Often, these witnesses are very difficult. Many times, they are not cooperative. It is common that they fear for their lives if they cooperate against the crew. But, it is essential that the team spend the time and effort necessary to conduct an aggressive grand jury investigation.

J. Step 10: Pull social media on second cut targets

While the prosecutor and agents are working the grand jury investigation, other agents should be assigned to collect corroborative evidence. One of the most valuable sources of such evidence against

street crews is their social media postings. Photos and videos of the street crew members together throwing gang signs while holding large amounts of cash and brandishing weapons and threatening rival gang members is solid evidence for the conspiracy charge. If a social media search under the gang members does not bear fruit, consider looking at their girlfriends' social media. They are often sources for equally damning evidence.

K. Step 11: Pull jail tapes and visits on second cut targets

The vast majority of crew members served time in the county jail prior to being investigated by the Don't Shoot Peoria team. Those stays can produce a wealth of incriminating jail tapes. One of the drawbacks to reviewing jail tapes is that it is so time-consuming. That is one reason why it is so important to bring down the number of targets to a manageable number in the second cut. Jail visitor logs also provide a valuable source of information about associates and persons who may become witnesses against the crew member.

L. Step 12: Do phone records—phones and tolls

Again, just as the jail information is important, the team should not overlook information obtained from seized phones in prior cases and tolls gathered in those cases or by grand jury subpoena in the present investigation.

M. Step 13: Bring team together to do final third cut

Bring the team together one more time to review the criminal histories of the targets, the affidavit quality summaries of the police incidents, the grand jury testimony of the talkers, the social media, jail, and phone evidence, and to make the third and final cut. Because this is the final cut, it is necessary to funnel down the focus to a manageable number. In Don't Shoot Peoria, the team decided that that number was between 12 and 15. It will differ city by city, depending on the capability of the team and the size of the crew. Those that do not make the final cut can be placed on a "waiting list" for subsequent indictments.

N. Step 14: Indict third cut targets

Don't Shoot Peoria has executed the New Orleans Strategy twice. Each time it used the same indictment format—Count one, membership in a street gang in violation of 18 U.S.C. § 521; Count two, conspiracy to commit § 924(c) violations in violation of § 924(o); Count three, conspiracy to distribute controlled substances in violation of 21 U.S.C. § 846; and numerous substantive 18 U.S.C. §§ 922(g), 924(c), and 21 U.S.C. § 841 charges. The indictment against the first street crew took over four months from shooting to indictment. The indictment against the second crew took a little under three months from murder to indictment. The goal is to be able to indict within 40 days from the date of the triggering shooting incident.

While it is too early to declare victory or assign reasons for success since implementing Don't Shoot Peoria and the New Orleans Strategy, police statistics show that violent crime in Peoria is down, fewer people are being shot, fewer shots are being fired, armed robbery is down, aggravated discharge of a firearm is down, and reckless discharge of a firearm is down. The results are promising.

III. Conclusion

A successful focused deterrence strategy relies on a severe, certain, and swift sanction when gang members refuse to put down their guns and continue to wreck violence on the community. Because gangs act and think as groups, the most effective way to address them in the federal system is through

conspiracy charges. The New Orleans Strategy, as implemented in Don't Shoot Peoria's 14-step plan, appears to provide that conspiracy-based severe, certain, and—most importantly—swift sanction.❖

ABOUT THE AUTHOR

❑**K. Tate Chambers** has been an Assistant U.S. Attorney in the Central District of Illinois for 30 years, where he has served in numerous capacities including Appellate Chief, Peoria Branch Chief, Outreach Coordinator, and PSN coordinator. He is currently serving as the Lead OCDETF Task Force Attorney and Violent Crime Coordinator. From 2007 to 2009, he served at Main Justice as the PSN National Coordinator. Mr. Chambers served on the Evaluation and Review Staff in Washington, D.C. as Criminal Program Manager from 2009 to 2010. He is retired from the Illinois Army National Guard where he served in the Judge Advocate General Corp. ✠

The author wishes to sincerely thank the men and women of the ATF and USAO offices in New Orleans, especially ATF Special Agent Michael Eberhardt and AUSA Maurice Landrieu, for their work designing and implementing the New Orleans Strategy and mentoring the rest of the team in its use.

Reentry Efforts and Gangs: Project GRIP

David L. Smith
Counsel for Legal Initiatives
Office of the Director
Executive Office for United States Attorneys

Gretchen C. F. Shappert
Assistant Director
Indian, Violent & Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

Investigation, prosecution, and incarceration are not the only challenges the Department of Justice must address in responding to America's gang problem. The Attorney General's Smart on Crime Strategy, issued in August 2013, makes clear that "recidivism rates are high" and advises the U.S. Attorneys to focus on reentry efforts as part of their strategy to create safer communities. *See* DEP'T OF JUSTICE, SMART ON CRIME: REFORMING THE CRIMINAL JUSTICE SYSTEM FOR THE 21ST CENTURY 5 (2013). But are gang members and gang-associated individuals realistic candidates for successful reentry efforts? One unique reentry program in the Eastern District of Missouri, the Gang Reentry Initiative Program (GRIP), is making a sustained and important effort to answer that question.

I. Introduction

There is a pressing need to reduce recidivism by gang members nationally. According to the FBI's 2011 National Gang Threat Assessment, there has been an overall increase in gang membership across the United States in recent years. Gangs are responsible for approximately 48 percent of violent

crime in most jurisdictions and up to 90 percent in others, according to a National Gang Intelligence Center analysis. NAT'L GANG INTELLIGENCE CTR., FED. BUREAU OF INVESTIGATION, 2011 NATIONAL GANG THREAT ASSESSMENT—EMERGING TRENDS 9 (2011), *available at* http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment (National Gang Threat Assessment). Academic research confirms that gang members engage in more delinquent and violent behaviors than non-gang youth, and joining a gang facilitates greater adherence to street code-related behaviors, attitudes, and emotions. Kristy N. Matsuda, Chris Melde, Terrance J. Taylor, Adrienne Freng & Finn-Aage Esbensen, *Gang Membership and Adherence to the "Code of the Street"*, JUSTICE QUARTERLY, May 18, 2012, at 1–2. It is axiomatic that active gang members in many urban gangs have significant criminal histories and that gangs can include extraordinarily violent individuals who have committed multiple crimes.

Research shows that reentry efforts are best directed toward those who have a high risk of committing new crimes upon release. Allocating time and treatment on lower risk participants wastes scarce resources. *See* EDWARD LATESSA, WHAT SCIENCE SAYS ABOUT DESIGNING EFFECTIVE PRISONER REENTRY PROGRAMS14–15, *reprinted in* LOOKING BEYOND THE PRISON GATE: NEW DIRECTIONS IN PRISONER REENTRY 13, 13–19 (Heidi Normandin & Karen Bogenschneider eds., 1st ed. 2008). Indeed, reentry programs targeted at low risk offenders actually hinders their progress. *See id.* at 15. Certainly gang members fit the "high risk of recidivism" criteria, but there is more going on with most gang members that can make their participation in reentry programs difficult and uncertain.

First, it has long been understood that gangs form a kind of substitute family for individuals who have lost the positive social structures that are needed to help form a person into a responsible citizen. Gangs represent a "type of street social control institution by becoming in turn a partial substitute for family . . . school . . . and police . . . ." JAMES DIEGO VIGIL, BARRIO GANGS, STREET LIFE AND IDENTITY IN SOUTHERN CALIFORNIA (1988), *reprinted in* JODY MILLER ET AL., THE MODERN GANG READER 29 (Oxford University Press ed., 2d ed. 2001). These deeply ingrained, familial-like bonds are hard to break.

Second, reentry is particularly difficult for gang members because many gang members continue to engage in gang activity while incarcerated. Some actually increase their gang adherence while in prison. *See* NAT'L GANG INTELLIGENCE CTR., FED. BUREAU OF INVESTIGATION, 2011 NATIONAL GANG THREAT ASSESSMENT—EMERGING TRENDS 3–4 (2011), *available at* http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment. Indeed, the National Gang Threat Assessment opines that gang membership nationally has increased in part as a result of "the release of incarcerated gang members from prison." *Id.* at 9.

Finally, in spite of the growing interest in reentry initiatives, there is a paucity of research and evaluation of gang-specific reentry and prevention programs. *See generally* Finn-Aage Esbensen, Dana Peterson, Terrance J. Taylor & D. Wayne Osgood, *Results from a Multi-Site Evaluation of the G.R.E.A.T Program*, JUSTICE QUARTERLY, Aug. 15, 2011, at 128; NATIONAL INSTITUTE OF JUSTICE, *available at* http://www.nij.gov/topics/corrections/reentry/pages/welcome.aspx (2014) (providing an overview of the National Institute of Justice's Reentry Research Portfolio). *See also* EDMUND F. MCGARRELL, NICHOLAS CORSARO, CHRIS MELDE, NATALIE HIPPLE, JENNIFER COBBINA, TIMOTHY BYNUM & HEATHER PEREZ, AN ASSESSMENT OF THE COMPREHENSIVE ANTI-GANG INITIATIVE: EXECUTIVE SUMMARY 1 (2013), *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/240758.pdf. Therefore, developing suitable reentry programs for gang members and gang-associated individuals is an ongoing process that poses unique challenges for the Department of Justice and federal probation officers.

II. Project GRIP: The Eastern District of Missouri's Gang Reentry Initiative Program

A. Background of Project GRIP

Like most districts, the Eastern District of Missouri (EDMO) has experienced a growth in gang-related crime in recent years. According to U.S. Probation Officer (USPO) Michael P. Nicholson II, most of the gangs in EDMO consist of street gangs with Blood, Crip, Gangster Disciples, and Vice Lords affiliations. There are also small numbers of Eastern European, Somalian, Haitian, and Vietnamese gang elements. Although EDMO's probation revocation rate is better than the national average, representatives from the federal court, U.S. Probation, the U.S. Attorney's Office, and the Federal Defender's Office believed that the growing number of gang members completing federal sentences and being placed on supervised release required a more individualized approach to the challenges of reentry for former gang members. Enabling returning offenders to resist the temptations of their former gang lifestyles and to successfully reintegrate into their communities is the focus of Project GRIP.

Project GRIP began in March 2010 under the leadership of Doug Burris, the Chief USPO in EDMO. Modeled in part after the district's successful drug reentry court, Project GRIP offers a unique approach to the reentry challenges of former gang members. According to USPO Nicholson, Project GRIP was created in response to an obvious need. Former gang members who were serving probationary sentences or terms of supervised release were failing to complete their terms of supervision at astonishingly high rates. Chaotic personal histories and drug abuse were certainly part of the problem, but the issues went deeper. Nicholson, a 10-year veteran of the St. Louis Metropolitan Police Department and former detective, states that the one quality he observes in many former gang members is undiagnosed trauma. Gang members have experienced lifetimes of "unofficial wars." "They fight in jail and they fight outside of jail. It's the only life many of them have ever known," said Nicholson. Telephone Interview with Michael P. Nicholson II, U.S. Probation Officer, Eastern District of Missouri (Feb. 18, 2014). Creating a reentry program capable of addressing deep-seated needs required a heightened level of commitment from all components of the EDMO criminal justice system.

U.S. District Court Judge Henry Edward Autrey, one of the original founders of Project GRIP and the judicial representative on the GRIP Team, agrees with Nicholson's assessment that gang members are different from the participants in the district's drug court program. "Gang members are different from mainstream society. They spend their entire lives looking over their shoulder. Their lives have been traumatized by street violence, as if they have been in a war. Virtually all of the participants seem to be suffering from post-traumatic stress disorder. Their lives have been war-like. And it's difficult to move forward when you have a big cloud hanging over your head." Telephone Interview with Henry Edward Autrey, U.S. District Court Judge, Eastern District of Missouri (Feb. 19, 2014). "We are learning as we go along," he said. *Id.* "Those of us on the GRIP Team use our own experiences, while borrowing from other fields and disciplines, such as psychology." *Id.*

Project GRIP is expressly designed for individuals on supervised release or probation with a history of gang association. Participation is voluntary, and all individuals must agree to abide by the rules of the program, including regularly scheduled court appearances, where participants report on their progress. Each participant signs an agreement upon entry into the program, and program participation becomes a condition of supervised release. Failure to comply with program conditions may result in termination from the program and additional consequences, including possible revocation of supervision. U.S. PROBATION OFFICE, EASTERN DISTRICT OF MISSOURI, PROJECT GRIP SUMMARY 1 (2013) (SUMMARY).

Selection for Project GRIP participation requires, among other things, that the candidate: (1) be a documented/validated gang member or a member of a security threat group and admit gang membership, (2) have arrests and/or convictions for crimes of violence, such as murder, manslaughter,

serious assaults, and firearm-related crimes, (3) have a "risk prediction index" (RPI)—that is, a BOP assessment of likelihood to commit another crime after release—of seven to nine, with nine being the highest possible score, and (4) a general history of substance abuse, although offenders with current, serious substance abuse issues are not eligible. *Id.* at 2, 4–5.

According to USPO Nicholson, Project GRIP is unique. "Gang members rely on the gang to provide structure and support in their lives. Our goal is to replace the gang structure with a different set of values. The program facilitates a transition to a more law-abiding lifestyle." Telephone Interview with Michael P. Nicholson II, U.S. Probation Officer, Eastern District of Missouri (Feb. 18, 2014). Because participants face so many challenges, many—perhaps most—will not ultimately complete the program successfully, but Nicholson emphasizes that even participants who fail to graduate may be successful by other measures. "If they can make the transition out of the gang life, that's a form of success," he said. *Id.* "And if they are no longer in the gang, they are no longer contributing to gang violence in our communities." *Id.*

B. The Project GRIP team

Once an individual is screened and accepted into the program, he is interviewed by the U.S. Probation Office and signs an agreement describing the expectations and obligations of the program. The agreement is signed by members of the Project GRIP team, consisting of representatives from U.S. Probation, the U.S. Attorney's Office, the Federal Defender's Office, and the U.S. District Court. In keeping with the program's collaborative focus, each member of the team is an active participant in a less adversarial, more managerial approach to supervision. The USPO is assigned a specialized caseload of screened participants and is charged with providing appropriate treatment referrals based on a participant's particularized needs. At least twice monthly, the USPO prepares a Progress Report on each Project GRIP participant, informing the rest of the team of the participant's status and progress. Contact with each participant occurs at least four times a month. Serious problems with supervision are brought to the immediate attention of the other members of the team in order to provide immediate intervention and to address pending issues. SUMMARY, at pg. 2–3.

When a participant is succeeding, the district court judge offers positive feedback. Other rewards for successful compliance include decreased frequency of court sessions, a graduation certificate upon program completion, and up to a one year reduction of the supervision sentence. When a participant is noncompliant or in violation of supervision, the judge will be advised through the Progress Report. The judge will then receive recommendations from the other team members before imposing the appropriate sanction. Whenever possible, sanctions are progressive in terms of severity. Potential sanctions include increased reporting, writing assignments, a verbal/written/judicial reprimand, increased frequency of meetings with the USPO or treatment provider, increased self-help meetings, community service, curfew, electronic monitoring/home confinement, residential placement, incarceration, indictment/new prosecution, or revocation. When the team determines that a participant has exhausted all opportunities to continue in the program, the team will make the final decision to commence revocation proceedings before the sentencing judge. *Id.* at 2–4.

Assistant U.S. Attorney (AUSA) Tom Rea, one of the original team members, gives special credit to the U.S. Probation Officers. "This program requires extra work from the U.S. Probation Officers because the program is so intensive. That's why the program needs to start small—no more than 4 to 6, perhaps up to 10 to 12 participants as it evolves. To optimize success, it must remain focused." Telephone Interview with Tom Rea, Assistant U.S. Attorney, Eastern District of Missouri (Feb. 19, 2014). Rea, who has been an AUSA for almost eight years, is unaware of any federal reentry program comparable to Project GRIP. He stressed that former gang members are a unique population. They must develop a value system and a worldview apart from the gang lifestyle if they are to become contributing members of society. One former gang member, ultimately revoked from the program, told Judge Autrey, "This is hard. It's easy to be me—to do what I've done before." Interview by Henry Edward Autrey with a former

gang member, in the Eastern District of Missouri. According to Judge Autrey, "Divorcing yourself from the gang lifestyle requires coming to the point where you can say: to thrive, I must leave this." Telephone Interview with Henry Edward Autrey, U.S. District Court Judge, Eastern District of Missouri (Feb. 19, 2014). "It falls on the participant to follow through," said Rea. Telephone Interview with Tom Rea, Assistant U.S. Attorney, Eastern District of Missouri (Feb. 19, 2014).

Judge Autrey believes that the small size of the program allows for increased communication not only between the team members, but also between the program participants. Gang members are not inclined to discuss their life experiences or share their frustrations and concerns. Keeping the program small enables participants to feel less threatened and to share while learning from each other. Rea agrees. "I am looking for two main things: candor and progress. Candor and honesty are necessary when a participant falters. But progress is required, too. Even a half-step back is problematic for this group. We, as a team, must be pushing our participants to move forward—always forward." *Id*.

C. Key provisions of the Project GRIP Program

The GRIP program relies on several key components. Most importantly, participants appear in regularly scheduled court sessions twice a month. Like most reentry programs, court oversight is the most important feature of the program. These court hearings place the program participants, the judge, and the team members together in a positive context. Participants who meet the employment/education requirements are required to attend court only once a month. Regular contact between the participants and the USPO is also essential. Noncompliance with the reporting requirement will be brought to the immediate attention of the team. Program participants are required to obtain and maintain full-time employment or be enrolled in school unless disabled. Disabled participants are expected to perform community service. If a participant is unemployed, employed part-time, or becomes unemployed while in the program, the participant must participate in the Employment Program. Both students and employed participants are required to provide ongoing verification of their schooling or employment status. SUMMARY, at 4–8.

Education is a key component of Project GRIP. Participants who lack a GED are strongly encouraged to obtain one, and all participants are required to complete a cognitive behavioral program, such as Think for a Change or Making it Work. Participants are responsible for any court-ordered financial payments, such as child support, and the participant's financial status is reported to the judge during each court session.

Because Project GRIP is designed to meet the particularized needs of its participants, different services and opportunities will be made available, based upon need. For example, some participants may need assistance obtaining identification, a driver's license, social security card, or birth certificate. Others may require drug treatment or aftercare. Still others require transportation for work, such as bus passes. Some may require assistance with tattoo removal. In sum, Project GRIP helps identify service-care providers who can provide the necessary assistance.

One of the most important components of Project GRIP is the participants' personal input in the goal-setting process. Each participant is required to select and identify three to five personal goals that he will be responsible for achieving. These goals typically include finding employment, establishing a bank account, meeting child support obligations, and obtaining a GED. The goals are documented and incorporated into each participant's Progress Report. Team members assist the participant in identifying the means and methods necessary to meet these goals. As goals are met, new goals are established. "The goals keep pushing participants forward, and the process creates personal responsibility," said Nicholson. Telephone Interview with Michael P. Nicholson II, U.S. Probation Officer, Eastern District of Missouri (Feb. 18, 2014).

D. Proposal to direct greater resources toward trauma-focused cognitive behavioral therapy

The GRIP team is currently considering a cutting edge proposal to direct greater treatment resources toward trauma-focused cognitive behavioral therapy in an effort to address the root causes of violence and anti-social gang behaviors in GRIP participants.

As noted above, the lives of many individuals involved with gangs are permeated with the strains of daily violence. Gang members, of course, have an increased risk for being victimized by, and to participate in, violence. Finn-Aage Esbensen, Dana Peterson, Terrance J. Taylor & D. Wayne Osgood, *Results from a Multi-Site Evaluation of the G.R.E.A.T Program*, JUSTICE QUARTERLY, Aug. 15, 2011, at 128. The media at times refers to gang violence as "urban war." *See* CHICAGO MUCKRAKERS, *available at* www. chicagonow.com/chicago-muckrakers/2012/06/new-anti-gang-plans-do-little-to-fix-root-cause-of-urban-warfare-advocate/ (2014). Conversations between the GRIP team and gang members in the St. Louis area reveal that many gang members feel that they are in a state of constant war. *See* GRIP PROPOSAL FOR TRAUMA FOCUSED COGNITIVE BEHAVIORAL THERAPY 1(CBT PROPOSAL) (on file at EOUSA). Thus, it is not surprising that gang members experience symptoms identical or similar to post-traumatic stress disorder (PTSD). *See* AMERICAN PSYCHIATRIC ASSOCIATION, DIAGNOSTIC AND STATISTICAL MANUAL OF MENTAL DISORDERS (5th ed. 2013).

Research shows that trauma-focused cognitive behavioral therapy can provide an effective intervention for trauma. CBT PROPOSAL, at 2. Under the current GRIP proposal, trauma focused cognitive behavioral therapy will be offered to 10 gang offenders in Project GRIP, as determined by the treatment provider. "The treatment will include education about distinguishing between thought and feeling; awareness of ways in which thoughts influence feelings; evaluating thoughts; and developing the skills to be aware, interrupt, and intervene with thoughts. The treatment must be individual to alleviate the risk of traumatizing or triggering other treatment participants through exposure to memories." *Id.* at 3.

The purpose of trauma focused cognitive behavioral therapy will be to "address behaviors that inhibit successful progress while on supervised release, including chronic drug use, continued engagement in violence, and lack of pro-social associates and activities." *Id.* at 1. The trauma focused therapy is designed to increase the opportunity for success by "significantly addressing the criminogenic factors (factors related to the increased likelihood of recidivism), while focusing on mental health and behavior of individual offenders." *Id.* at 2. To be eligible for the GRIP treatment proposal, a formal DSM-V PTSD diagnosis is not necessary. Rather, to the extent an offender exhibits the signs and symptoms of trauma, he will be considered eligible.

By incorporating trauma focused cognitive behavioral therapy, the GRIP program is seeking to address the underlying causes of crime and is charting new territory in the process.

E. Project GRIP's first graduate

Christopher L. Harper was a member of the Crip-affiliated Laclede Town Thunder Cats with a history of violence. He was apprehended in 2003 with a shotgun and stolen pickup truck shortly after a shooting. Police recovered two more guns and $8,000 from Harper's residences. He was sentenced to seven years in federal prison as a result of his crimes. In March 2011, he was the first graduate from Project GRIP. As a result of successfully completing the program, he was allowed to conclude his supervised release term a year early. When he completed the program, he had a full-time job with an auto service company and a part-time job at a fast food restaurant. He was also in the process of saving enough money to buy his first home. *Gang Courts' are a New Approach to Old Problem*, CBS ST. LOUIS (Mar. 28, 2011), *available at* http://stlouis.cbslocal.com/2011/03/28/gang-courts-are-a-new-approach-to-old-problem.aspx.

USPO Jennifer Siwiecki supervised Harper during his participation in Project GRIP. "Chris was incredibly motivated," she said. Telephone Interview with Jennifer Siwiecki, U.S. Probation Officer, Eastern District of Missouri (Feb. 19, 2014). "He worked multiple jobs and stayed focused. Among the goals that Chris set for himself were paying his child support and buying a home. To that end, Harper enrolled in a preparatory home ownership program, Project Home, and he also availed himself of the Smart Money class." *Id.* According to Siwiecki, Harper has since relocated out of state and at last report was doing well.

III. Conclusion

Judge Autrey emphasizes that Project GRIP is very much a work-in-progress and the challenges are many. Locating appropriate resources to address the mental health issues of participants who may be suffering from PTSD is one challenge. Encouraging participants who are trying to leave a gang lifestyle while residing in a halfway house with confirmed gang members is another. Applying gradated sanctions, to include weekend incarceration, at a time of budgetary constraints, is a third. Still, Judge Autrey believes that the benefits of the program strongly weigh in its favor. "This program is working really well in terms of our mission," he said. Telephone Interview with Henry Edward Autrey, U.S. District Court Judge, Eastern District of Missouri (Feb. 19, 2014). Not every participant will graduate, and some will continue to be involved with criminal activity. Thus, success must be measured in relative terms. Still, as Judge Autrey is quick to note, the overwhelming majority have not resumed a violent gang lifestyle, and, for many, Project GRIP has been an opportunity for a brighter future. ❖

ABOUT THE AUTHORS

❑ **David L. Smith** is Counsel for Legal Initiatives at the Executive Office for U.S. Attorneys (EOUSA), where he works on a mixed portfolio of issues including reentry, criminal practice, and national security. Previously at EOUSA, he served as Legislative Counsel and Acting Director of the Equal Employment Opportunity Staff. Before joining EOUSA in 2002, Mr. Smith was in private practice for several years, and prior to that was an Assistant U.S. Attorney in the District of Columbia for 10 years. ✠

❑ **Gretchen C. F. Shappert** is the Assistant Director for the Indian, Violent and Cyber Crime Staff for EOUSA. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004 to 2009. She was also an Assistant U.S. Attorney from 1990 to 2004 and specialized in violent crime and outlaw motorcycle gang prosecutions. ✠