November 2014
Volume 62
Number 6

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 to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201

Border Issues

In This Issue

The Border Search Doctrine: Warrantless Searches of Electronic Devices after *Riley v. California*

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

Warrantless searches of persons and property at our nation's borders have an "impressive historical pedigree" as old as the Fourth Amendment. *United States v. Villamonte-Marquez*, 462 U.S. 579, 585 (1983); *United States v. Ramsey*, 431 U.S. 606, 619 (1977). Indeed, "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border . . . ." *Ramsey*, 431 U.S. at 616. Routine border searches may be conducted without a search warrant, even in the absence of reasonable suspicion, because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004) (upholding a warrantless border search of a vehicle, including removal and disassembly of the gas tank, despite the lack of reasonable suspicion). In *Flores-Montano*, the Court stated that "reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to" personal property, such as vehicles, at the border. *Id.* at 152. The executive branch has always had plenary authority to defend the nation's borders and to regulate commerce. Complex balancing tests to determine what is a "routine" versus an "intrusive" search, have no place in the border search of vehicles. *Id.* at 152–53.

At the same time, the Fourth Amendment includes a reasonableness requirement, which considers the nature and scope of the search. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 538, 541 (1985) (searches or seizures that are especially intrusive, such as detention of suspected alimentary canal smugglers, require at least reasonable suspicion). The Supreme Court has never defined precisely what constitutes a reasonable versus an unreasonable border search. *See Ramsey*, 431 U.S. at 618 n.13. Rather, the Court has emphasized the necessity for a case-by-case analysis. *See United States v. Cotterman*, 709 F.3d 952, 963 (9th Cir. 2103) (en banc).

Warrantless border searches are also authorized by statute. *See generally* 8 U.S.C. § 1225(d)(1) (2014) (authority to board and search any conveyance believed to be bringing aliens into the United States); 8 U.S.C. § 1357(c) (2014) (immigration officers at the border may conduct warrantless searches of any person seeking admission to the United States if there is reasonable cause to suspect that grounds for denial of admission would be disclosed by such search); 19 U.S.C. § 482 (2014) (search of vehicles and persons regarding merchandise); 19 U.S.C. § 1467 (2014) (special inspection, examination, and search); 19 U.S.C. § 1496 (2014) (examination of baggage); 19 U.S.C. § 1499 (2014) (examination of merchandise); 19 U.S.C. § 1581 (2014) (boarding of vessels/searching of vehicles); 19 U.S.C. § 1582 (2014) (search of person and baggage—regulations). The fainterplay between the sovereign's right to conduct border searches without a search warrant or reasonable suspicion and the statutory provisions for

customs inspectors operating at the border was the focus of the Supreme Court's analysis in *United States v. Ramsey*, 431 U.S. at 608–09, for example. In that case, customs officials inspecting incoming international mail observed eight suspiciously bulky envelopes from Thailand, all apparently typed on the same typewriter. The Court stated that the custom officials had a "reasonable cause to suspect" a violation of the customs laws when they opened the first class mail for inspection without first obtaining a search warrant. *Id.* at 607–08. The Court stressed that "reasonable cause to suspect" a customs law violation of 19 U.S.C. § 482 is "a practical test," less stringent than the probable cause standard for the issuance of warrants imposed by the Fourth Amendment. *Id.* at 611–13. Indeed,

> [t]he Congress which proposed the Bill of Rights, including the Fourth Amendment . . . had, some two months prior to that proposal . . . granted customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed . . . ."

Id. at 616. The Court concluded that border searches are not subject to the warrant provisions of the Fourth Amendment and are "reasonable" within the meaning of the Amendment. *Id.* at 617–18 (citing *Carroll v. United States*, 267 U.S.132, 162 (1925)).

The broad scope of the border search doctrine as applied to the warrantless searches of electronic devices is subject to refinement and reassessment by virtue of the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473, 2493 (2014), in which a unanimous Court held that "a warrant is generally required" before searching information stored on a cell phone seized incident to an arrest. The Court indicated that law enforcement officers may search cell phones without a warrant in exigent circumstances, where there is a "need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, [or] to assist persons who are seriously injured or are threatened with imminent injury." *Id.* at 2494 (citing *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011)). Absent these exigencies, law enforcement must obtain a warrant. Hence, the question becomes: Is the historically broad border search doctrine in any way limited by the *Riley* decision?

II. Federal court decisions regarding border searches of electronic devices before the Supreme Court's *Riley* decision

A. *United States v. Ickes*

Legal issues surrounding the search of electronic devices at the border are a relatively new phenomenon, spurred by ever-changing technology. One of the earliest circuit cases addressing the issue of warrantless searches of electronic devices at the border is *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), where the defendant was charged with transporting child pornography. In *Ickes* the defendant was attempting to return to the United States from Canada when U.S. Customs agents searched his van at the Ambassador Bridge port of entry near Detroit. At the primary inspection point, the defendant told the Customs Inspector that he was returning from a vacation. The inspector became suspicious because the defendant's van appeared to contain "everything he own[ed]." *Id.* at 502. The defendant was referred to a secondary inspection station where agents confiscated pictures of nude and semi-nude boys, marijuana seeds, and a copy of a Virginia arrest warrant for the defendant. The defendant was placed under arrest and, while he was detained, agents discovered two additional outstanding arrest warrants for the defendant. A more thorough search of his van revealed a computer and approximately 75 disks of child pornography.

Prior to his trial, the defendant moved to suppress the contents of the computer and the disks, contending that the warrantless search of his vehicle violated his First and Fourth Amendment rights. The district court denied defendant's motion, noting that the search was authorized by the extended border search doctrine, an established exception to the Fourth Amendment warrant requirement. The defendant was convicted following a bench trial and gave notice of appeal.

The Fourth Circuit's affirmance of the defendant's conviction contains an excellent analysis of the border search doctrine and of 19 U.S.C. § 1581(a) (inspecting and searching a vessel or vehicle). Quoting extensively from *Ramsey* and *Flores-Montano*, the Fourth Circuit noted:

> the same Congress which proposed the Fourth Amendment to state legislatures also enacted the first far-reaching customs statute in 1790. . . . Thus, since the birth of our country, customs officials have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause.

Id. at 505 (citations omitted). The competing interests of Government and of the individual arrestee are weighed differently at the border than at an individual's residence. A port of entry is *not* analogous to a residence and, therefore, the individual's expectation of privacy is "substantially lessened" at the border. *Id.* at 506 (citing *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (plurality opinion)). A traveler approaching the border should not be surprised to have his or her baggage searched by customs officers, intending to prevent illegal items from entering the country.

The *Ickes* court emphasized that the statutory language of 19 U.S.C. § 1581(a) is sweeping:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters . . . or at any other authorized place . . . and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board . . . .

Id. at 504.

Indeed, the broad language of the statute augurs in favor of the Government's expansive border search authority. The defendant's claim that the statutory language was insufficient to cover the computer and computer disks was rejected by the court, which noted that Congress chose to use the embracive term "cargo," which, according to its ordinary definition, would include the items seized from the defendant's van. *Id.*

The Fourth Circuit also declined defendant's invitation to carve out a First Amendment exception to the border search doctrine, noting that the ramifications of a First Amendment exception would be "quite staggering." *Id.* at 506. The sovereign's interest in protecting its borders includes a national security interest in uncovering terrorist communications, which the court emphasized are inherently "expressive." *Id.* "[A] First Amendment exception to the border search doctrine would ensure significant headaches for those forced to determine its scope." *Id.*

The argument in *Ickes*, which may ultimately call into question the breadth of warrantless border searches for electronic devices, pertains to the increasingly ubiquitous nature of computer technology. The defendant in *Ickes* warned that denying his motion to suppress the warrantless search of his computer meant that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive." *Id.* at 506–07. According to the Fourth Circuit, "[t]his prediction seems far-fetched." *Id.* It is important to note that the computer search in *Ickes* was a conventional search and not a forensic search. As will be seen, with the development and widespread use of forensic searches, to include the creation of a bitstream copy of the hard drive and use of specialized software to conduct the search, the defendant's warning appears more credible. As a result of technological advancements, courts are scrutinizing more closely the reasonableness of a given border search.

B. *United States v. Arnold*

Whether airport customs officials may examine the electronic contents of a passenger's laptop computer without reasonable suspicion or a search warrant under the border search doctrine was

addressed by the Ninth Circuit in *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008). The defendant in *Arnold* was a returning passenger on a flight from the Philippines whose computer was examined as he re-entered the United States. While conducting a routine search, Customs Border Patrol (CBP) officers found numerous images of child pornography and proceeded to seize the defendant's computer. It is important to note that law enforcement officers did not conduct a forensic search of the defendant's computer. The defendant was subsequently charged with transporting child pornography. He moved to suppress the images. The district court granted defendant's motion, finding that reasonable suspicion was necessary to search a laptop computer and that the Government failed to meet its burden of demonstrating that CBP officers had reasonable suspicion to search. The Government appealed.

The defendant argued before the Ninth Circuit that a laptop is analogous to a home because "a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home." *Id.* at 944. Using the same argument unsuccessfully advocated by the defendant in *Ickes*, the defendant in *Arnold* also claimed that the First Amendment requires a higher level of suspicion for searches of "expressive materials." *Id.* (citing *Ickes*, 393 F.3d at 506–08). The Ninth Circuit rejected both arguments, reiterating that "[t]he authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity." *Id.* (citing *Torres v. Puerto Rico*, 442 U.S. 465, 472–73 (1979)). The court further emphasized that searches conducted at the border of closed containers and their contents do not require a particularized suspicion. "[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Id.* at 946. *See generally United States v. Bunty*, 617 F. Supp. 2d 359, 365–66 (E.D. Pa. 2008) (holding that agents did not need reasonable suspicion to conduct a routine border search of computer equipment, but on the facts of this case, reasonable suspicion supported the search). *See also United States v. Romm*, 455 F.3d 990, 996–97 (9th Cir. 2006) (upholding border search of a computer; suggesting, but not holding, that reasonable suspicion is not required for non-destructive border searches); *United States v. McAuley*, 563 F. Supp. 2d 672, 679 (W.D. Tex. 2008) (border search of a personal computer is a routine search and does not require reasonable suspicion to search computer disks, hard drive, or other related devices).

The Ninth Circuit in *Arnold* noted that, with regard to especially intrusive border searches of an individual, reasonable suspicion is required because the Fourth Amendment protects "[t]he interests in human dignity and privacy." *Arnold*, 523 F.3d at 945 (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 540 n.3 (1985) (search of traveler's alimentary canal)) (internal quotations omitted). The Ninth Circuit noted that "the Supreme Court has left open" the possibility that a border search might be considered unreasonable and in violation of the Fourth Amendment because of the *way* that the search was executed. *Id.* (citing *United States v. Flores-Montano*, 541 U.S. 149, 155 n.2 (2004)) (citations omitted). Based on the facts in *Arnold*, the court concluded that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Id.* at 946. *See also United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (border inspection of a sealed package; a court assessing the Fourth Amendment's reasonableness requirement must consider the intrusiveness of the search, the manner in which the search was conducted, and the initial justification for the search).

Finally, the *Arnold* court stated that because the defendant never claimed that the border search of his laptop damaged it in any way, the court was not required to consider whether exceptional damage to property required a particularized suspicion to support the search. The court did, however, examine the defendant's claim that the search of his laptop was conducted in a "particularly offensive manner." *Arnold*, 523 F.3d at 946–97. The court noted that the search was routine and that the laptop's significant storage capacity did not make the search "particularly offensive." *Id.* at 947. Finally, the *Arnold* court adopted the reasoning of the Fourth Circuit in *Ickes* and declined to carve out a First Amendment exception to the border search doctrine based on the fact that expressive material was the subject of the search. *Id.* at 948 (citing *Ickes*, 393 F.3d at 506–08).

C. *United States v. Cotterman*

In *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc), the Ninth Circuit re-visited issues discussed in *Arnold*. In *Arnold* the border search of the defendant's computer was a routine search. However, the border search of the defendant's computer in *Cotterman* was a forensic search. Indeed, *Cotterman* is the first and the only circuit court case that has held that the forensic search of electronic devices at the border is *not* a routine search and, therefore, requires reasonable suspicion. *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 552 (D. Md. 2014). *Cotterman* arose from the seizure of the defendant's two laptop computers at the Lukeville, Arizona, Port of Entry in response to an alert based, in part, on the defendant's 15-year-old conviction for child molestation and, in part, upon intelligence information suggesting that the defendant might be involved in child sex tourism. The initial search of the laptops did not reveal any incriminating information. After the initial search at the border, agents created copies of the hard drives and conducted forensic examinations of the defendant's computers. Only after the computers were shipped almost 170 miles and subjected to a forensic examination were images of child pornography located.

The scope of the *Cotterman* analysis is summarized in the Ninth Circuit's opening paragraphs:

> This watershed case implicates both the scope of the narrow border search exception to the Fourth Amendment's warrant requirement and privacy rights in commonly used electronic devices. The question we confront "is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 . . . (2001). More specifically, we consider the reasonableness of a computer search that began as a cursory review at the border but transformed into a forensic examination of Cotterman's hard drive.

Cotterman, 709 F.3d at 956–57.

There were two questions for the court to resolve: Was the warrantless search of the computer hard drives within the ambit of the border search exception? If so, were the searches reasonable within the provisions of the Fourth Amendment? The court held that the scope and manner of the search was constitutional under the Fourth Amendment.

In its opinion, the Ninth Circuit began by restating that border searches form "a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause." *Id.* at 960 (quoting *United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008)) (internal quotations and citations omitted). The Ninth Circuit acknowledged that in its earlier *Arnold* decision the court stated broadly that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Id.* at n.6 (quoting *Arnold*, 533 F.3d at 1008). Sitting en banc, the *Cotterman* court expressly narrowed *Arnold* "to approve only the relatively simple search at issue in that case, not to countenance suspicionless *forensic* examinations." *Id.* (emphasis added). Notwithstanding a diminished expectation of privacy at the border, there must be "some level of suspicion" in situations involving "highly intrusive searches." *Id*. at 963 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)).

Even at the border, individual privacy rights must be balanced against the sovereign's interests. Insofar as the Fourth Amendment expectation of privacy is concerned, the question comes down to reasonableness. Because "the touchstone of the Fourth Amendment analysis remains reasonableness," courts must examine the scope of the search, including the period during which the owner is deprived of his property. *Id.* (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985); *United States v. Jacobsen*, 466 U.S. 109, 124 (1984); *United States v. Duncan*, 693 F.2d 971, 977 (9th Cir. 1982)).

The court noted that international travelers expect that their property will be searched at the border. What they do not expect is an exhaustive and lengthy search of personal effects, absent some articulable suspicion. The constitutionality of the initial examination of Cotterman's laptops was never in doubt. Had the search concluded with only a routine cursory inspection, the search almost certainly would have been reasonable, even without a particularized suspicion. However, the search was transformed into something quite different when agents proceeded to request a forensic examination that comprehensively analyzed the hard drives. "It was essentially a computer strip search." *Cotterman*, 709 F.3d at 966.

It is important to note that the forensic search of the hard drives was a border search and not an extended border search, because Cotterman's computers never cleared customs. Extended border searches consist of a search occurring after "the subject has regained an expectation of privacy." *Id.* at 962. It is defined as "any search away from the border where entry is not apparent, but where the dual requirements of reasonable certainty of a recent border crossing and reasonable suspicion of criminal activity are satisfied." *Id.* at 961 (quoting *United States v. Guzman-Padilla*, 573 F.3d 865, 878–79 (9th Cir. 2009)) (internal quotation and citations omitted). *Accord United States v. Stewart*, 729 F.3d 517, 525–26 (6th Cir. 2013) (defendant, who arrived at a U.S. airport from Japan, was not subjected to an extended border search where the non-forensic search of his computer, following the random stop and search of the defendant, occurred one day later at a field office 20 miles away from the airport; the laptop computer never cleared the border), *cert. denied*, 134 S. Ct. 1044 (2014). The fact that the defendant's laptop computers in *Cotterman* were transported to another location for examination did not transform the nature of the border search. The computers remained in the possession of border agents; the defendant never regained custody.

The "comprehensive and intrusive nature of a forensic examination—not the location of the examination," requires that there be a reasonable suspicion to support the warrantless search under the Fourth Amendment. *Cotterman*, 709 F.3d at 962. Reasonable suspicion requires "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Id.* at 968 (quoting *United States v. Cortez*, 449 U.S. 411, 417–18 (1981)). The assessment includes the "totality of the circumstances." *Id.* Rejecting concerns raised in the dissenting opinion, the Cotterman court emphasized that reasonable suspicion is "a modest, workable standard," already applied in the context of the extended border search doctrine, the *Terry* stop. *Id.* at 966 (citing *Terry v. Ohio*, 392 U.S. 1, 30 (1968)).

A forensic analysis of a computer hard-drive "directly implicat[es] substantial personal privacy interests." *Id.* at 964. Historically, the amount of private information carried by an international traveler was circumscribed by the size of one's luggage or vehicle. The court noted that in the electronic age, this is no longer true. "Electronic devices are capable of storing warehouses full of information." *Id.* The nature of the contents of electronic devices is also distinguishable from luggage. Electronic devices "are simultaneously offices and personal diaries." *Id.* The contents of electronic devices are "papers," protected by the Fourth Amendment. *See* U.S. CONST. amend. IV. These records are intended to be kept private, and this expectation of privacy is "one that society is prepared to recognize as 'reasonable.' " *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). "A person's digital life ought not be hijacked simply by crossing a border." *Id.* at 965.

Indeed, electronic devices actually contain a different quality of information as compared with luggage. In *Cotterman* agents recovered incriminating files that the user had ostensibly deleted. "It is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried." *Id.* The court surmised that with the emergence of cloud computing, the Government's search of personal data becomes even more problematic: "The point is technology matters." *Id.* The unique quality and quantity of electronic data creates a significant expectation of privacy, thereby rendering exhaustive exploratory searches more intrusive than with other forms of property.

According to the Ninth Circuit, applying a reasonable suspicion standard does not impede the deterrent effect of routine, suspicionless searches, such as vehicle checkpoints near the border. Suspicionless searches, as approved in *Arnold*, will continue. Forensic examinations will be justified in those situations where suspicions are aroused by specific, articulable factors—"subtle cues that criminal activity may be afoot." *Cotterman*, 709 F.3d at 967. Reasonable suspicion does not require complex legal determinations, even in a circumstance where officers examine an electronic device during a border search. What is required, is "a commonsense differentiation between a manual review of files on an electronic device" and a forensic examination of the computer hard drive. *Id.* The latter must be premised upon a "particularized and objective basis for suspecting the person stopped of criminal activity." *Id.* (quoting *United States v. Tiong*, 224 F.3d 1136, 1140 (9th Cir. 2000)).

Focusing on the specific facts of the border search in *Cotterman*, the Ninth Circuit noted that the decision to search the defendant's personal effects was premised on the Treasury Enforcement Communications System (TECS) hit, which indicated that the defendant not only had a 1992 prior conviction for child molestation, but that he was a sex offender who frequently traveled outside of the country and who was possibly involved in child sex tourism. *Id.* at 957, 968. Two other factors supported the agent's reasonable suspicion to search the hard drives of the defendant's laptops. First, Mexico is a country associated with child sex tourism. Second, the TECS alert was part of Operation Angel Watch, which targeted individuals potentially involved in child sex tourism and which alerted law enforcement officers to be on the alert for laptops, cameras, and other paraphernalia associated with child pornography. The court stated that the defendant's 1992 conviction alone was not sufficient to support reasonable suspicion but, combined with the other factors articulated by law enforcement, gave rise to reasonable suspicion of criminal activity.

One additional factor offered by the Government, to which the court was reluctant to give much weight, was the existence of password-protected files. Because passwords have become ubiquitous, that factor alone would not create reasonable suspicion. "To contribute to reasonable suspicion, encryption or password protection of files must have some relationship to the suspected criminal activity." *Id.* at 969. In a situation where other factors point to the possible existence of child pornography, password-protected files are a factor that may contribute to the basis for reasonable suspicion to conduct a forensic examination, because child pornography is usually kept hidden. Indeed, the existence of password-protected files is also relevant to assessing the scope and duration of a forensic search, because the search of password-protected files is necessarily more time-consuming.

The *Cotterman* court concluded that the agents' observations and experience supported reasonable suspicion to justify the scope and manner of the search under the Fourth Amendment. The defendant's innocent explanation that at least one of the computers was a company computer that had multiple users did not tip the balance and did not undermine the reasonable suspicion of the agents. Therefore, the search was valid.

D. Other federal courts

Similar issues have been addressed by other federal courts. Less than nine months after the Ninth Circuit's en banc *Cotterman* decision and roughly six months before the Supreme Court's *Riley* decision, Judge Edward R. Korman, Senior U.S. Judge in the Eastern District of New York, issued a memorandum and order in *Abidor v. Napolitano*, 990 F. Supp. 2d 260 (E.D.N.Y. 2013). This lawsuit was originally filed in 2010 by Pascal Abidor, a graduate student in Islamic studies, whose laptop was seized by border patrol agents as he traveled from Canada into the United States on an Amtrak train. Abidor, together with the National Association of Criminal Defense Lawyers and the National Press Photographers Association, sought a declaratory judgment that CBP and U.S. Immigration and Customs Enforcement (ICE) policies violate the First and Fourth Amendment. The plaintiffs also sought to enjoin the defendant law enforcement agencies, CBP and ICE, from enforcing their policies of searching, copying, and detaining electronic devices at the international border without reasonable suspicion. The case was ultimately

resolved by the district court's determination that the plaintiffs lacked standing and that a declaratory judgment was unwarranted based upon the facts before the court. *Id.* at 275. The court also concluded that customs agents did not need a reasonable suspicion to examine or confiscate a traveler's electronic devices, including laptop computers and cell phones, at the border. *Id.* at 270–73, 276–77. *See also* Susan Stellin, *District Judge Upholds Government's Right to Search Electronics at Border*, N.Y. TIMES, Dec. 31, 2013, at B3.

Notwithstanding the plaintiffs' lack of standing, the district court felt compelled to discuss the merits of plaintiffs' claims "to complete the record and avoid the possibility of an unnecessary remand . . . ." *Abidor*, 990 F. Supp. 2d at 277. Plaintiffs challenged regulations that were adopted by the Department of Homeland Security, CBP, and ICE, to regulate border searches of electronic devices. Specifically, the regulations authorized "the inspection of any files and images stored on electronic devices, the performance of searches on the electronic devices, the detainment of electronic devices for a reasonable time to perform such searches, and the copying of stored information to facilitate inspection." *Id.* at 264. The court noted that all of these activities were authorized by agency regulations, even where agents lacked reasonable suspicion that the electronic devices contained materials within the jurisdiction of CBP or ICE. The court emphasized that both the CBP and ICE directives contained protocols related to the handling of privileged or sensitive materials. Legal materials, medical records, work-related materials maintained by journalists, proprietary business information, and trade secrets do not enjoy a per se exemption from a border search, but the CBP and ICE directives require notification of agency legal counsel and possible consultation with the U.S. Attorney's office. *Id.* at 266–67.

The district court also discussed in considerable detail the apprehension of graduate student Pascal Abidor at the CBP inspection point near Service Port-Champlain, New York, and the seizure of his laptop computer, digital camera, two cellular telephones, and an external computer hard drive. When a CBP officer examined the plaintiff's passport, the plaintiff told the officer that he had briefly lived in Jordan and visited Lebanon during the previous year. The visas he had obtained from these two countries did not appear in his U.S. passport. Instead, they were contained in a French passport, which was also in the plaintiff's possession. Officers inspected the plaintiff's laptop computer and asked him to enter his password, which he did without objection. The officer in turn, examined photos contained in the laptop that depicted rallies of Hamas and Hezbollah, both of which have been designated as terrorist organizations by the Department of State. The plaintiff explained that research for his Ph.D. was focused on the modern history of the Shiites of Lebanon, a country where Hezbollah operates openly. Plaintiff's laptop and external drive were retained for 11 days before being returned to him.

The district court agreed with the Ninth Circuit in *Cotterman* that reasonable suspicion is not required to conduct a preliminary, cursory search of an electronic device at the border. *Id.* at 277 (citing *Cotterman*, 709 F.3d at 960). The district court also concurred that transporting an electronic device away from the border, in order to conduct a forensic examination, does not transform the search into an extended border search. *Id.* at 277–78; *see also Cotterman*, 709 F.3d at 962 (Extended border searches consist of a search occurring after "the subject has regained an expectation of privacy."). Finally, the district court adopted the Fourth Circuit analysis in *Ickes* and the Ninth Circuit analysis in *Arnold*, refusing to carve out a First Amendment exception to the border search doctrine. *Abidor*, 990 F. Supp. 2d at 277–78 (citing *United States v. Arnold*, 533 F.3d 1003, 1010 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005)).

The district court observed that the Second Circuit has not addressed the issue of border searches of electronic devices. The Third Circuit, in an unpublished opinion, and the Fourth Circuit in *Ickes*, have held that searches of electronic devices constitute routine border searches with no requirement of reasonable suspicion. *Abidor*, 990 F. Supp. 2d at 281 (citing *United States v. Linarez-Delgado* , 259 F. App'x 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment . . . may be inspected and viewed during a reasonable border search."); *Ickes*, 393 F.3d at 506–07. The district court next turned to *Cotterman* and the Ninth Circuit's conclusion that the sheer volume and intrinsic sensitivity of materials

contained in contemporary electronic devices requires that a forensic examination must be premised upon reasonable suspicion. *Abidor*, 990 F. Supp. 2d at 281–82 (citing *Cotterman*, 709 F.3d at 966, 968).

The *Abidor* court agreed with the Ninth Circuit's rationale that requiring reasonable suspicion to support a forensic search of electronic devices at the border would have no practical effect on current practices because the resources to conduct forensic examinations are severely limited and, therefore, forensic searches are conducted only where some level of suspicion is present. The district court concluded that "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required." *Id.* at 282. At the present time, however, "locking in a particular standard for searches would have a dangerous, chilling effect as officer's often split-second assessments are second-guessed." *Id.* (quoting Michael Chertoff, *Searches Are Legal, Essential*, USA TODAY, July 16, 2008, at A10).

In the case of the plaintiff in *Abidor*, the district court concluded that there was reasonable suspicion to support the searches of his electronic devices. CBP agents observed images of the rallies of designated terrorist groups, Hamas and Hezbollah, on the plaintiff's computer; the plaintiff had recently traveled to Lebanon, a country inhabited by Hamas leaders and facilitators; Hezbollah is based in Lebanon and has strong influence in Lebanon's Shia community; the plaintiff explained to customs agents that the area of research for his Ph.D. was the modern history of Shiites in Lebanon; the plaintiff, while living in Canada, possessed both a U.S. and French passport. Taken together, these factors created reasonable suspicion that supported a forensic search of the plaintiff's electronic devices. *Id.* at 282–83.

Notwithstanding the court's determination that reasonable suspicion supported the forensic search, it is important to remember that first, the *Abidor* court found that the plaintiffs lacked standing, so the subsequent analysis of the border search doctrine is purely hypothetical. Second, the court never reached the question of whether reasonable suspicion was necessary to support the forensic search of an electronic device seized during a border search. *Id.* at 272 ("[W]hether reasonable suspicion was required for the search that took place in [the *Cotterman*] case, the procedural posture of the present case makes such a consideration inappropriate."). *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 554–558 (D. Md. 2014) (comparing the analysis used by the *Cotterman* and *Abidor* courts, stating "whereas *Cotterman* did not adequately explain why a forensic search differs from a conventional one, *Abidor* did not appear to recognize any meaningful distinction between the two at all").

The most recent extensive analysis of the border search doctrine, as applied to the search and seizure of electronic devices, appears in *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014), which originated in the District of Maryland. The defendant and his wife were stopped by CBP agents at the Rainbow Bridge outside Buffalo, New York, as they returned from Canada. The defendant, a dual American-Iranian citizen, and his wife were referred to secondary inspection because his name produced a "hit" in TECS. Testimony before the district court indicated that actually there were two TECS hits and that at the time of his apprehension at the border, the defendant was under investigation for possible exports to an embargoed country, Iran. The defendant and his wife were briefly questioned and released. The defendant's two cell phones were seized, subjected to a forensic examination, and ultimately returned to the defendant some 14 days later. Following his indictment for multiple charges of unlawful export to an embargoed country and one count of conspiracy, the defendant moved to suppress the evidence obtained from the forensic search of his electronic devices. The Government responded that the search of the devices was a routine border search and that neither a warrant nor particularized suspicion was needed to support the search.

In its thorough analysis of the border search doctrine and subsequent case law, the district court noted that the Supreme Court has laid out only "the broad strokes" of what constitutes a routine versus a non-routine search, and that the Court has expressly refrained from defining what level of suspicion is required for non-routine border searches. *Id.* at 545–46 (citing *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531, 538, 541 n.4 (1985)). The

Saboonchi court went into considerable detail to explain what actually takes place during a forensic computer search and the substantial difference between a conventional, routine computer search and a forensic search. *Id.* at 547–48, 549–50. The court explained that "the computer forensics process always begins with the creation of a perfect 'bitstream' copy or 'image' of the original storage device saved as a 'read only' file." *Id.* at 547 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005)). A computer forensic expert using special software searches the full contents of the image hard drive, examining individual files, and probing the drive's "slack space" to reveal deleted files. *Id.* at 548. Indeed, a forensic search of an electronic device is a different procedure than a conventional search because of the creation of the bitstream copy of internal files and the use of specialized software when a forensic search is conducted.

Because there is only a limited amount of time to conduct a conventional search of an electronic device at the border, a conventional search of an electronic device is analogous to the search of a suitcase or luggage. As a practical matter, the search will be cursory due to the time constraints. A forensic search, by contrast, may occur over days or weeks, at a location away from the border, and inevitably will include the use of specialized software and the creation of a bitstream copy, which may be examined later. The district court emphasized the sheer volume and breath of data that travelers typically carry in their respective electronic devices that may be subject to this search. Data may include highly personal information, contacts, calendar appointments, purchases, financial and medical records, texts, email, and voicemail, as well as browsing history and deleted information.

The *Saboonchi* court reasoned that "a forensic search is a different *search*—not merely a search of a different object—and it fundamentally alters the playing field for all involved." *Id.* at 564. The court surmised that a computer forensic search "is at least as invasive as an x-ray" and has tremendous "potential for personal indignity and intrusiveness." *Id.* at 569. It is "essentially a body search of a computer," and "[i]f any property search can be considered non-routine, a forensic search of an electronic device must fall in that category." *Id.* The district court noted that *Cotterman* is the only circuit court that has held that a forensic search of an electronic device seized at the border was not a routine search. The *Saboonchi* court could not rely upon the *Cotterman* analysis *in toto*, however, because *Cotterman* was premised on Ninth Circuit case law, which asserts that the border search doctrine is a narrow exception to the Fourth Amendment. Moreover, Fourth Circuit precedent, as defined in *Ickes*, holds that even if the border search doctrine is narrow in geographical scope, it provides broad authority for border searches as an exception to the Fourth Amendment. The district court was careful to note that its conclusion that the forensic search of an electronic device at the border must be supported by reasonable suspicion was not inconsistent with *Ickes*, which involved a routine border search of a computer and did not address forensic searches.

The *Saboonchi* court gave three reasons that a forensic search of a computer is *sui generis*. First, it involves creation of the previously referenced bitstream copy and the use of specialized software in order to conduct the search. Second, a forensic search enables law enforcement to retrieve previously deleted material. Third, a forensic search provides information about a person's domestic activities away from the border that would not be discoverable in a conventional search, including metadata, browser history, unsaved data, and device location information. The court quoted Judge Posner:

> [A]n iPhone application call iCam allows you to access your home computer's webcam so that you can survey the inside of your home while you're a thousand miles away. At the touch of a button a cell phone becomes a house search, and that is not a search of a "container" in any normal sense of that word, though a house contains data.

Id. at 563–64 (quoting *United States v. Flores-Lopez*, 670 F.3d 803, 806 (7th Cir. 2012)). Taken together, these reasons supported the court's conclusion that "a search of imaged hard drives of digital devices taken from the Defendant at the border and subjected to forensic examination days or weeks later cannot be performed in the absence of reasonable suspicion." *Id.* at 569.

Returning to the circumstances of the defendant's stop and search in the case before it, the court stated that Saboonchi was already the subject of two investigations when he and his wife arrived at the Rainbow Bridge Port of Entry. As noted above, the TECS inquiry identified two flags, one out of Washington, D.C., and one out of Baltimore, Maryland. The district court concluded that the circumstances of the defendant's interdiction at the border was "more than sufficient" to give rise to "reasonable, particularized suspicion—if not probable cause" that the defendant was involved in federal export law violations. Therefore, CBP and HIS/ICE officers did not violate the Fourth Amendment when they seized the defendant's electronic devices and subjected those devices to a forensic search. *Id.* at 571.

III. *Riley v. California*

In *Riley v. California*, 134 S. Ct. 2473 (2014), a unanimous Supreme Court held that officers must secure a search warrant before searching information contained in an arrestee's cell phone, absent exigent circumstances. Writing for the Court, Justice Roberts stated that neither the Government's interest in protecting officers' safety, nor its interest in preventing the destruction of evidence, justified dispensing with a search warrant for searches of cell phone data. *Id.* at 2484–87. Even though the search incident to arrest exception does not apply to the digital content of cell phones, the Court noted that "other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 2494. Exigent circumstances, which would justify a warrantless search, include imminent destruction of evidence, flight of a suspect, or the threat of imminent injury. The facts of the case did not involve a border search and did not involve a forensic search of electronic devices. Nonetheless, the High Court's highly instructive analysis of the Fourth Amendment reasonableness standard and society's expectation of privacy may shed light on how appellate courts will review border searches of electronic devices in the future.

Riley is a consolidation of a California Court of Appeal firearms and attempted murder prosecution and a First Circuit narcotics and firearms case, both of which involved warrantless searches of cell phones seized incident to the arrest of the respective defendants. Riley was apprehended in a traffic stop for driving on expired tags. California officers impounded the car and, during a routine inventory search, confiscated firearms concealed under the car's hood. After arresting Riley for possession of concealed firearms, officers searched his pockets and recovered a cell phone, from which pictures and evidence of gang affiliation were recovered. Evidence from Riley's cell phone was introduced at trial in connection with his involvement with a criminal street gang, and he received an enhanced sentence for committing those crimes for the benefit of a gang. Wurie was observed by officers making an apparent drug sale from a car. He was arrested and, at the police station, officers seized and searched two cell phones. Information contained in one of the phones lead to the search of a residence identified as "my house" on the phone's external screen. Officers recovered narcotics, firearms, and drug paraphernalia from the residence. Both cases raised the issue of "the reasonableness of a warrantless search incident to a lawful arrest." *Id.* at 2482.

The *Riley* Court recognized that, although the search incident to arrest exception to the Fourth Amendment warrant requirement has been in existence for nearly a century, the scope of that exception has generated considerable debate. According to the *Riley* Court, "the ultimate touchstone of the Fourth Amendment is reasonableness." *Id.* (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). A warrantless search is reasonable only when it falls within the ambit of a specific exception to the Fourth Amendment warrant requirement. *Id.* (citing *Kentucky v. King*, 131 S. Ct. 1849, 1856–57 (2011)). After reviewing some of its own previous decisions, the Court stated that it was necessary "to decide how the search incident to arrest doctrine applies to modern cell phones . . . technology nearly inconceivable just a few decades ago." *Id.* at 2484. The *Riley* Court noted that the contemporary iteration of the search incident to arrest doctrine was premised upon "concerns for officer safety and evidence preservation . . . ." *Id.* (citing *Chimel v. California*, 395 U.S. 752, 763 (1969)). Four years after *Chimel*, in *United States v. Robinson*, 414 U.S. 218, 235–36 (1973), the justification for a search incident to arrest was deemed reasonable under the Fourth Amendment, even when there was no specific concern about a

loss of evidence or officer safety. In *United States v. Chadwick*, 433 U.S. 1, 15 (1977), the Court clarified that the warrantless search incident to arrest exception is limited to personal property closely associated with the person being arrested. Finally, in *Arizona v. Gant*, 556 U.S. 332, 343 (2009), a case involving the search of a vehicle, the Court concluded that, following the reasoning of *Chimel*, law enforcement officers could search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."

Once the *Riley* Court identified the underlying reasons that support a warrantless search incident to an arrest—officer safety and preservation of evidence—the Court proceeded to consider whether the same reasoning was applicable to warrantless searches of electronic devices, such as cell phones. When a subject is arrested, cell phones may be subjected to an initial examination to ensure that the physical characteristics of the cell phone do not threaten officer safety—checking to see if a phone contains a hidden razor blade, for example. However, cell phone *data* does not pose a threat to law enforcement. The Court rejected suggestions that a search of cell phone data might help ensure officer safety more indirectly, such as alerting officers that criminal associates of the arrestee were heading to the scene. Neither California nor the United States was able to cite specific examples of safety concerns based on actual experience. Therefore, the Court recommended that those rare situations where accessing cell phone data might be necessary to ensure officer safety "are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances." *Riley*, 134 S. Ct. at 2486 (citations omitted).

With regard to the second rationale to support a warrantless search—the preservation of evidence—both Riley and Wurie conceded that officers could seize and secure cell phone to prevent the destruction of evidence while seeking a warrant. California and the United States urged that even seized cell phones are vulnerable to destruction because of the possibility of remote wiping of data and data encryption. The *Riley* Court was unpersuaded: "We have . . . been given little reason to believe that either problem is prevalent." *Id.* The Court noted that threat of remote wiping can be addressed by turning off the device, disconnecting the device from the network, or by placing the device in a Faraday bag to isolate the phone from radio waves. Furthermore, the opportunity for law enforcement officers to search a password-protected phone before the data-encryption software is activated is extremely limited. To the extent that officers have a credible concern about losing data in a particular situation, they may be able to demonstrate exigent circumstances that would justify an immediate search of the phone. A warrantless search of a cell phone incident to an arrest is inherently unreasonable, absent specific exigent circumstances suggesting a " 'now or never' situation." *Id.* at 2487 (quoting *Missouri v. McNeely*, 133 S. Ct. 1552, 1561–62 (2013)).

The second portion of the *Riley* Court's analysis focuses both on the arrestee's expectation of privacy and society's expectation of privacy as applied to the modern-day cell phone. The Supreme Court drew no distinction between a routine search and a forensic search of a cell phone, and the Court's analysis appears to conflate the two. Echoing the language of the *Saboonchi* court, the Supreme Court in *Riley* observed that the information contained in a cell phone is both quantitatively and qualitatively different from other objects that may be kept on the arrestee's person. The immense storage capacity; the co-location of many diverse types of information in one device; the fact that information contained in a cell phone may pre-date the actual purchase of the cell phone; the Internet search and browsing history maintained in the cell phone; the GPS location features in many phones; and the fact that information viewed on cell phones may be stored in a location apart from the phone, such as the cloud, all combine to alter the traditional search incident to arrest analysis. "Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. . . . But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." *Id.* at 2491.

The Government conceded that the search incident to arrest exception does not apply to remotely stored digital information, and this concession has consequences for agents and prosecutors involved in investigations involving border searches, as will be discussed below. The Court recognized that

"[p]rivacy comes at a cost." *Id.* at 2493. Limiting the ability of law enforcement officers to search cell phones confiscated from an arrestee will have consequences for law enforcement investigations. Cell phone data, nonetheless, is obtainable with a search warrant, and "case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 2494. Returning to the reasonableness requirement of the Fourth Amendment, the Court noted that warrantless searches based upon exigent circumstances must be "objectively reasonable" and that a court must make the ultimate determination as to whether an emergency justified the search in a particular case. *Id.* (citing *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011); *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 (2013) (holding in a drunk-driving prosecution that metabolization of alcohol in the bloodstream does not support a per se exigency exception to the Fourth Amendment warrant requirement for non-consensual blood-testing; exigency in this context must be determined case-by-case, based on the totality of the circumstances)).

The *Riley* Court concluded that because of the availability of exigent circumstances, law enforcement officers would still have the ability to search electronic devices without a search warrant in extreme circumstances, such as "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone." *Id.* In all other circumstances "[the] answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." *Id.* at 2495.

IV. Consequences of *Riley* for border searches of electronic devices

As noted, *Riley* did not involve a border search, but the Court's decision does impact the seizure and inspection of electronic devices at the border. In *Riley* the Government acknowledged that the search incident to arrest exception "may not be stretched" to cover files stored in the cloud—"[s]uch a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Id.* at 2491. If a search incident to arrest "may not be stretched" to cover cloud data, then a routine border search "may not be stretched" either. In order to avoid the possibility of accessing remotely stored cloud information, it will be necessary for law enforcement officers at the border to take protective measures when seizing electronic devices in all but extraordinary (exigent) circumstances. One technique involves pressing the power button to activate airplane mode, thereby ensuring that cloud data is not accessed until a search warrant can be obtained.

Second, *Riley* underscores that there are certain case-specific exceptions to the Fourth Amendment's warrant requirement. In the recent *Saboonchi* decision from the District of Maryland, the court concluded that the border exception is one of them. Following the District Court of Maryland's published opinion in that case, the defendant filed a motion to reconsider, citing the *Riley* decision. In denying the defendant's motion, the court concluded that "*Riley* did not diminish the Government's interests in protecting the border or the scope of the border search exception." *United States v. Saboonchi*, No. 8:13-cr-00100-PWG, slip op. at 8 (D. Md. July 28, 2014). "Time and again, [the Supreme Court has] stated that 'searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border.' " *Id.* at 3 (quoting *Flores-Montano*, 541 U.S. 149, 152–53 (internal quotations omitted)).

Finally, Justice Alito's concurrence in *Riley* suggests that the Supreme Court is likely to re-visit the perimeters of the Fourth Amendment in the digital age. He noted that the Court's *Riley* decision created an interesting anomaly where "the Court's broad holding favors information in digital form over information in hard-copy form." *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring). Thus, the phone bills and wallet photos of one suspect are subject to seizure and examination incident to the suspect's arrest, while the cell phone of a second subject may not be examined absent exigent circumstances or a search warrant. *Id.* at 2496–97. Justice Alito called "for a new balancing of law enforcement and privacy interests," although he did not offer a workable alternative. *Id.* For Justice Alito the proper forum for review of privacy is not the federal courts, but the legislatures, who are in a better position "to assess and respond to

the changes that have already occurred and those that almost certainly will take place in the future." *Id.* at 2497–98.❖

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. ✠

The Southwest Border Districts: More Than Immigration Cases

Linda Seabrook
Program Attorney
Indian, Violent and Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

Lately, the evening news often leads with a story about the influx of unaccompanied children, primarily from Central America, into the United States, seeking asylum from the violence and poverty of their respective countries. While the volume of this inflow may be newsworthy, people from Mexico, Central America, and South America, illegally enter the United States through the Southwest border daily. As a result, a majority of the immigration cases prosecuted by the U.S. Attorney's offices are prosecuted by the Southern District of California, the Districts of Arizona and New Mexico, the Western District of Texas, and the Southern District of Texas (collectively, the SWB Districts). According to U.S. Customs and Border Protection, federal agents apprehended 414,397 illegal immigrants along the Southwest border in fiscal year 2013 alone. The SWB Districts prosecuted 99 percent of federal misdemeanors and 42 percent of the nation's federal felony immigration cases in fiscal year 2013.

The SWB Districts share a 1,951-mile border between the United States and Mexico, stretching from San Diego, California, to Brownsville, Texas. The SWB Districts encompass many of the most populous and fastest-growing cities in the United States, such as Houston, Phoenix, San Antonio, Austin, El Paso, and San Diego. Such dense population centers create the opportunity for a significant volume of violent crime, identity theft, child exploitation offenses, tax offenses, and many other federal crimes. The SWB Districts also contain Indian Country and many of the nation's critical military installations, and are home to the energy, high-tech, biotech, and financial industry, which generate growing numbers of ever-complex fraud cases. The federal law enforcement interests along the Southwest border are varied and significant.

I. Narcotics

U.S. Department of Transportation data reveals that over 5 million trucks, more than 66 million personal vehicles, approximately 9,000 trains, more than 400,000 rail containers, and over 170 million people entered the United States in 2013 through the Southwest border. Home to 15 of the 20 busiest land ports of entry to the United States, the SWB Districts handle over 98 percent of the nation's Border Patrol apprehensions. Many of these apprehensions include seized illegal narcotics, such as methamphetamine, marijuana, cocaine, and heroin. The Office of National Drug Control Policy states that more than half of the cocaine and most of the heroin, marijuana, and methamphetamine found on the streets of the cities and towns of the United States enter the country across the Southwest border. Illegal drugs pass through the Southwest border via all modes of conveyance—cars, trucks, trains, rail cars, and on pedestrians crossing the border. In fiscal year 2013, 13,942 drug cases were prosecuted in federal court, with the 5 SWB Districts handling 39 percent of those cases.

Sophisticated criminal organizations based in Mexico control and direct this drug supply into the United States, bringing guns and violence across the border, as well. In addition to the assertive prosecution of drug trafficking activity along the border, the SWB Districts proactively pursue violent drug cartels, including Los Zetas, La Linea, the Knights Templar, and the Sinaloa Cartel. A case from the

Southern District of California provides an example of such efforts. Armando Villareal Heredia, a leader in the Fernando Sanchez Arellano drug trafficking organization, pleaded guilty to federal racketeering and drug charges for his participation in cartel activities, such as murder, kidnapping, intimidation, bribery of public officials, and smuggling of methamphetamine into the United States. This successful prosecution by the Southern District of California was the result of a long-term investigation conducted by the multi-agency San Diego Cross Border Violence Task Force, formulated to target those responsible for violent and organized crime along the border. Villareal, who was arrested by Mexican authorities and extradited to the United States, received a 30-year sentence in December 2013. *See* Press Release, U.S. Attorney's Office, S. Dist. of Cal., Top Lieutenant in Fernando Sanchez Arellano Cartel Sentenced (Dec. 16, 2013), *available at* http://www.justice.gov/usao/cas/press/2013/cas13-1216-VillarealHerediaSent.pdf.

The SWB Districts also forcefully pursue those who assist the cartels, often through the prosecution of money laundering or public corruption offenses. The *Marco Antonio Delgado* case, prosecuted by the Western District of Texas, provides a recent example of such efforts. Delgado, an El Paso attorney, conspired with other individuals to launder approximately $600 million in illegal drug proceeds for the Milenio Drug Trafficking Organization through cash deposits made to his Attorney Interest on Lawyers' Trust Account bank account. Delgado was sentenced in January 2014 to the maximum term of 20 years' imprisonment for this conduct. *See* Press Release, U.S. Attorney's Office, W. Dist. of Tex., El Paso Attorney Marco Delgado Sentenced To Maximum 20 years in Federal prison for multi-Million dollar money laundering scheme (Jan. 24, 2014), *available at* http://www.justice.gov/usao/txw/news/2014/Delgado_EP_sentencing_1.html.

Aggressive prosecution efforts toward these illegal drug organizations ensure that the violence and corruption of the cartels that plague numerous cities and towns in Mexico do not spread across the border to infect the United States. *See* Press Release, U.S. Attorney's Office, W. Dist. of Tex., El Paso Attorney Marco Delgado Sentenced To Maximum 20 years in Federal prison for multi-Million dollar money laundering scheme (Jan. 24, 2014), *available at* http://www.justice.gov/usao/txw/news/2014/Delgado_EP_sentencing_1.html.

II. Human trafficking

Comprised of both labor and sex trafficking, human trafficking remains one of the most low-risk, but high-profit, crimes. The Southwest border presents a prime location for human trafficking activity, given the mass influx of individuals primarily from Mexico and Central and South America seeking a new life and prosperity in the United States. Traffickers use the illegal status, lack of documentation, poor English skills, or financial insecurity of those trafficked, to create dependency on the traffickers for survival. The densely-populated metropolitan areas within the Southwest border create significant opportunities for labor and sex trafficking to meet the demands of industry and the vices of the populace. The victims of such trafficking are not only adults but, increasingly, children. In fiscal year 2013, the Southern District of California and the Western District of Texas were among the U.S. Attorney's offices with the highest numbers of successful prosecutions of 18 U.S.C. § 1591 offenses.

In November 2013, a federal jury in the Western District of Texas convicted Charles Marquez of sex trafficking of a minor; sex trafficking by force, fraud, or coercion; transporting for prostitution; conspiracy to coerce or entice a minor to engage in sexually explicit activity; coercion or enticement; and importation of an undocumented alien for an immoral purpose. Marquez, along with a female conspirator, placed advertisements in a Ciudad Juarez newspaper offering opportunities for those seeking legitimate jobs in the United States. Females answering the advertisement were instead unwittingly recruited for a prostitution scheme. Numerous women, including one minor female, were smuggled into the United States through El Paso by Marquez and his associate. Once in the United States, these victims were held in motels and forced to engage in prostitution. On September 3, 2014, Marquez was sentenced to life in federal prison for these offenses and fined $10,000. *See* Press Release, U.S. Attorney's Office,

W. Dist. of Tex., El Paso Man Sentenced To Life In Federal Prison On Human Trafficking Charges (Sept. 3, 2014), *available at* http://www.justice.gov/usao/txw/news/2014/Marquez_human_trafficking_EP_sen.html. The SWB Districts aggressively prosecute those who smuggle children across the border to be exploited and abused, as well as those who otherwise prey on migrants and immigrants for financial gain.

III. White collar crime

The epicenter of the energy industry in the United States is located in the Western and Southern Districts of Texas. The energy industry produces substantial revenue for these areas, attracts foreign investors, and generates considerable personal wealth for its residents. In addition, Austin, Texas, was rated by Forbes Magazine as the fastest growing city for 2013, with Houston not far behind at number 10. Erin Carlyle, *America's Fastest Growing Cities*, FORBES (Feb. 14, 2014), *available at* http://www.forbes.com/sites/erincarlyle/2014/02/14/americas-20-fastest-growing-cities/. A large, prosperous population often entices those who seek to defraud its citizens, and generally necessitates robust white collar crime enforcement. One of the more notable fraud prosecutions from the Southern District of Texas was Robert Allen Stanford's 20-year, $7 billion international investment fraud scheme through his bank, Stanford International Bank (SIB)—a scheme that the trial judge described as "one of the most egregious frauds ever tried in a federal courtroom." Laurel Brubaker Calkins and Andrew Harris, *Stanford Gets 110-Year Sentence for $7 Billion Fraud*, BLOOMBERG (June 15, 2012), *available at* http://www.bloomberg.com/news/2012-06-14/allen-stanford-sentenced-to-110-years-in-prison-for-ponzi-scheme.html.

In sheer scope, duration, and magnitude, Stanford's crimes were historic. For more than 20 years, Stanford solicited individuals, ranging from highly sophisticated investors to retirees living on fixed incomes, to purchase CDs from SIB, an offshore bank based in Antigua. The bank then purportedly invested the proceeds in conservative investments, such as stocks of multinational corporations and bonds offered by stable governmental entities. To sell the CDs, Stanford established brokerage firms based in the United States and outside the country, particularly in Venezuela, and acquired several other financial services companies, which served as a pipeline for new victims.

Stanford was ultimately convicted in March 2012 and sentenced to 110 years' imprisonment, which resulted in a $330 million forfeiture jury verdict—the largest in history—and a $5.9 billion personal money judgment against Stanford. While the Chief Financial Officer and the Chief Investment Officer of Stanford's business empire pleaded guilty, Stanford's Chief Accounting Officer, Gilbert Lopez, and Global Controller, Mark Kuhrt, went to trial in November 2012. Those defendants were each recently sentenced to 20 years' imprisonment and assessed personal money judgments in excess of $2 billion. *See* Press Release, Dep't of Justice, Former Executives of Stanford Financial Group Entities Sentenced to 20 Years in Prison for Roles in Fraud Scheme (Feb. 14, 2013), *available at* http://www.justice.gov/opa/pr/former-executives-stanford-financial-group-entities-sentenced-20-years-prison-roles-fraud.

IV. Indian Country and federal land

The Environmental Protection Agency estimates that federal land encompasses over 70 percent of the State of Arizona, due primarily to tribal trust land, military installations, and national parks and forests. The National Park Service reports that Grand Canyon National Park receives approximately five million visitors each year. Federal land comprises 35 percent of the District of New Mexico. Because these federal enclaves are often improved and maintained through government contracts, the SWB Districts have extensive experience prosecuting federal contracting fraud cases, including the corruption of governmental employees or the fraudulent use of straw contractors to obtain non-competitive contracts. The extensive network of national parks and forests contained within the SWB Districts creates a steady volume of work for the SWB Districts, ranging from petty offenses and citations to violent crime. It also affords those Districts the opportunity to prosecute unique cases protecting our nation's wildlife and resources.

According to the Bureau of Indian Affairs, 22 sovereign Native Indian tribes reside in both the Districts of New Mexico and Arizona. High rates of poverty, poor infrastructure, lack of educational and vocational opportunities, and the alcohol and drug abuse that often accompany these problems, creates fertile ground for the proliferation of violent crime. In fact, Bureau of Justice Statistics data demonstrates that, collectively, Indian reservations have violent crime rates more than 2½ times higher than the national average. Crimes committed in Indian Country are generally not the type of offenses prosecuted by a U.S. Attorney's office—sexual assault, domestic violence, kidnapping, and child sexual assault, as opposed to bank robberies, wire fraud, and other more common federal offenses. The complexities of domestic and intra-familial violence, and the difficulties of prosecuting cases with reluctant witnesses and victims, create a challenging additional caseload for the SWB Districts.

United States v. Marshall, No. 13-CR-8050-PCT-NVW (D. Ariz. Dec. 16, 2013), a case prosecuted by the District of Arizona, clearly demonstrates these challenges. Marshall, within the confines of the Havasupai Indian Reservation in Arizona, committed two separate violent assaults against two different women. Marshall brutally sexually assaulted one victim, and he assaulted the other by ramming the sharp end of a shovel into her face. The resulting injury left the second victim permanently disfigured and blind in one eye. Marshall demonstrated no remorse for his actions and, in fact, seemed proud of his conduct upon arrest. The victim who was assaulted with the shovel, despite the heinous and brutal attack she sustained and the significant injuries she suffered, declined to meaningfully participate in the prosecution. A quote from this victim, as relayed by Assistant U.S. Attorney Christine Keller (AUSA Keller) during Marshall's sentencing hearing, demonstrates the dynamics and difficulties such cases present. During an initial interview, AUSA Keller asked the victim why she would stay with someone who would brutalize her so severely. At the sentencing hearing, AUSA Keller quoted the victim's response verbatim: "Because I love him, and I want him to take care of me. If he's gonna kill me, then I want to give him permission to take care of my body and do whatever he want [sic] to do with me. It's kind of like suicidal, but I'm not suicidal. It's just I love him like that." Marshall received concurrent sentences of 10 years for both assaults. *Id.*

V. National security

The SWB Districts house numerous military installations, including the largest, Fort Hood, located in the Western District of Texas. The Southern District of California contains more military bases and facilities than any other district in the United States. Military installations not only serve as economic drivers for the districts where they are housed, but also heighten security concerns for those areas. The District of New Mexico, which has five military bases, a NASA facility, and national laboratories, recently prosecuted a husband and wife who were former employees of the Los Alamos National Laboratory (LANL). The cases against Majorie Roxby Mascheroni, a former technical writer and editor, and her husband, Dr. Pedro Leonardo Mascheroni, a physicist, illustrate the complexity of national security cases and the importance of vigorously protecting military facilities and national laboratories in the United States.

Dr. Mascheroni, a naturalized U.S. citizen from Argentina, worked as a scientist at LANL from 1979 to 1988, and held a security clearance which allowed him access to "Restricted Data." Mrs. Mascheroni worked at LANL from 1981 until 2010, and similarly held a security clearance allowing access to "Restricted Data." The Atomic Energy Act defines "Restricted Data" as information "concerning (1) the design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy." 42 U.S.C. § 2014 (y) (2014). Both defendants were charged with conspiracy to communicate and communicating restricted data to an individual with the intent to secure an advantage to a foreign nation, as well as other related offenses. In their respective guilty pleas, the couple admitted that they unlawfully communicated restricted data to another individual with reason to believe that the data would be used to secure an advantage to Venezuela. *See* Press Release, Dep't of Justice, Former Workers at Los Alamos National

Laboratory Plead Guilty to Atomic Energy Act Violations (June 21, 2013), *available at* http://www.justice.gov/opa/pr/former-workers-los-alamos-national-laboratory-plead-guilty-atomic-energy-act-violations. In addition to a lengthy 18-month undercover operation, these cases generated over 6 terabytes of discovery. Mrs. Mascheroni was sentenced in August 2014 to a year and a day in federal prison, followed by three years of supervised release. Dr. Mascheroni is currently in federal custody awaiting sentencing. *See* Press Release, U.S. Attorney's Office, Dist. of N.M., Former Los Alamos National Laboratory Worker Sentenced for Violating Atomic Energy Act Violations (Aug. 20, 2014), *available at* http://www.justice.gov/usao/nm/press-releases/2014/Aug/316-%202014-08-20_mascheroni.html. While these cases did not uncover any involvement of the Venezuelan government or any Venezuelan officials, and no information was passed to any governmental officials, the potential threat the actions of the Mascheronis posed to the national security interests of the United States cannot be denied.

VI. Conclusion

While the SWB Districts conduct the majority of immigration-related prosecutions in the United States, the population, industry, Indian Country, and concentration of federal facilities that reside north of the 1,951-mile border demand that these offices concentrate on more than immigration offenses. These districts prosecute some of the most sophisticated white collar cases in the country, play a substantial role in combating violent and organized crime in the United States, and obtain impressive numbers of convictions against those who harm children, Native women, and other vulnerable populations along and within the Southwest border. In sum, the SWB Districts serve a critical function in helping the Department of Justice meet its stated prosecutorial priorities. ❖

ABOUT THE AUTHOR

❑ **Linda 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. ✠

The author would like to thank the people of the SWB Districts and especially Assistant U.S. Attorneys Christine Keller (AZ) and Jason Varnado (SDTX) for their input and assistance with this article.

Issues Presented by the Use of Confidential Informants in Investigating and Prosecuting International Criminal Activities on the United States-Mexico Border

Chris Blanton
Del Rio City Chief
United States Attorney's Office
Western District of Texas

Katherine Nielsen
Assistant United States Attorney
Western District of Texas

Although the border between the United States and Mexico legally separates two countries and two judicial systems, the criminal enterprises orchestrating international drug and human smuggling activities between these two countries often recognize no boundaries. The business model for these organizations requires that its criminal participants travel freely between the United States and Mexico to further their criminal ventures in both countries. Narcotics shipped from Central and South America must traverse the cartel-controlled border region of Mexico, where the drug owners are either cartel members themselves or pay tariffs to the cartels to cross through their territory. The drug trade involves couriers, load drivers, stash-house operators, mixers, cooks, and countless others before the retail product reaches its end user. Federal agents and prosecutors work diligently on the U.S. side of the border to prosecute criminal activities originating in, and controlled by, criminal participants in Mexico.

In many cases those prosecuting and investigating these international criminal activities must rely on confidential informants (CIs) willing to provide information in exchange for reduced sentences, favorable treatment, or other compensation in order to get a glimpse into this international criminal world operating on both sides of the border. The use of CIs can be fraught with difficulty. To be useful to the investigation, the CI must often continue to associate with the illicit activity, which requires prosecutors to balance the safety of the CI, the safety of the public, and the investigatory needs of the agency, while still focusing on the goal of criminal interdiction.

This article seeks to provide the border prosecutor with a perspective on the use of CIs and some of the important discovery and trial tactics to consider when using informants.

I. Who is a confidential informant?

The first hurdle facing a prosecutor who has been approached by an agent with the prospect of using an "informant" or "source" is to determine the particular relationship of said individual to the investigation of the case. The terms "confidential informant," "source," "source of information" (SOI), or "cooperator" are often used interchangeably to refer to a broad range of individuals. The Department of Justice has defined "confidential informant" as "any individual who provides useful and credible

information . . . regarding felonious criminal activities, and from whom . . . additional useful and credible information regarding such activities in the future" is expected to be obtained. THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS I.B.6 (2002), *available at* http://fas.org/irp/agency/doj/fbi/dojguidelines.pdf (AG Guidelines). A similar term, "confidential human source," is defined as

> any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information or relationship with the FBI warrants confidential handling.

THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF FBI CONFIDENTIAL HUMAN SOURCES I.B.7 (2006), *available at* http://fas.org/irp/agency/doj/fbi/chs-guidelines.pdf. These two types of informants, while distinctly labeled in their respective Guidelines, are more generally referred to as "CIs," "sources," and "SOIs." These individuals will be the main subject of this article and will be collectively referred to as "CIs."

CIs generally have a more-or-less formal relationship with the agency with which they work. They may have entered a formal agreement with the agency and will have been vetted and provided with rules and guidelines related to their conduct while acting as a CI, which will be discussed further below. *See* Memorandum from James M. Cole, Deputy Attorney Gen., Dep't of Justice 6–7 (Dec. 7, 2013) (Cole Memorandum) (requiring agencies to conduct a "suitability determination" of the CI prior to opening him or her as an informant, including assessing criminal history, immigration status, and history as an informant). CIs may either be paid or may be "working off" some potential criminal charges of their own, but they almost always stand to gain something personally from their cooperation. This personal gain makes them distinct from a mere "tipster" or witness, who provides law enforcement with information without prospective personal gain, but who wishes to remain anonymous for his own protection, either from retaliation or unwanted attention. *See United States v. McDowell*, 687 F.3d 904, 911 (7th Cir. 2012) (describing the difference between a "mere 'tipster' " and a " 'transactional witness' who participated in the crime charged against the defendant," like the Mexican cartel informant involved in that case).

CIs are distinct from "cooperating defendants," who are generally coconspirators with a defendant in a criminal case and who have agreed to testify against that coconspirator at trial in the hope of receiving a lesser sentence. *See* AG GUIDELINES I.B.7. The AG Guidelines also specifically define an SOI as a person who provides information to authorities because of their particular access, for example, as part of their occupation. *Id.* at I.B.8. However, the term SOI is also often used to describe a CI. While these definitions are designed to assist in determining which set of rules and protections may apply to a certain individual, in practice, because these terms are often used interchangeably, a prosecutor should have a full and candid discussion with agents about the nature of any CI, as different rules will apply regarding disclosure requirements and confidentiality. The AG Guidelines and the Cole Memorandum outline for the respective agencies the conduct required in dealing with CIs.

II. Getting involved with a CI during the investigation

While federal agents may have interacted with a CI for a lengthy period of time prior to seeking the indictment of a case, the prosecutor may not become aware of the CI's existence until he or she is presented with a charging decision. Even then, it may require pointed questioning regarding the reasons a suspect was stopped before the agent reveals the involvement of a CI. When a CI is presented to the prosecutor in this way, the prosecutor's job is fairly discrete: determine the strengths of the case, assess the reliability of the CI and the nature of his involvement, and decide whether his identity can or should be withheld based on the discovery and trial considerations outlined below. *See also* Steven Trott, *Criminals as Witnesses: DOs and DON'Ts*, ACLU (2007), *available at* https://www.aclu.org/files/pdfs/drugpolicy/informant_trott_dosanddonts.pdf.

Ideally, agents should consult with a prosecutor about the proposed use of a CI at the beginning of an investigation. In these proactive investigations, the AG Guidelines are instructive, both for Department of Justice (DOJ) policy on appropriate uses of CIs and also to determine whether the proposed use will be in violation of said policy and, consequently, open to challenge in court. There is nothing simple about these situations, and there are few bright lines. Balancing the safety of the CI and the community with the need to further the investigation is of particular concern when involving a CI in an investigative plan. Cole Memorandum, at 1 ("Law enforcement agents and prosecutors should be mindful whether the benefits of any operation continue to outweigh the potential public safety risks as the investigation moves forward."). CI-related investigations are generally considered by DOJ to be "sensitive investigations" and have been the subject of recent guidance to both prosecutors and agents. *See id.*

The Cole Memorandum states that "[t]he use of confidential informants is one of the most powerful tools of law enforcement." *Id.* at 6 (footnote omitted).

> Without informants, it would be difficult if not impossible to identify or penetrate the workings of criminal organizations and gain an understanding of their illegal activities . . . . [But] confidential informants with access to high-level criminals and their activities may be involved in criminal activities themselves and create a unique set of concerns.

Id. The Cole Memorandum provides specific guidance in risk assessment to both prosecutors and agents involved in investigations in which there is a likelihood of CI involvement in criminal activity. It requires agents to instruct CIs that they cannot "engage in criminal activity unless specifically authorized to do so." *Id.* at 7. The AG Guidelines allow CI participation in certain illegal acts, including drug trafficking, with prior permission. AG GUIDELINES III.C.2; *see also* Cole Memorandum, at 8. There is, however, a blanket prohibition on certain criminal conduct, including participation in acts of violence. AG GUIDELINES III.C.1. Even when illegal activity has been authorized, the AG Guidelines require the agency to closely supervise the activity and minimize adverse effects on others. *Id.* at III.C.5; *see also* Cole Memorandum, at 10 (including, as a law enforcement protocol, a process for first- and second-level supervisors to review otherwise illegal activities on a regular basis). These directives are particularly difficult to follow when the CI operates on the border and in Mexico, where U.S. agents cannot follow.

Investigative control can be diminished when a CI crosses the border into another sovereign nation, like Mexico, where U.S. law enforcement has only a limited presence and limited authority. However, the need to balance public and CI safety with the needs of the investigation does not cease, although it becomes more challenging. The ability of the CI to participate in Government-condoned illegal activity may become restricted once the CI passes into Mexico. *See* Cole Memorandum, at 10. In these instances, the prosecutor must not only seek supervisor and DOJ-level approval, but may be required to consult with the Office of International Affairs to ensure U.S. Government coordination with Mexican counterparts. *See id.* (requiring agencies to enact "[p]rocedures to ensure that requests to conduct otherwise illegal activities in a foreign country will . . . be approved following consultations with the Office of International Affairs and the U.S. Chief of Mission to that country"). Practically speaking, this means CIs operating in Mexico or another foreign country may be used to provide information to assist the Government in apprehension and indictment of criminals who cross back into the United States, but they may not actively participate in foreign criminal activity in furtherance of the investigation.

As a result of the difficulty of overseeing CI-related investigations that operate in Mexico, a prosecutor must openly discuss the use of CIs with agents, and the entire team must balance the safety of the CI and the public with the needs of the investigation. CIs who double-deal, or work with the criminal element covertly while purportedly working for the Government, hurt the investigation, cast doubt upon their credibility as a witness, and pose an extreme risk to public safety. Prosecutors and agents must make it clear to their informants that they must be forthcoming with agents, follow government instructions, and not participate in criminal activity unless they have received prior authorization to do so.

III. Charging decisions

In reactive cases, charging decisions will often precede the prosecutor's receipt of discovery. In cases involving a CI, however, strong consideration should be given to reversing that sequence. Why? Because sometimes it is necessary to forego immediate prosecution to protect the identity of a CI. Informant confidentiality traditionally derives from an agreement entered into between the agency and the source, without input from the prosecutor. Accordingly, agents are often surprised when, after consultation with the prosecutor, they realize the potential need to reveal their CI. The AG's Guidelines make clear that the prosecutor is "required to maintain as confidential the identity of any CI and the information the CI has provided, unless obligated to disclose it by law or court order." AG GUIDELINES I.F.2. What these agents fail to realize is that, given the involvement of the CI, neither the AG's directive nor the informant privilege—which allows the Government in certain instances to withhold from disclosure the CI's identity—may be adequate protection. To the extent that this affirmative duty to protect the CI's identity conflicts with the disclosure requirements of Rule 16 of the Federal Rules of Criminal Procedure or other obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972), the decision whether to charge may be affected. Thus, in some instances, a promise of confidentiality made by an agent may compel the Government to forego prosecution in order to honor the agency's representation to the source. Prosecutors and agents must be realistic about their ability to protect a CI's identity. As Judge Trott notes in his Informer Checklist, "there are no secrets, everything will come out in its worst possible light." Trott, at 1, *available at* https://www.aclu.org/files/pdfs/drugpolicy/informant_trott_dosanddonts.pdf.

As a result of often unrealistic expectations regarding the Government's ability to shield a CI's identity and involvement in an investigation, a candid conversation between prosecutor and case agent is often required to determine the right time to bring charges. For a variety of reasons, which may include instant gratification, the need to justify their investigation with arrests, or lack of experience, federal agents may push for early indictment or arrest of relatively minor targets, without considering the ramifications to the CI or the investigation. Also, when agents become impatient with a lack of progress in their own investigation, despite the likelihood of more complete and consequential future results, they may begin advocating for the arrest of low-level targets. Be mindful, however, that any arrest, even of the most insignificant player in a criminal enterprise, starts the clock on speedy trial rights and discovery. Therefore, prosecutors must discuss the timing of apprehensions and indictments with agents and their supervisors, weighing agency demand for progress, which is often only measured by indictments and arrests, against other risks and benefits.

Conversely, there may be a desire to expand the scope of the investigation beyond the point where indictment is viable in order to reach further targets or support more serious charges. This expansion occurs more frequently in proactive CI-related matters, where prosecutors and agents must determine when to shut down an investigation, file the indictment, and risk burning the CI. This decision can be a difficult one, and agents, prosecutors, and their respective supervisors should maintain open channels of communication to facilitate the determination. *See* Cole Memorandum, at 2–3, 5 (requiring both regular supervisory consultation regarding the progress of an investigation and continuous communication between prosecutor and agent "as to when an investigation should end"). In particular, a prosecutor has a duty to determine when the public safety risks of an investigation "outweigh the investigative and prosecutorial benefits." *Id.* at 5. When the need to protect the public outweighs the needs of the investigation, the decision is weighted heavily in favor of terminating the investigation and proceeding to prosecute the readily provable charges.

There is a constant interplay between CI safety and viability, investigative need, agency accountability, and discovery. Quite simply, agencies that rely heavily on CIs in proactive investigations frequently want to have their cake and eat it too. That is, they want to generate a continuous stream of arrests and indictments, but they want assurance that their CIs will not be burned in the process because

their CI is needed for the larger investigation. The role of the prosecutor is to emphasize patience and manage expectations because, although it is incumbent upon the prosecutor to maintain the confidentiality of the CI, the prosecutor will not be able to do so in the face of a court order.

IV. Discovery

The biggest pitfall in border prosecutions involving CIs or cooperating defendants is the discovery process. The flow of drugs and humans from Mexico into the United States, and cash and guns from the United States into Mexico, involves a complex network of criminal participants and organized gangs or cartels. Gangs and cartels make their money by controlling territories and claiming exclusive right to traffic through them. Others who wish to use their routes are taxed. These gangs require blood oaths of their members. When a load of contraband is intercepted by law enforcement, the gangs require the person that lost the load to show "paper." In the drug smuggling context, "paper" is a police report or some official document that clearly shows that the defendant innocently lost the load due to diligent police work, rather than because they have "flipped" and turned informant for the Government. Theoretically, an unwillingness to provide "paper" leads the gang to assume that their courier flipped, and violent consequences may result.

The gangs and cartels controlling the Southwest border trade in contraband and rely heavily on their blood oaths. Coconspirators who cannot prove their loyalty after losing a load with "paper" are, at the very least, threatened, and confirmed informants may be killed. The threat to family and friends of informants living in Mexico often hangs even more heavily over cooperators. Loyal gang defendants play "chicken" with the criminal justice system, risking life in prison at trial, rather than taking a plea deal, so that the Government must continue to provide discovery and potentially reveal the identities of informants. Prosecutors and agents constantly hear tales of criminal defense attorneys or their staffs who either do not fully appreciate the consequences of turning over discovery to their client or his family or, more problematically, who corruptly sell documents and presentence investigation reports (PSRs) that reveal informants to gangs and cartels. Prosecutors must be constantly vigilant during the discovery process to ensure anonymity; simply turning over unredacted discovery may have grave consequences.

As the following discussion shows, the prosecutor's first priority is to completely avoid disclosure regarding a CI. If that fails, the focus should be to minimize disclosure and, if necessary, to shield the informant in the aftermath. Border prosecutors must become skilled in employing discovery techniques to protect CIs, including watermarking their discovery, obtaining protective orders, and timing the release of information so that they comply with the discovery rules while still besting loyal gang members in their game of "chicken."

A. Pre-plea discovery

Rule 16 of the Federal Rules of Criminal Procedure requires that the Government provide certain discovery to a defendant in a criminal case, including documents and other information that is "*material* to preparing the defense." FED. R. CRIM. P. 16(a)(1)(E)(i) (emphasis added). It is this provision, along with a conglomeration of claims related to Rule 26.2, 18 U.S.C. § 3500, *Brady*, *Giglio*, and a host of constitutional rights, that commonly forms the basis for defense demands for discovery related to CIs. However, most of these bases are not pretrial rights and are, thus, at least temporally, limited in that they cannot be used to force pretrial disclosure. For example, the Supreme Court has held that the Constitution does not require the Government to provide the defense with material impeachment evidence regarding CIs prior to entering a plea agreement with the defendant. *United States v. Ruiz*, 536 U.S. 622, 629–30 (2002) ("[T]he Constitution does not require the prosecutor to share all *useful* information with the defendant." (emphasis added)); *see also Weatherford v. Bursey*, 429 U.S. 545, 559 (1977) ("There is no general constitutional right to discovery in a criminal case[.]"). As a result, if, as is frequently the case, a

defendant pleads guilty prior to trial, the identity of a CI can generally be entirely protected from disclosure.

B. Informant's privilege

If the defendant has failed to plead, or defense counsel has demanded discovery regarding a CI, then the border prosecutor may seek some protection in the so-called "informant's privilege." This is a common-law doctrine generally allowing the Government to withhold information that would identify a CI, except under certain circumstances. The seminal case recognizing the "informant's privilege" is *Roviaro v. United States*, 353 U.S. 53, 58–61 (1957). In that case, the Supreme Court explained that the privilege was originally designed to encourage citizens to recognize their obligation to tell law enforcement what they know about the commission of a crime, by protecting their anonymity and shielding the informer "from those who would have cause to resent his conduct." *Id.* at 60 n.8. This "privilege" provides federal agents and prosecutors with a certain amount of confidence in assuring CIs that their identity will remain confidential in many circumstances, particularly when their participation consists only of providing information. However, in practice, the value of a CI lies more in the things he or she can do to further an investigation, such as performing drug buys and transporting illegal proceeds, rather than the things he can tell the investigators. When CIs move from merely providing information to actively participating in criminal activities on behalf of the agents, the informant's privilege weakens. As the Supreme Court stated,

> The scope of the privilege is limited by its underlying purpose. Thus, where the disclosure of the contents of a communication will not tend to reveal the identity of an informer, the contents are not privileged. Likewise, once the identity of the informer has been disclosed to those who would have cause to resent the communication, the privilege is no longer applicable.

Id. at 60 (citations omitted).

The Court recognized that the privilege was further limited by the "fundamental requirements of fairness." *Id.* Hence "[w]here the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." *Id.* at 60–61. The *Roviaro* Court recognized that, particularly in narcotics-related cases, the privilege increasingly was being used "to withhold the identity of an informer who helped to set up the commission of the crime and who was present at its occurrence." *Id.* at 61 (footnotes omitted). In such cases, the Court noted, the privilege generally must give way, as it did in that case. The Court held that the Government could not withhold the identity of its *non-testifying* informant, who in that case was the only other participant involved in the drug transaction and was, therefore, the only possible witness other than the accused himself, that the defendant had as to certain elements of the crime. *Id.* at 64.The CI in that case helped set up the crime and played a significant role. As a result, his testimony, the Court opined, might have disclosed an entrapment defense or shown a lack of knowledge on the defendant's part. *Id.* at 65.

In his dissent, Justice Clark pointed out the difficulty with the position taken by the *Roviaro* Court in relation to prosecuting drug crimes:

> Because drugs come in small pills or powder and are readily packaged in capsules or glassine containers, they may be easily concealed. They can be carried on the person or even in the body crevasses where detection is almost impossible. Enforcement is, therefore, most difficult without the use of "stool pigeons" or informants. Their use has long had the approval of the courts. To give them protection governments have always followed a policy of nondisclosure of teir [sic] identities. Experience teaches that once this policy is relaxed . . . its effectiveness is destroyed. Once an informant is known the drug traffickers are quick to retaliate. Dead men tell no tales.

Id. at 66–67 (Clark, J., dissenting).

The situation presented in *Roviaro*, though over 50 years old, still represents the struggle that agents, prosecutors, and courts have with discovery in relation to CIs. There is a sliding scale of protection that the Government can offer a CI. On one end, the mere "tipster" will generally enjoy full protection of his identity. At the other, the true CI, who is involved in the commission of the crime, can count on less protection. A defendant may compel the Government to disclose an informant's identity by clearly showing that the disclosure would be "relevant and helpful" to his defense. *Cf. United States v. Jiles*, 658 F.2d 194,197 (3d Cir. 1981) ("The burden is on the defendant to show the need for disclosure."); *see also United States v. Scafe*, 822 F.2d 928, 933 (10th Cir. 1987) (to meet the defendant's burden, he or she must show more than "mere speculation about the usefulness of an informant's testimony").

Over time, courts have developed several processes to help decide when the public's interest in nondisclosure of a CI's identity outweighs the defendant's interest in obtaining the information. Some use a three-part test to make the determination, focusing the inquiry on (1) "the extent of the informant's participation in the criminal activity," (2) "the directness of the relationship between the defendant's asserted defense and the probable testimony of the informant," and (3) "the government's interest in nondisclosure." *United States v. Tenorio-Angel*, 756 F.2d 1505, 1509 (11th Cir. 1985); *see also United States v. Flores*, 572 F.3d 1254, 1265 (11th Cir. 2009) (reviewing the district court's application of the *Tenorio-Angel* three-part test); *United States v. Ayala*, 643 F.2d 244, 246–47 (5th Cir. 1981). Other courts maintain that the trial judge may not order disclosure of a CI's identity unless the defendant has demonstrated that the testimony of the CI would be material to the determination of the case. *See United States v. Harrington*, 951 F.2d 876, 877 (8th Cir. 1991). Still other courts have held that the defendant must show that the CI was a participant in, or witness to, the charged offense in order to compel disclosure. *See United States v. Mangum*, 100 F.3d 164, 172 (D.C. Cir. 1996).

It must be remembered that *Roviaro* applies only in the context of a CI that *will not testify* at trial, but who the defendant has shown might have information helpful in establishing, for example, an entrapment defense or a lack of knowledge on the defendant's part. The defendant bears the burden of establishing a potential defense about which the CI may provide material information. But, if the defendant meets this burden, as may be the case with a non-speculative entrapment defense, the CI's identity is in jeopardy. *See, e.g., United States v. Arechinga-Mendoza*, 566 F. App'x 713, 718 (10th Cir. 2014) (remanding case for *in camera* proceedings where defendant asserted a need for non-testifying CI information in establishing an entrapment defense); *but see United States v. Mendoza-Salgado*, 964 F.2d 993, 1000–01 (10th Cir. 1992) (declining to compel disclosure of a CI's identity where the defendant failed to do more than speculate about the possible relevance of the CI's testimony).

The *Roviaro* tests described above all revolve around the defendant's need. However, on the border, the CI and agents will point to the heightened retaliatory danger to the CI and/or his or her family in Mexico as the paramount reason for nondisclosure, as well as reluctance to "burn" an informant they want to continue to use in ongoing investigations. Some courts have held that proof of a threat to CI safety may properly be considered as part of the Government's interest in nondisclosure. *See, e.g., Flores*, 572 F.3d at 1265 (finding no error with the trial court's decision not to reveal CI identity based, in part, on the Government's "legitimate interests in nondisclosure, including the informant's safety and the informant's involvement in other ongoing investigations"); *United States v. Ibarra*, 493 F.3d 526, 532 (5th Cir. 2007) (finding the district court did not err in ruling against disclosure of CI identity based, in part, on the Government's "substantial interest in nondisclosure because there could be a 'real risk' to the safety of the informant and his family and because disclosure could also jeopardize other ongoing criminal investigations"); *United States v. Tenorio-Angel*, 756 F.2d 1505, 1510 (11th Cir. 1985); *United States v. Ayala*, 643 F.2d 244, 247 (5th Cir. 1981). On the other hand, some courts have held that "it is error of constitutional dimension to deny disclosure solely because of the potential danger to the informant." *United States v. Scare*, 822 F.2d 928, 934 (10th Cir. 1987); *see also United States v. Ordonez*,

737 F.2d 793, 809 (9th Cir. 1984) ("[I]t was error of constitutional dimension to deny disclosure solely because of the potential danger to the informer.").

If the defendant demands the disclosure of the CI's identity and makes the required showing of need, the prosecution may request, and the trial court may, and in some cases must, hold an *ex parte, in camera* hearing to determine the relevant value of an informant's testimony. *See United States v. Tenorio-Angel*, 756 F.2d 1505, 1511 (11th Cir. 1985); *see e.g.*, *Alvarez v. United States*, 525 F.2d 980, 982 (5th Cir. 1976) (stating that an *in camera* hearing is an appropriate way to determine whether a CI's identity is material to the defense and must be disclosed); *United States v. Anderson*, 509 F.2d 724, 729–30 (9th Cir. 1974) (finding that an *in camera* hearing was a proper way for trial judge to determine whether an informant's identity must be revealed to defense); *see also United States v. Rutherford*, 175 F.3d 899, 902 (11th Cir. 1999) (remanding to the district court to conduct an *in camera* hearing to determine if CI information would help defendant establish misidentification defense); *United States v. Ramirez-Rangel*, 103 F.3d 1501, 1508 (9th Cir. 1997) (holding that the trial judge erred in not conducting an *in camera* hearing before denying a motion to disclose CI identity); *United States v. De Los Santos*, 810 F.2d 1326, 1329, 1335 (5th Cir. 1987) (holding that the defendant was not denied his Sixth Amendment rights to a public trial and to confront his accusers when the trial court held an *in camera* hearing, at which only the judge and prosecution were present, to determine whether to disclose an informant's identity).

The informant's privilege is useful, but limited. It should be noted that, while the identity of a CI may be shielded under the privilege, that of a cooperating defendant is not. Nor does the privilege extend to information or communications from the informant that would not reveal his identity. *See Roviaro*, 353 U.S. at 60. Furthermore, under circumstances like those in the *Roviaro* case, the Government may actually be responsible for ensuring that the defendant has an opportunity to interview non-testifying, paid CIs who will not be called by the Government, but who may be potential witnesses for the defense. *See United States* v. *Barnes*, 486 F.2d 776, 779–80 (8th Cir. 1973); *United States v. Hayes*, 477 F.2d 868, 871 (10th Cir. 1973); *see also Velarde-Villarreal v. United States*, 354 F.2d 9, 13 (9th Cir. 1965) (suggesting the rationale of potentially unreliable character of paid informants and the possibility of entrapment). An additional layer of complexity is added on the border, where CIs are often not U.S. citizens. Assuming that the defendant has made an appropriate showing of need, the Government may have an affirmative responsibility to ensure that an alien witness is not deported before defense counsel can interview him. *See United States v. Henao*, 652 F.2d 591, 593 (5th Cir. 1981) (deportation of an alien witness prior to defense interview may have deprived the defendant of his right to compulsory process and due process); *see also United States v. Avila-Dominguez*, 610 F.2d 1266, 1269 (5th Cir. 1980) ("[A] criminal defendant's constitutional rights are violated if an alien witness is deported before the defendant is given an opportunity to interview the witness."); *United States v. Tsutagawa*, 500 F.2d 420, 423 (9th Cir. 1974) ("A defendant has the right to formulate his defense uninhibited by government conduct that, in effect, prevents him from interviewing witnesses . . . ."). As a result of the numerous exceptions to the informant's privilege, disclosure of at least some information regarding a CI may be unavoidable, in which case some of the protective techniques noted below may become important.

C. Production, protective orders, and watermarking

If an *in camera* hearing has been held and the court determines that information pertaining to the CI must be disclosed to the defense, there are still ways to help prevent the CI's identifying information from falling into the wrong hands. Rule 16(d)(1) of the Federal Rules of Criminal Procedure provides that the court may, "for good cause," restrict discovery or inspection or "grant other appropriate relief." FED. R. CRIM. P. 16(d)(1). If the court heard the Government's *in camera* arguments and still ruled that the identity of or other identifying information about a CI must be disclosed, the prosecution may, and by policy must, consider requesting a protective order if disclosure of the information might compromise the safety of an informant. *See* Memorandum from David Ogden, Deputy Attorney Gen., Guidance for Prosecutors Regarding Criminal Discovery to Dep't Prosecutors (Jan. 4, 2010), *available at* http://www.

justice.gov/dag/memorandum-department-prosecutors; *see also*, *United States v. Pelton*, 578 F.2d 701, 706–07 (8th Cir. 1978) (court properly issued a protective order denying defendant access to recordings that disclose the identity of cooperating sources based on concern for their safety); *United States v. Anderson*, 509 F.2d 724, 729–30 (9th Cir. 1975) (stating that a defense attorney should be placed "under enforceable orders against unwarranted disclosure of the evidence that he has heard" regarding informant's identity (citing *Alderman v. United States*, 394 U.S. 165, 185 (1969))).

In a world where "paper" may mean death for an informant, a protective order only works if the defendants and their attorneys can be held accountable for violating the order. Discovery and PSRs are as much commodities in the drug business as cash. It is not unprecedented for prosecutors in border locations to find their case discovery in the hands of codefendants, or even published in newspapers across the border. *See* Miguel Vargas, *Usó la DEA a la Municipal para secuestrar a juarense* (DEA used the Municipal Police to kidnap a Juárez citizen), NORTE DE CIUDAD JUÁREZ, Jan. 8, 2014, at 1A (showing a picture of discovery documents from a U.S. federal court case in a Mexican article about U.S. law enforcement agents).

When disclosure of documents containing information about a CI is required, prosecutors have several options to deal with sensitive materials, foremost being redaction. Any information related to the CI that is not specifically required to be turned over by court order or other prosecutorial obligation should be removed prior to production. Judicious redaction is the frontline against unwanted disclosure. Additionally, prosecutors can watermark discovery that must be produced to the defense, uniquely marking each document so that if it gets out, it is traceable back to a specific defendant and his attorney. This way, the court can hold accountable those who violate a protective order. Over time, this has the effect of preventing disclosure. Prosecutors may also make certain documents available only to the defense attorney, and only at the prosecutor's offices.

These examples represent only a few of the many creative ways to monitor discovery. The lesson is that the information contained in discovery can reveal, even inferentially, the identity of a CI, and the prosecutor's obligation to protect a CI continues through the discovery process and beyond.

D. CI file review and other agency issues

To ensure compliance with ethical obligations and court-ordered discovery, a prosecutor must be aware of all the information in the possession of the Government related to a CI; that includes the agency's CI file. Each federal agency that has a formal relationship with a CI will maintain a file containing all of the materials related to that CI and his or her conduct with, and on behalf of, the Government. Although the agencies have internal policies on who has access to the files, it is essential for the prosecutor handling the case involving that CI to review this file, both in anticipation of trial and to comply with *Brady* and *Giglio* obligations. The AG Guidelines provide that the prosecutor will maintain the confidentiality of the information contained in that file, and ultimately all information regarding CI identity. AG GUIDELINES I.F.2. If the prosecutor finds that information regarding the CI, or contained in the agency's CI file, must be produced to the defense or in open court, the prosecutor must discuss this with the agency in advance of disclosure and provide the agency the opportunity to state its position. *Id.* at I.F.2.d. The AG Guidelines further outline the procedures for dealing with a dispute between an agency and the Criminal Division, if one should arise. *Id.* at I.G.

V. Protecting CI identity at trial

Once discovery and plea negotiations have concluded and the defendant decides to proceed to trial in a case involving a CI, a prosecutor is faced with some difficult decisions. An initial consideration is whether the CI will make a good witness at all, as they may come with criminal baggage that makes them unattractive to the jury. The CI will also likely express great hesitation, or even refuse to testify, based on fear of reprisal, both against himself and, as is often the case along the border, against family

members who live in Mexico. The agents may likewise object to "burning" the CI, usually due to a desire to use the source in ongoing or future investigations.

In the face of this type of resistance, the surest option, if trial is unavoidable and the identity of the CI must remain secret, is to move the court to dismiss the case. Short of this drastic step, courts have allowed certain other methods of safeguarding the identity of, or identifying information about, a CI who fears retaliation by the defendant or the criminal organization of which he or she is a part. These methods include delayed disclosure, anonymous testimony, and disguise. *See, e.g.*, Lisa I. Karsai, *You Can't Give My Name: Rethinking Witness Anonymity in Light of the United States and British Experience*, 79 TENN. L. REV. 29, 38–56 (2011) (providing an overview of cases in which courts have allowed anonymous and disguised testimony).

A. Delayed disclosure

The least legally controversial way to provide some protection of a CI's identity is delayed disclosure. Nothing requires the Government to provide advance notice of witnesses to the defendant. *See, e.g.*, *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977) (noting that prosecution need not reveal before trial names of witnesses who will testify unfavorably); *see also United States v. Edwards*, 47 F.3d 841, 843–45 (7th Cir. 1995) (finding no impropriety, based on fear of retaliation, in delayed disclosure of identity of government witness until third day of trial, and noting that neither the Constitution nor Rule 16 requires pretrial disclosure of prosecution witnesses); *United States v. Edelin*, 128 F. Supp. 2d 23, 32–34 (D.D.C. 2001) (allowing delayed disclosure of names of government witnesses and related information, due to threat to witnesses's safety).

Delaying disclosure of witness identity until trial may be effective in preventing witness tampering, but it provides little protection from post-testimony retaliation. It is also likely to cause interruption to proceedings if defense counsel seeks a continuance to discover impeachment evidence and prepare cross examination. For the foregoing reasons, in border cases, delayed disclosure is likely to be insufficient to address concerns regarding disclosure of CI identity, although it is a useful strategy when the prosecutor suspects the defendant is merely prolonging proceedings in order to see what the Government will be forced to reveal as trial nears.

B. Anonymity

A trial option that provides greater protection to the CI than simply postponing disclosure is seeking the court's approval to allow the CI to testify anonymously. *See generally* Jason Buch, *Snitch tells of spying on Zetas*, SAN ANTONIO EXPRESS-NEWS (Jan. 20, 2012) (discussing the testimony of a DEA informant under a false name during trial involving a Zetas gang member). Courts have approved three general types of witness anonymity. First, in certain cases, witnesses have been allowed complete anonymity—denying the defendant, defense counsel, and the public, the real name and personal identifying information of the witness. *See United States v. Zelaya*, 336 F. App'x 355, 358 (4th Cir. 2009) (per curiam) (granting complete anonymity to a government witness in a RICO prosecution of MS-13 gang members based on "actual threat" to witnesses); *United States v. Borda*, No. 96-4752, 1999 WL 294540, at *7 (4th Cir. May 11, 1999) (unpublished) (upholding complete non-disclosure of CI identity where the Government made a showing that disclosure would endanger the CI and his family); *Miller v. United States*, 28 F.3d 1213, 1213 (6th Cir. 1994) (unpublished) (granting complete anonymity to CI who testified at trial under a pseudonym, based on threats against the CI). Second, some courts have allowed restricted disclosure to defense counsel only for pretrial investigation under the terms of a protective order. *See United States v. Celis*, 608 F.3d 818, 826 (D.C. Cir. 2010) (per curiam) (upholding restricted disclosure of witnesses' true identities to defense only, and allowing witnesses to testify under pseudonyms where actual threat was shown in drug trafficking case involving Fuerzas Armadas Revolucionaras de Colombia); *see also United States v. Alaniz*, 726 F.3d 586, 608 (5th Cir. 2013) (finding

no violation of Confrontation Clause in Mexican drug cartel case where two CIs were permitted to testify anonymously, with limited disclosure of true identity and impeachment information to defense counsel). Finally, in order to maintain public anonymity, courts have permitted witnesses to testify under false names and/or closed the courtroom to the public during testimony, while still revealing the true identity of the witness to the defendant and defense counsel. *See United States v. Maso*, No. 07-10858, 2007 WL 3121986, at *4 (11th Cir. Oct. 26, 2007) (finding no violation of defendant's right to a public trial where the trial court conducted an *in camera* hearing regarding CI identity and allowed the CI to testify using a pseudonym, based on fear of safety of the CI and his family in Mexico); *see also United States v. Jesus-Casteneda*, 705 F.3d 1117, 1121 (9th Cir. 2013) (suggesting that the courtroom could be sealed to protect a testifying CI's identity from the pubic); *but see* DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-5.150 (2014) (explaining requirements for court closure and requiring federal prosecutors to obtain prior authorization from the Deputy Attorney General before moving for the closure of any criminal proceeding).

While potentially useful, each of these three types of anonymity has similar drawbacks. First, in order to withstand a defendant's discovery and Sixth Amendment challenges to witness anonymity, the Government must make a specific showing of legitimate fear of reprisal. The recent Tenth Circuit case, *United States v. Gutierrez de Lopez*, No. 13-2141, 2014 WL 3765720 at *10 (10th Cir. Aug. 1, 2014), is instructive. The district court in that case allowed two CIs to testify anonymously for their own safety based on the Government's assertion of Mexican drug cartel involvement in the matter. *Id*. The prosecutor recounted to the court another case in which a cooperating witness was decapitated in retaliation for his cooperation. The defendant challenged the anonymity, asserting that his Sixth Amendment Confrontation Clause rights had been violated because he had been denied the opportunity for effective cross examination, even though the Government had provided the defense with background information on the CIs, including criminal histories, compensation figures, and immigration status. The Tenth Circuit determined that the Government had, in fact, failed to make an adequate showing to justify withholding the CI's identities because it did not produce "specific evidence of a threat" to the CIs. *Id.* at *16. However, the *Gutierrez de Lopez* court upheld the trial court's ruling because the defendant was not deprived of the opportunity for effective cross examination based on the impeachment material provided. *Id.* at *17; *see also United States v. Alaniz*, 726 F.3d 586, 610 (5th Cir. 2013) (identifying weakness in the Government's position based on failure to provide specific evidence of legitimate fear of reprisal). *Gutierrez de Lopez* points out the inadequacy of making general statements about the risk to a CI or witness based solely on the assertion that drug cartels in Mexico are dangerous and vindictive, which frequently will be the only articulated basis for the CI's fear.

Additional drawbacks to anonymous testimony include, as noted above, a challenge by the defendant on Sixth Amendment grounds, such as the confrontation clause and right to a public trial, and, practically the most important, the fact that even testifying under a false name, the CI will still be visible to the defendant. As a result of the latter concern, anonymous testimony is only really useful as a stand-alone technique where the defendant does not know the CI. If the defendant would recognize the CI by sight or name, then anonymity may be useful only if employed with an in-court disguise.

C. Disguise

In *United States v. Jesus-Casteneda*, 705 F.3d 1117, 1121 (9th Cir. 2013), the Ninth Circuit held, in a matter of first impression, that a CI's testimony in disguise did not violate the defendant's Sixth Amendment confrontation rights. In that case the CI testified at trial wearing a wig and mustache to help protect his identity out of fear of reprisal form the Sinaloa Cartel. The court ruled that the light disguise in this case was "necessary to further an important state interest," protecting the CI's identity, and the reliability of the CI's testimony was otherwise assured. *Id.* at 1120–21. The Ninth Circuit's ruling was consistent with a similar ruling by the Second Circuit in *Morales v. Artuz*, 281 F.3d 55 (2d Cir. 2002). The *Morales* court held that permitting a witness to testify in dark sunglass at trial did not violate the

defendant's right to confront the witness where the jury had the "opportunity to assess the [witness's] testimony" and credibility through demeanor, speech, and body language. *Id.* at 60–62; *see also* Lisa I. Karsai, *You Can't Give My Name: Rethinking Witness Anonymity in Light of the United States and British Experience*, 79 TENN. L. REV. 29, 56–57 (2011). As with anonymous testimony, disguised testimony is of limited use, but combined, they can provide a measure of protection to a CI who is not intimately known to the defendant or other potential court spectators.

D. *Brady*/*Giglio* responsibilities

If the CI testifies publicly, anonymously, and/or in disguise, or even if he or she does not testify at all, a prosecutor always has a duty to provide exculpatory and impeaching information in compliance with *Brady* and *Giglio*. If the CI testifies under a pseudonym or in disguise, as noted above, this duty can take the form of providing information such as criminal histories, government compensation, immigration status, and incentives to testify, as in any case.

A particular trap for the unwary exists in cases involving a CI where either the CI does not testify at trial, as in the *Roviaro* case, or where a CI's involvement is not known to the prosecutor. In such cases a prosecutor may still have an obligation to provide the defense with impeaching information about the CI. Even if the Government prevails in its efforts to maintain the confidentiality of an informant, the Supreme Court has held that statements of, or information related to, a non-testifying government informant may be considered exculpatory or favorable to the defense and require disclosure if they call into question the defendant's guilt or the thoroughness of the Government's investigation. *See Kyles v. Whitley*, 514 U.S. 419, 445 (1995). In *Kyles* a police informant made numerous inconsistent statements to police officers, had a potential interest in setting up the defendant, and might, in fact, have been the perpetrator of the crime involved, but police failed to further investigate and failed to provide the balance of this information to the prosecutor. The prosecutor, in turn, failed to provide this information to the defense. The informant did not testify. The court held that the information was nevertheless required to have been turned over because it raised the opportunity for the defense to attack the probative value of physical evidence and the thoroughness and good faith of the police investigation. *Id.* at 445. Hence, the information was potential *Brady* and *Giglio* material. It would also have offered the defense the opportunity to call the informant as a witness. *See id.* at 421, 445 (noting that the prosecutor remains responsible, regardless of any failure by the police to bring favorable evidence to the prosecutor's attention).

A prosecutor must thoroughly explore the evidence with case agents and discover *any* CI or source participation therein. This chore may be more difficult than it sounds, as agents may not realize the significance of the information or attempt to shield the prosecutor from knowledge of CI participation because they fear the prosecutor will do exactly what *Kyles* dictates: disclose that fact to the defense.

VI. Post-trial considerations

Assuming the investigation is complete and either the defendants have pleaded guilty or proceeded to trial and successfully been convicted, there is still no rest for the prosecutor involved with a border CI. The specter of CI safety continues to haunt the Government and, in fact, can become more complicated when the case is concluded, particularly where, as in most cases on the border, the CI is not a U.S. citizen.

A. Target defendant plea agreements and PSRs

Some of the more routine administrative tasks of the criminal prosecutor can require heightened attention in cases involving CIs. With respect to factual recitations in plea agreements and PSRs prepared for defendants against whom a CI has cooperated, care should be taken to ensure that neither the name nor any identifying information regarding the CI is included. This task is particularly important with

respect to PSRs, as these are generally not prepared by the prosecutor's office. This caution is equally valid even if the identity of the CI was ultimately revealed to the defendant against whom the CI cooperated. Although these documents are generally not available to the public, it is well known on the border that cartels and criminal organizations routinely obtain copies of PSRs. As a result, information about cooperation with law enforcement may become known, which can obviously be detrimental to CI safety.

B. CI plea agreements and 5K1.1 motions

While the same cautions regarding inclusion of sensitive material in court documents discussed above also apply to the CI's own plea agreement and PSR, additional factors must be considered in relation to a CI's plea agreement and motions for reduction in sentence under § 5K1.1 of the U.S. Sentencing Guidelines. U.S. SENTENCING GUIDELINES MANUAL § 5K1.1 (2013).

First, where a CI who is also a criminal defendant is an illegal alien and has not been promised any kind of legal status as part of his cooperation agreement with the Government, the prosecutor should consider adding language to the plea agreement indicating that the CI understands that return to his home country at the conclusion of sentencing will result and that contesting deportation will be in violation of his plea agreement. *See Perez-Guerrero v. U.S. Atty. Gen*., 717 F.3d 1224, 1227 (11th Cir. 2013) (acknowledging inclusion of language in plea agreement by which the cooperator agreed "that he would be removed to Mexico after the completion of his sentence and that he would be in violation of the plea agreement if he contested his deportation on any grounds other than that he faced death or injury in Mexico as a result of the cooperation he provided to the United States"). This ensures that there will be no misunderstanding about consideration for cooperation with the Government and can provide valuable evidence in later proceedings.

Second, the prosecutor should exercise extreme caution in drafting motions under § 5K1.1. While these recommendations are welcomed by the CI who has also been charged with a crime and likely form the basis for the cooperation, they can prove problematic for two reasons. The first concern is the same as with PSRs: despite being sealed, they can become known to others. The second problem, which is entirely peculiar to the alien CI, is that any indication of threat to the CI or danger he faces as a result of cooperation, although persuasive to the court in granting the motion, may be used in later proceedings by the CI to resist removal based on some form of state-created danger. *See Ramirez-Peyro v. Holder*, 574 F.3d 893, 901 (8th Cir. 2009) (holding that an alien government informant could not be deported to Mexico under the Convention Against Torture because he faced torture or death at the hands of drug cartels about which he had informed, either through or with the acquiescence of the Mexican authorities).

Finally, a prosecutor must also take care to review the PSR of a CI who pleaded guilty to a federal offense to ensure that the information contained therein does not contradict testimony given at trial or contain previously undisclosed exculpatory or impeaching evidence material to another defendant's case. *Brady* and *Giglio* created continuing obligations on the part of the Government. Therefore, if the PSR does contain such information, the prosecutor must disclose it to the defense. *See Brady v. Maryland*, 373 U.S. 83, 87 (1963). However, most courts provide the opportunity to review such information *in camera* prior to making any disclosure. *See, e.g.*, *United States v. Miller*, 698 F.3d 699, 705 (8th Cir. 2012) (acknowledging that a district court should conduct an *in camera* review of a cooperating witness's PSR if the Government recognizes the possibility that the PSR contains *Brady/Giglio* information and so requests); *United States v. Carreon*, 11 F.3d 1225, 1238 (5th Cir. 1994) (recognizing the need to balance protecting the confidentiality of PSRs with the right of the defendant to access exculpatory and impeachment evidence by holding *in camera* hearing to review cooperating witness PSRs).

VII. Conclusion

A myriad of potential complications may arise when using CIs on the United States-Mexico border, but ask any agent, and they will tell you CIs are invaluable in this region where politics, poverty, and crime converge. When employed with foresight and caution, a good CI can help dismantle a cartel and win another small battle in the war against the drug trafficking organizations that plague the border. It is hoped that the tools and techniques discussed in this article will assist prosecutors to avoid some of the pitfalls inherent in working with CIs, while still successfully incorporating their contributions in cross-border cases. Although prosecutors and agents must be ever vigilant regarding risk assessment when employing an informant in a border investigation, CIs are often the best source of information about cartel activity available to federal law enforcement. ❖

ABOUT THE AUTHORS

❑ **Chris Blanton** is the City Chief of the U.S. Attorney's Office in the Del Rio Division of the Western District of Texas. Mr. Blanton began his career with the Department of Justice in 2006, during which he has served as a Criminal Assistant U.S. Attorney in both the El Paso and Del Rio Divisions of the Western District of Texas before becoming a supervisor in 2012. ✠

❑ **Katherine Nielsen** has been an Assistant U.S. Attorney in the Del Rio Division of the Western District of Texas since 2012. Prior to joining the office, she was in private practice, with a focus in entertainment and corporate law. She clerked for the Honorable Harris L Hartz, Circuit Judge, U.S. Court of Appeals for the Tenth Circuit, and the Honorable Mark E. Fuller, District Judge, U.S. District Court for the Middle District of Alabama. ✠

Preying on Hope—The Case Against Notario Fraud

Andy Choate
Assistant United States Attorney
Immigration Unit Chief
District of Utah

As news of immigration reform and amnesty programs dominate national headlines, those in the country without legal status have reason for hope. Unfortunately, until action is taken to address immigration legislation, hope is all that the undocumented population has. Sensing this, dishonest immigration consultants, often called "notarios," prey on vulnerable immigrants hoping to legalize their immigration status. STOP NOTARIO FRAUD, http://www.stopnotariofraud.org/. The number of cases prosecuting these fraudsters has dramatically increased in recent years. Those promulgating the fraud come from a variety of backgrounds, including notaries, those practicing law without a license, those impersonating employees of the Department of Homeland Security (DHS), those claiming an inside connection to DHS employees, and worse yet, licensed attorneys committing fraud. Given the variety of contexts in which this type of immigration fraud has occurred, prosecutors have been challenged to find the correct charges to apply to any particular case. However, several theories have been used successfully to prosecute these cases.

I. Charging options

A. Wire fraud: 18 U.S.C. § 1343

As in many fraud cases, the wire fraud statute has many helpful applications in the notario fraud context. Given that "wires"—including texts, emails, and other types of electronic and cell phone communications—have become the primary method of communication in today's society, the wire fraud statute has been the most valuable tool for prosecutors seeking to charge those committing notario fraud. Around the country, there are several cases of perpetrators communicating directly with victims via text messaging or related technology. In this context, the elements of the wire fraud statute can be fulfilled by proving that the perpetrator devised a scheme to defraud and sent a wire communication, or caused wires to be sent, in an attempt to execute the fraud. Even perpetrators who will not discuss the substance of the agreements have been known to send text messages to victims to set up meetings or request money, which can provide the evidence necessary for wire fraud counts.

B. Mail fraud: 18 U.S.C. § 1341

Many of the perpetrators will engage in the mailing back and forth of immigration applications or passport photos to avoid meeting the victims in person. Some perpetrators will even mail the victim's fraudulent application to U.S. Citizenship and Immigration Services. If this factual scenario presents itself, an application of the mail fraud statute will have great importance.

C. Impersonation of a public employee: 18 U.S.C. § 912

Impersonation charges also play an important role in prosecuting notario fraud. Many times, perpetrators will assume the role of a governmental employee or official through the use of badges, uniforms, or agency embroidered clothing in order to gain credibility and money from the victims. These

cases are especially important given that each of these cases can erode the public trust that governmental agencies struggle to maintain in immigrant communities. A helpful source of information to establish whether an individual is employed for a particular agency is the Office of the Inspector General (OIG) for that department. Work with the OIG to confirm whether your target is an actual employee, as purported. As in other cases, the use of certificates of non-existence for employee records has fallen out of favor due to hearsay issues. These hearsay issues can be avoided by bringing in the actual employee that performed the search for the employee records to testify.

D. Alien smuggling: 8 U.S.C. §1324

Traditional alien smuggling charges can also be helpful in the notario fraud context. The applicable statute, 8 U.S.C § 1324, requires that the perpetrators encourage and induce illegal aliens to come to, or reside illegally in, the United States. A brief discussion with your victims can be a valuable source of information and evidence when contemplating these charges. A fake green card or naturalization document is the vehicle through which these immigrants will seek to work and reside in the United States. Many victims will also engage in frank discussion with the perpetrators of the fraud and ask pointed questions, such as "can I work legally with this document" or "can I come and go from the United States," to which, many times, the victims are given affirmative answers.

E. Visa fraud: 18 U.S.C. § 1546

Any time that a perpetrator makes a fraudulent or counterfeit document purporting to confer any immigration right or permission to work in the United States, the traditional rules for visa fraud prosecutions apply. If the perpetrator is dealing with authentic visas unlawfully obtained, for example by false statement, then prosecution under this statute remains appropriate.

F. Identity fraud: 18 U.S.C. §§ 1028 and 1028A

When perpetrators produce false identification documents, 18 U.S.C. § 1028 can be a valuable tool to combat notario fraud. Additionally, when perpetrators misuse identity documents of others, including those identity documents from actual persons that are stolen or used without permission, then use of the aggravated identity fraud statute, 18 U.S.C. § 1028A, can be helpful and carries a two-year minimum mandatory sentence.

G. Conspiracy to commit any of the above crimes: 18 U.S.C. § 371

Prosecutors have been able to charge multiple defendant schemes through the use of the conspiracy statutes. As in other conspiracy cases, reference to the Department of Justice guidance on the use of conspiracy charges can be a valuable asset.

II. Investigative Techniques

A. Confidential informants (CIs) and undercover officers (UCs)

It is always helpful to have a fraudster caught on tape committing a crime. To that end, CIs that are current victims of the scheme have been invaluable to some prosecutions. CIs were especially helpful when they were willing to wear a wire or a camera during their interactions with the targets. UCs are also extremely valuable. Because a majority of these crimes are committed based on greed, notario fraud targets seem extremely willing to take on new clients, consequently providing an opportunity for the use of CIs and UCs.

B. Working with U.S. Department of Citizenship and Immigration Services

For those targets that are actually filing applications, it is helpful to develop a contact within the U.S. Citizenship and Immigration Services, especially their fraud investigators that are located within many field offices. If you can help the investigating officer develop a method to identify the fraudulent applications, your documentary evidence will grow exponentially as you discover the breadth and depth of the fraud your target has perpetrated.

C. Search warrants

The value of email search warrants and physical location search warrants can also add obvious evidentiary strength to your case. Many targets keep stockpiles of immigration applications and pay-owe sheets that detail customer lists and payments. If the applications are done on computers, or computers have been used to create fake documents or receipts of any type for your victims, then the computer search can also pay dividends for your case.

III. Victim centered approach

As in any type of case, there are special considerations when dealing with a class of victims that are illegally in the United States. Your victims may already have a general fear and distrust of law enforcement and the judicial system, rooted in their perception of law enforcement from their birth country. Fear can be heightened by the behavior of the perpetrator, who may have threatened to call immigration officials and have those victims who could not pay the perpetrator's fees deported. There may also be a general fear of U.S. immigration officials, and your victims may all believe that they will be deported if they report the crime. To combat this chilling effect, after the target's arrest, it has been helpful to publicize the arrest through methods that reach the immigrant community. Examples include local television news and radio stations, especially radio and news stations that service your victims' community. Be sure to have translation services ready for any language barriers that may arise. Offices that have engaged in this type of publicity have been treated to a veritable flood of new victims once word of the fraudster's arrest was publicized.

IV. Victims' eligibility for immigration benefits

Although this area is fraught with peril, illegal alien victims can be eligible for benefits through the course of your prosecution and beyond. If it is unlikely that your victims can be located in the future, Homeland Security Investigations (HSI) can extend benefits to illegal aliens, such as deferred action or parole, that create a vehicle through which your victims can obtain work authorization and permission to be in the United States through the pendency of your case. The work permit is valuable because it requires the alien to keep in contact with HSI in order to keep the permit current, and allows the victims to apply for jobs they may not be eligible for without the authorization. However, it is highly recommended that you, as the prosecutor, do not directly offer those benefits to the victims in exchange for testimony. It is always helpful to partner with HSI early in your investigation so that you are not scrambling to help victims at the last minute. Your victim witness coordinator can be an invaluable resource by helping to coordinate these permissions through HSI. Other types of long-term benefits can come in the form of U-visas or S-visas, both of which confer permanent immigrant status on the victim. However, to be eligible for a U-visa, the victim has to be a victim of a violence-based crime or extortion-based crime, as the crime must be one of, or closely related to, the enumerated crimes in the U-visa application—DHS form U-918. Likewise, the S-visa is a very narrow and highly sought after benefit conferred on only 200 aliens yearly in consideration for their cooperation during a criminal investigation and prosecution.

V. Sentencing concerns

A. Loss amount and number of victims

In order to hold the defendant responsible for the entirety of his or her conduct, it is important to make sure that the maximum number of victims and their respective loss is presented to the court during sentencing. As previously stated, your district's victim coordinator will be an invaluable source of help to coordinate your victim witness efforts in the notario fraud context.

B. Vulnerable victim enhancement

The use of the vulnerable victim enhancement under U.S. Sentencing Guideline § 3A1.1(b)(1) has been applied with great success by prosecutors throughout the country. In virtually every notario fraud case that has been prosecuted federally to this point, judges have enhanced defendants' sentences through the use of the vulnerable victim enhancement. In cases around the country, many victims illegally in the United States have been found to be less educated and unfamiliar with U.S. law and the English language, and to have a generalized fear of reporting their crimes due to their fear of being discovered by immigration officials and being deported, making them more susceptible to the perpetrator's scheme. As with every other victim centered prosecution, make sure that your victim witness coordinator is notified about the victims and the arrests in your case to ensure that your victims' rights are preserved and their facts are presented to the court at sentencing. ❖

ABOUT THE AUTHOR

❑ **Andy Choate** is an Assistant U.S. Attorney in the District of Utah and former counsel for the Department of Homeland Security Immigration and Customs Enforcement. Currently, Mr. Choate supervises the immigration caseload in his district and prosecutes matters involving national security and immigration-related crimes. He recently prosecuted two high profile notario fraud cases, one involving a licensed immigration attorney who received a 56-month sentence of imprisonment and who also forfeited a million dollars, and another involving a defendant who impersonated a DHS officer and received a 41-month sentence of imprisonment. ✠

Effective Tracking of Alien Smuggling Organizations: The Bitter Green Investigation—A Case Study

Kristen Brook
Assistant United States Attorney
National Security and Border Security Section
District of Arizona

I. Following the money

Human-smuggling networks typically charge between $3,000 and $6,000 to smuggle a single person across the United States-Mexico border to a final destination within the United States. Rates increase significantly if the journey starts in Central America instead of Mexico, involves traveling by plane or by train instead of walking through the desert, involves bringing children separately, or requires travel to more distant U.S. locations like New York or Florida. In other instances, organizations regularly exploit the vulnerability of their human cargo and increase the passage rate after crossing the border into the United States.

A. The rise of funnel accounts

Historically, money transfer services like Western Union were the method of choice for smugglers moving cash or value across the United States. In recent years, agents have observed a shift from money transmitter services to alien smuggling organizations (ASOs) using traditional banks throughout the United States. The reasons may be simple—anonymity and cost. At money transfer services like Western Union, Sigue, MoneyGram, PreCash, etc., the money transferor must provide—for both themselves and the receiver—a name (presumably their own), along with dates of birth, addresses, and phone numbers. Money transfer services also charge a fee for each transaction.

In contrast, providing a bank deposit option means that smugglers do not have to hand over their name and personal information. They are insulated by a layer of protection—the money launderer. Smugglers hand over the name of their money launderer and his or her bank account number. Families of undocumented people can walk into a local branch of a national bank, pick up a bank deposit slip, fill in the information provided by the smuggler—the account number and the name on the account—provide the cash, and walk away without having to provide identification or specific information such as an address, a telephone number, or date of birth. Bank accounts also allow smuggling organizations to collect cash deposits made anonymously throughout the country and then withdraw them immediately without any transfer fees. With regard to cost, the simple act of depositing money into a specified bank account does not require the payment of a fee.

Funnel accounts are ordinary bank accounts opened through banks with a nationwide footprint, where money can be deposited into the account from all over the United States. The money launderer may then withdraw any and all deposits out of the account, generally from one location and usually within hours of the deposit. Thus, the transactions begin to take the form of a funnel, funneling money to the location of the money launderer.

B. How payment is made

To move money through the ASO, the organization may pay an associate—that is, a money launderer—to open one or more bank accounts at various banks with branches spread throughout the United States. The more banks utilized, the easier it is for relatives to find a convenient branch in their hometown and the more difficult it is for law enforcement to detect the unlawful activity. Relatives of the undocumented immigrants deposit cash into the account to pay for at least part of their relative's passage. Ordinarily, part of the payment is due before the illegal immigrant is guided into the United States. What remains once they arrive is the second part—payment for passage from the drop house to their final destination farther in the interior of the United States.

On one hand, this makes financial activities difficult to detect because the transactions usually involve amounts below $10,000, the amount that triggers automatic reporting to banking regulators. However, funnel accounts form a pattern, and once that pattern is detected, the money becomes vulnerable to law enforcement investigation and possible seizure.

II. The source—the money launderer

ASOs tend to be compartmentalized into cells, with members separated by role. The guides, the load drivers, the drop house operators, the leaders, and the managers oftentimes work in relative isolation within their own role, only infrequently coming into contact with other members in the ASO. In the Bitter Green investigation, Homeland Security Investigations (HSI) agents identified the money launderer, the common denominator among the various individuals performing their respective roles, and used him to dismantle the ASO. In Bitter Green, this one person linked together different smugglers, drop house operators, load drivers, guides, and leaders. He used his bank accounts to collect and launder funds deposited by family members of smuggled aliens at locations throughout the United States and distributed those funds to people within the ASO.

In Bitter Green, the leaders of the organization typically worked the phones and talked to family members to secure payment. The money launderer did not contact families and did not pass along his bank account information personally. Instead, the money launderer would receive notification from the leaders that a deposit was to be made, and then he would receive direction to withdraw money and give it to another smuggler. The money launderer would contact the other smugglers to coordinate the transfer.

A. Finding the source

In some investigations, finding the money launderer is the real challenge. If an ASO is using a funnel account, the common thread among these money launderers is the manner in which they conduct business—using a bank account through a financial institution to receive deposits from locations throughout the United States, and then withdrawing the funds shortly after they have been deposited. The bank account will be under a full name, which may be an alias.

In Bitter Green HSI identified the money launderer through the paper trail he left behind. That paper trail is central to the organization. The paper trail not only implicates the money launderer, but is a clue that reveals the interconnectedness of each individual to the organization.

What is the paper trail, and what does it look like? In some cases, it looks like doodles left on slips of paper near cell phones or on countertops in stash houses. Sometimes it is notations etched in a "pollo" ledger. ASOs often refer to their clients as "pollos" (the Spanish translation for chickens). Thus, a "pollo" ledger is a notebook used to keep track of the people who have transited a drop house. It often will include the smuggled person's name, the name or nickname of the smuggler responsible for that individual, the contact information of relatives, money owed/paid, and the bank account into which payment has been made. In other cases, the paper trail can be found in the pocket trash of the drop house

operator or inside the cell phone of the drop house operator or driver. On the paper or in a note in the phone, agents can look for a name, bank account numbers, and bank names.

Time is of the essence when processing this type of evidence. Assistant U.S. Attorneys should ask agents to look for the paper trail as soon as they secure a search warrant on the drop house. It is important to move quickly and make efforts early to identify and locate the money launderer(s) before the ASO tips them off that the drop house has been busted. Once a house has been taken down, it is common for those associated with the house to go quiet and be dormant for a period of time. Consequently, it is important to catch the money launderer before the smugglers change their pattern of business.

B. Acting on the information in the paper trail

Once agents find a possible bank account number, the next step is to determine whether the account is active and open. At this stage, agents can coordinate with a special agent in the financial accounting group to reach out to the financial institution. In the Bitter Green investigation, agents identified a bank name and account number inside a drop house. Agents reached out to the bank and learned that the named individual typically frequented one branch and was present on a near-daily basis. The agents went to the bank and were waiting when the target returned to withdraw money. The agents met him in the parking lot as he left the bank and began to use him as a source.

In the absence of a proactive source, another way to search is by using FinCEN. HSI agents, in particular, can use FinCEN, which operates a database that collects and reports on suspected illegal activity.

C. Developing a prosecution strategy

If agents can hook the money launderer, he may physically lead them to the middle management smugglers, those who have been trusted enough to be in contact with the money and to pay others within the ASO. With the Bitter Green source, agents wired the money launderer and recorded and photographed all pre-meeting phone calls and money transfers. With that said, during the conversations surrounding the transfers, the smugglers were guarded about discussing the source of the money and their business practices. As a result, agents strategized each arrest so that each individual smuggler was taken down in the act of smuggling, harboring, or transporting undocumented persons.

D. Charging options: 18 U.S.C. § 1956(h)

Consider charging the smuggler with a violation of 18 U.S.C. § 1956(h) if the smuggler was not arrested with aliens, but instead was involved in laundering proceeds of alien smuggling by virtue of having directed others to make a deposit or a payment, having directed other smugglers to pick up proceeds or distribute proceeds, or themselves having picked up proceeds, concealed proceeds, or transferred proceeds of alien smuggling. Successful prosecution under this statute requires more evidence than a suspect merely picking up money. The statute requires proof that the suspect knew the proceeds were from alien smuggling. A conspiracy charge under § 1956(h) may be an elegant way to efficiently charge this conduct. Moreover, a focus on the concealing aspects of funnel accounts may also have significant jury appeal. In the indictment, the specified unlawful activity is transporting and harboring illegal aliens in violation of 8 U.S.C. § 1324(a)(1)(A)(ii)–(iii).

The manner and means used to accomplish the objectives of the conspiracy can include, among other means: (1) the use of nominee bank accounts in order to conceal and disguise the nature, location, source, ownership, and control of the illegal alien smuggling proceeds; or (2) the use of accounts at financial institutions to negotiate and deposit cash and then withdraw U.S. currency in order to further conceal and disguise the nature, location, source, ownership, and control of the illegal alien smuggling proceeds.

A plea to the § 1956(h) charge will result in a U.S. Sentencing Guidelines (U.S.S.G.) calculation either under U.S.S.G. § 2S1.1 (the money laundering and monetary transaction reporting Guideline) or under U.S.S.G. § 2L1.1 (the smuggling, transporting, or harboring of an unlawful alien Guideline), depending upon which calculation yields the highest Guideline sentence. Assistant U.S. Attorneys should keep in mind that the 18 U.S.C. § 1956(h) charge will also yield a two-level enhancement under U.S.S.G. § 2S1.1(b)(2)(B).

E. Taking down the members as they are found

In Bitter Green, more than 50 members of the ASO were prosecuted and charged over the course of a year, most within a period of 5 months. For risk mitigation reasons, the investigation had, from its inception, an established end date for the proactive use of the source. Members were arrested one at a time, rather than in a one-day event, because we wanted to increase the likelihood of arresting smugglers in the act of moving or harboring illegal aliens. Middle and upper level managers were not charged until the end of the operation, which helped protect the source and allowed us to disclose the recordings all at one time. Most of the lower-level ASO members were charged in walled-off cases in which local police established their own probable cause and arrested defendants without disclosing the existence of the broader investigation.

F. Establishing knowledge during the interview

Agents should ask smuggling suspects about the number of aliens moved by the organization during their post-arrest interviews. This figure has a significant impact on the Guidelines calculation under U.S.S.G. § 2L1.1(b)(2). Agents can also use money movement—the amount received per alien, the number of transactions, and the amount received overall—as a means to account for the number of aliens during the interview with the smuggling suspect. Agents should be explicit and question the suspect about how long they have been in the business, during which months the business has the most customers, and what a busy month looks like. They should ask the smuggling suspect how they are paid and how they pay others. For example, if the suspect suggests that they were paid $30 per alien and received a total of $3,000, then have the agents ask if it sounds accurate that they moved about 100 aliens.

III. Finding the leaders and organizers—despite their anonymity and physical distance from the drop houses

In Bitter Green, three leaders ran the ASO by phone from locations far from the Mexican border. They ran it from Arkansas, Louisiana, and New York. Not a single member of the organization could or would visually identify any of these leaders. Despite their anonymity, agents were able to track them down, arrest them, and prosecute them in the District of Arizona.

A. The clues left behind: Rony Gonzalez-Herrera, the Arkansas leader

HSI agents recovered multiple pollo ledgers that contained the name "Rony," "Roni," "Rony Arkansas," and "Rony Abimael Gonzalez Little Rock Arkansas" written in the margins. Based upon the repeat appearance of his name in the pollo books, the agents believed Rony was possibly a smuggler who collected human smuggling fees and who could be responsible for the movement of the undocumented aliens (UDAs) to their destination into the United States. *See* Press Release, Dep't of Justice, Arkansas-Based Man, Responsible for Over 800 Illegal Aliens Smuggled Into Arizona From Mexico, Sentenced to Federal Prison (May 8, 2014) (Case Number CR13-1141- PHX -NVW); Becky Bratu, *Man Who Helped Smuggle Over 800 People Into U.S. Sentenced*, NBC NEWS (May 8, 2014), *available at* http://www.nbcnews.com/news/us-news/man-who-helped-smuggle-over-800-people-u-s-sentenced-n101011.

Agents searched the pocket trash of UDAs found at drop houses. Inside one UDA's pocket, they found a piece of paper with the name "Rony" and a telephone number. Agents called the U.S.-based

relatives/sponsors of the UDA and inquired about the smuggling fee payment. The UDA's brother stated that he was instructed by Rony to deposit $2,700 in a Bank of America bank account to pay the UDA's smuggling fee. The brother stated that his only communications were with a man named Rony at a phone number that matched the number found on the piece of paper inside the UDA's pocket. The brother also stated that after he learned the UDA had been arrested by U.S. Immigration and Customs Enforcement (ICE), he called Rony to request a refund of part of the smuggling fee he had paid. He told Rony that his brother had been arrested and detained by ICE and that he needed to pay a bond for his brother's release. Rony told the brother it would be best for the UDA to request an immediate removal from the U.S. Rony refused to return any of the smuggling fees that were paid. When the brother made additional efforts to request a refund of some of the money, Rony verbally threatened him by saying, "Your family will pay if you keep asking for the return of any money!"

The Intelligence Research Specialist (IRS), in partnership with HSI, conducted a search through the Consolidated Lead Evaluation and Reporting (CLEAR) database of the telephone number and discovered that it was listed to a Rony Gonzalez and a Rony Abimael Gonzalez, with an address in Little Rock, Arkansas. CLEAR also listed a Tennessee driver's license (DL) number issued to a Rony Abimael Gonzalez. A record check from the State of Tennessee Integrated Criminal Justice Portal confirmed that Tennessee DL returned to a Rony Abimael Gonzalez, with additional information showing his date of birth and Social Security Number. The HSI IRS also conducted queries through the Southwest Border Anti-Money Laundering Alliance (known as DIG). DIG relays data from money transmitters, such as Western Union, MoneyGram, and Sique, to the Arizona Attorney General's Office pursuant to an order issued by the Superior Court in Maricopa County, Arizona. The Rony Abimael Gonzalez Tennessee DL number was listed next to three 2012 Sique money transmissions sent under the name Rony Gonzalez Herrera with the same telephone number stated above.

In connection with the investigation of another drop house within the same organization, agents stopped a Chevrolet Uplander minivan carrying 10 UDAs. Inside the vehicle they found a sales contract. The Buying Representative displayed on the contract was "Rony Gonzalez." Also located inside the Uplander was a 2013 Personal Property Assessment for Pulaski County, Arkansas, for Rony Gonzalez Abimael with an address listed in Little Rock, Arkansas. Listed on the Pulaski County Property Assessment were three additional vehicles. HSI queried the vehicle identification numbers of these three vehicles in Department of Homeland Security (DHS) databases and discovered one of the vehicles had been stopped for alien smuggling by the U.S. Border Patrol near Amarillo, Texas, in February 2013. Another one of the three vehicles listed on the Pulaski County Property Assessment was a Hummer H3 with a specific registered license plate. In May 2013 agents apprehended Rony driving this Hummer H3 in Little Rock, Arkansas. Rony was transferred to the District of Arizona to face charges.

The Arkansas leader, Rony Abimael Gonzalez-Herrera, pleaded guilty and was sentenced to 57 months' imprisonment for his part in operating the alien smuggling business from the assumed anonymity of Little Rock, Arkansas. The court found Gonzalez-Herrera and his associates responsible for illegally transporting and harboring at least 827 illegal aliens.

B. The Louisiana and New York leaders

The Louisiana leader, Otoniel Galindo Vasquez-Lopez, was identified in a similar fashion. Vasquez-Lopez was not physically identified by any member of the ASO, but he was apprehended through record searches and electronic and physical surveillance on the ground in Louisiana. Vasquez-Lopez is awaiting trial, scheduled for January 6, 2015, in the District Court of Arizona, for his part in operating the illegal business from the assumed anonymity of Shreveport, Louisiana.

The New York leader of this ASO, Joel Mazariegos-Soto, was sentenced by the District Court of Arizona to five years in federal custody for his part in operating the ASO from the assumed anonymity of Fonda, New York, where he also worked on a dairy farm. Mazariegos-Soto likewise was not physically

identified by any member of the ASO. Agents identified him by following leads in pollo ledgers that included references to New York next to his name. Agents surmised that Mazariegos-Soto might reside in New York. Agents also located a paper vehicle registration that listed a specific address for him in New York. Agents in New York confirmed Mazariegos-Soto lived at that address. During just four months of this investigation, Mazariegos-Soto laundered more than $70,000 by moving the money—directly from the U.S.-based families of illegal aliens—through an illegal funnel account and to his alien smuggler employees working in the Phoenix area. *See* Press Release, Dep't of Justice, New York Based Alien Smuggler and Associate Sentenced for Operating an Illegal Alien Smuggling Business in Arizona (Mar. 19, 2014) (Case Numbers CR13-898-PHX-SRB and CR13-955-PHX-SRB).

IV. Conclusion

The investigation and prosecution of this ASO was a long-term investigation targeting all tiers of one ASO. The agents appended and arrested almost every identified member of the organization, from the desert guides to the load drivers and even the remote leaders. ❖

ABOUT THE AUTHOR

❑ **Kristen Brook** joined the U.S. Attorney's Office for the District of Arizona in 2009 after serving for five years as a Deputy County Attorney at the Pima County Attorney's Office in Tucson, Arizona. Ms. Brook is currently an Assistant U.S. Attorney assigned to the National Security and Border Security Section. Prior to this she prosecuted cases arising out of OCDETF, violent and border crimes investigations. At the Pima County Attorney's Office Ms. Brook specialized in prosecuting cases in the Special Victim's Unit. Throughout her career Ms. Brook has tried over 90 criminal and civil cases to a jury. ✠

The Bitter Green investigation was conducted by Homeland Security Investigations in Phoenix, led by Special Agent George Long, Special Agent Christian Johnston, and Special Agent William Madril of HSI.

Prosecuting Marriage Fraud Conspiracies—Lifting the Veil of Sham Marriage

Kebharu H. Smith
Assistant United States Attorney
Southern District of Texas

Suzanne Elmilady
Assistant United States Attorney
Southern District of Texas

A sign caught my eye one morning while I headed to work on the D.C. Metro. Half of the sign was a photograph of a church prepped for a wedding. The other half was a hallway in a penitentiary. Written on the side of the sign with the penitentiary hall were the words, "If you commit marriage fraud, you could be spending five years walking down these aisles." Because I had recently prosecuted a marriage fraud case in the Southern District of Texas, I knew this statement was not exactly accurate. Although 8 U.S.C. § 1325(c), the marriage fraud statute, has a five-year *maximum* range of punishment, federal prosecutors who prosecute marriage fraud cases know that securing a five-year sentence on a stand-alone marriage fraud conviction, or any sentence close to five years, is highly unlikely under the U.S. Sentencing Guidelines.

Under § 1325(c), a person commits marriage fraud when the marriage is entered into for the purpose of "evading any provision of the immigration laws" of the United States. 8 U.S.C. § 1325(c) (2014). Marriage fraud can be an attractive pathway toward permanent residence and/or U.S. citizenship for foreign nationals who desire to migrate to, or remain in, the United States. The risk of prosecution and jail time is slim. Under the U.S. Sentencing Guidelines, a marriage fraud conviction for a defendant with no aggravating factors and no criminal history points results in a range of zero to six months. There are also no quotas on the number of visas that can be issued to foreign nationals that are married to U.S. citizens. Unlimited visas, combined with infrequent detection, make marriage fraud a low-risk way of skirting U.S. immigration laws.

This article will discuss the background, decisions, and challenges of the prosecution of a multi-defendant marriage fraud conspiracy in the Southern District of Texas, Houston Division, in *United States v. Mitema*, No. 4:10-CR-00804, slip op. at 1 (S.D. Tex. Apr. 23, 2014). We will also discuss strategies and considerations that Assistant U.S. Attorneys should be aware of in future marriage fraud prosecutions.

I. The *Mitema* conspiracy

The *Mitema* marriage fraud conspiracy was first uncovered by the Department of State's Diplomatic Security Service (DSS) in November 2009, when a passport agent detained two young women on suspicion of passport fraud. The two women had very similar names, and one of the women had recently acquired a passport. The women initially claimed they were traveling to Africa "to see the animals," but were unable to state *where* in Africa they were going. After continued questioning, the women admitted that they were getting their passports to travel to Kenya for the sole purpose of marrying Kenyan nationals in exchange for money, and to help the Kenyans get immigration status to enter the

United States. The two women told the agents about several other Kenyan nationals in the Houston area that were in fraudulent marriages with the women's family members and friends, solely for money and immigration status.

DSS agents cross-referenced this story with information contained within the Alien files (A-files) for the Kenyan nationals that the women identified. The DSS agents uncovered eight suspected sham marriages that had taken place over the previous decade, all between male Kenyan nationals and female U.S. citizens. The Kenyan nationals had arrived in the United States on student visas to attend Texas Southern University, although most of them never even enrolled. Once the student visas were set to expire, the Kenyan nationals would marry recruited U.S. citizens in sham Justice of the Peace ceremonies. The recruited women were promised between $2,500 and $5,000 to marry the Kenyan nationals although, in most instances, these promises were not honored.

As part of the scheme, the conspirators staged photographs of wedding ceremonies and submitted the photographs to U.S. Citizens and Immigrations Services (CIS). The Kenyan nationals also claimed the children of the U.S. citizen spouses (not fathered by the Kenyan nationals) on tax returns filed with the IRS and submitted to CIS to bolster the legitimacy of their marriages. Meanwhile, several of these men were carrying on meaningful relationships more akin to a legitimate marriage with Kenyan women during the course of the sham marriages to U.S. citizens.

The Kenyan nationals were all members of the Kissii Kenyan ethnic group, and several were related to each other. Interviews, surveillance, student records, and the A-files helped agents identify and untangle the web of marriages. Security camera footage from the passport office on the day the DSS agent interviewed the two women captured a man who was later identified as Andrew Mokoro. Mokoro, a Kenyan national, had acquired U.S. citizenship based upon a 2003 marriage to a U.S. citizen named Tequilla Rhymes. Further investigation revealed that in 2001, Valene Cornelius, a friend of Rhymes, married Alfonso Ongaga, an associate of Mokoro's. Sabrina Adams, the aunt of Valene Cornelius, encouraged her five daughters to marry Kenyan nationals for money, and she herself married Herman Ogoti for money in 2004. Her daughter, Anteal Adams, married Andrew Mitema in 2002. In 2005, another daughter, Vasha Adams, even flew to Kenya to marry Rebmann Ongaga when he was unable to obtain a visa to the United States.

II. Marriage fraud: the charging decision

In *Mitema*, we were faced with a marriage fraud conspiracy with up to 20 potential defendants. A major question that needed to be resolved was whether to charge the cooperating coconspirator U.S. citizens. We decided that including 20 people in the indictment would be a costly and inefficient use of USAO resources, especially in light of the ultimate sentences. We chose to focus on prosecuting those who had the most to gain from the sham marriages—five Kenyan nationals who had gained citizenship and/or permanent residency in the United States. In comparison, the U.S. citizen spouses had gained relatively little from the conspiracy.

The Kenyan nationals also were relatively more sophisticated than the U.S. citizen spouses. The Kenyan nationals sought out vulnerable women from Houston's Fifth Ward, who welcomed the idea of being paid $5,000 for a sham marriage. The men also gave additional money for food and clothing after the ceremonies. Most of the women were very young at the time of their sham marriage. For example, the conspirators waited until Sabrina Adams' youngest daughter, Anteal Adams, turned 18 so that she could marry Andrew Mitema.

It should be noted that a decision not to charge a conspiring U.S. citizen spouse will be scrutinized by defense counsel during cross-examination. However, in *Mitema*, the jury was visibly offended by the nature of some of the questions posed by defense counsel towards the U.S. citizen

spouses. The jury clearly agreed with the reasoning that went into our charging decision and understood that the U.S. citizen spouses did not truly appreciate the fact that marriage fraud was a crime.

III. Sentencing considerations for marriage fraud cases

A marriage fraud conviction for a defendant with no aggravating factors and no criminal history results in only zero to six months' imprisonment under § 2L2.2 of the U.S. Sentencing Guidelines. U.S. SENTENCING GUIDELINES MANUAL § 2L2.2 (Base Offense Level 8). Although the Guidelines do not give prosecutors much leverage to wield stiffer sentences, prosecutors can find recourse through other remedies. A defendant convicted of marriage fraud faces a fine, deportation, exclusion, removal from the United States, and, in some cases, denaturalization of his fraudulently acquired U.S. citizenship. *See* 18 U.S.C. § 1425 (2014) (fine and/or imprisonment); 18 U.S.C. § 1451 (2014) (providing for revocation of citizenship where citizenship was "illegally procured or w[as] procured by concealment of a material fact or by willful misrepresentation"). These factors, not the risk of jail time, increase the likelihood that cases will get resolved at trial.

In light of the relatively minor sentences associated with marriage fraud, it is best to avoid singular marriage fraud cases—that is, a case with one fraudulent marriage—to the extent practicable. This is largely based upon a combination of ensuring the most efficient use of USAO resources and smart, simple prosecutorial discretion. Of course, this is by no means a hard-and-fast rule. Although rare, a single marriage fraud case will be prosecuted if the marriage fraud defendant is suspected of being tied to other, more egregious criminal behavior, such as a violent crime, suspected terrorism, money laundering, or alien smuggling. While there are ways to increase the ultimate detriment to those convicted of marriage fraud, the complexity and difficulty in detecting and prosecuting marriage fraud cases make it an arduous task with very little sentencing reward.

IV. Marriage fraud: proving the "sham" by lifting the veil of the fraudulent marriage

The efficient use of resources supports the prosecution of multiple fraudulent marriages in a single case. Prosecutors should note, however, that cases involving just one fraudulent marriage are never clear-cut. The prosecutor will rarely be able to rely on direct evidence, such as wiretaps, corroborating bank records, enthusiastic witnesses, or cooperators that will substantially benefit from a § 5K1.1 downward departure motion. Lifting the veil of the fraudulent marriage at trial requires strong circumstantial evidence and the testimony of a cooperating coconspirator.

In most instances of marriage fraud conspiracy, coconspirators have agreed to engage in acts of recruitment, transportation, and payment or promises of payment to vulnerable U.S. citizen spouses. In *Mitema*, we uncovered at least eight fraudulent marriages (although not all were prosecuted) and discovered several attempts to have U.S. citizens fly to Kenya to marry Kenyan nationals. The Kenyan nationals did more than just offer to pay the U.S. citizens $5,000. They purchased clothes and manicures for the women and diapers for their children. They purchased the airline tickets to Kenya, paid for passports and passport photos, and drove the U.S. citizens to the airport for their flights to Kenya.

As in *Mitema*, a prosecutor will hopefully have at least one U.S. citizen spouse acting as a cooperating witness. A cooperating U.S. citizen spouse may give a prosecutor insight into the fraudulent marriage. For example, this witness can discuss financial expectations, living arrangements, and most importantly, expose the lack of expected knowledge that coconspirator spouses have about each other. The prosecutor can ask specific questions about the foreign spouse that the U.S. citizen spouse most likely cannot answer, like the foreign spouse's birthday, favorite color, and middle name. The prosecutor can also get information regarding any "prep sessions" that the U.S. citizen spouse and the foreign spouse had for CIS interviews. In *Mitema*, we were able to pull CIS interview notes from the A-files and present testimony from the cooperating U.S. citizen spouses about how they used CIS interview questions that

were posted on the Internet to prepare for CIS interviews. This testimony was instrumental in exposing the sham marriage.

During the commission of a marriage fraud conspiracy, there are often other crimes and overt acts committed that either further the marriage fraud conspiracy or attempt to give the sham marriage an appearance of legitimacy. As evidenced in *Mitema*, this activity may range from taking staged photographs for submission to CIS to forging and lying on tax documents by claiming the children of the U.S. citizen spouse. During trial, we were able to present copies of the staged photographs of Sabrina Adams' children at defendant Herman Ogoti's house for a pizza party. Sabrina Adams testified at trial that even though she and Ogoti were "married," those photographs depicted the only time that her children ever visited Ogoti's home.

V. Defense tactics: spousal privilege and cultural norms

Because the testimony of the U.S. citizen spouse is so instrumental in proving the sham marriage, defense counsel will try to prevent it from being presented at trial. In *Mitema*, defense counsel filed a joint pretrial motion to exclude communication made amongst the coconspirators during the course of the marriages, as protected by spousal privilege. We argued the spousal privilege did not apply because the marriages were fraudulent and entered into solely for the sake of evading the immigration laws of the United States. We proffered that the cooperating U.S. citizen spouses would testify that they married the Kenyan nationals solely for money and to help them "stay in the United States." The court denied their motion and allowed the cooperating U.S. spouses to testify about the fraudulent nature of their union.

Marriage fraud defendants will often use alleged cultural norms and traditions as a defense to the sham marriage. Under this argument, the marriages were not entered into to evade U.S. immigration law, and any immigration benefit that resulted from the arranged marriages was legal and permissible in the defendant's culture. The *Mitema* defendants first argued that Kenyan Kissii tradition involves arranged marriages and that these marriages are consistent with Kissii cultural values and norms. They then claimed that the witnesses best suited to testify about the arranged marriages and the compliance with cultural traditions were in Kenya and either too sick or too poor to travel to the United States to testify at trial. To rectify the alleged hardship of unavailable critical defense witnesses, the court ordered an international deposition. The deposition was conducted via video teleconference with the U.S. Embassy in Nairobi and at the U.S. Attorney's Office in Houston. Before the deposition, we fortunately secured Dr. Tabitha Otieno, a sociology professor at Jackson State University, as an expert witness. Dr. Otieno, a naturalized U.S. citizen from Kenya and a member of the Kissii ethnic group, testified on cultural norms and characteristics of the Kissii. Dr. Otieno's trial testimony was crucial to rebut the defendants' "cultural norms" argument. After she testified at trial, the defense did not offer the video deposition that they initially claimed supported the arranged marriage theory.

VI. Conclusion

Four of the *Mitema* defendants chose to proceed to trial. The jury found all defendants guilty of visa fraud, marriage fraud, and conspiracy to commit marriage fraud. Two defendants were also convicted of procurement of citizenship or naturalization unlawfully, in violation of 18 U.S.C. § 1425. As a result of the § 1425 convictions, the court revoked the fraudulently acquired U.S. citizenship of defendants Herman Ogoti and Alfonso Ongaga. At sentencing, defendants Andrew Mokoro and Alfonso Ongaga were sentenced to 16 months' imprisonment, and defendants Herman Ogoti and Rebmann Ongaga were sentenced to 6 months' imprisonment. The final defendant, Andrew Mitema, pleaded guilty to conspiracy to commit marriage fraud and tampering with a witness and was sentenced to 21 months' imprisonment.

As long as the immigration laws provide for limitless marriage visas and the U.S. Sentencing Guidelines offer a range of zero to six months, marriage fraud will remain one of the primary ways that people evade U.S. immigration laws. The prosecution of marriage fraud cases requires vigilant Assistant

U.S. Attorneys who are not deterred by the low sentences and convoluted facts, and who see the importance of closing off this loophole to illegal immigration. ❖

ABOUT THE AUTHORS

❑ **Kebharu H. Smith** is an Assistant U.S. Attorney for the Southern District of Texas, Houston Division. Mr. Smith is currently serving on a detail to the Executive Office for United States Attorneys General Counsel's Office. Prior to working as an AUSA, Mr. Smith worked as a state prosecutor for seven years in the Fort Bend and Harris County District Attorneys' Offices. ✠

❑ **Suzanne Elmilady** is an Assistant U.S. Attorney for the Southern District of Texas, Houston Division. Mrs. Elmilady is currently assigned to the Major Fraud Section. Prior to working as an Assistant U.S. Attorney, she worked as a state prosecutor at the Harris County District Attorney's Office in Houston, Texas for approximately five years. ✠

The New Wild West: Justice in the Bakken

Laura Weiss
Assistant United States Attorney
District of Montana

I. Introduction

The siren song of gold and the promise of quick riches. A flurry of young men headed west. A sudden spiral into vice and lawlessness. It is a dramatic tale, one would think, reserved for the memory of the Gold Rush, but a similar narrative has resurfaced more than 150 years later. In America. In 2014. This time, the gold is liquid. It is called the Bakken—a vast swatch of oil-rich land stretching approximately 150,000 square miles from Saskatchewan, Canada, into western North Dakota, and crossing into eastern Montana. In the course of approximately the last five years, it has caused a social eruption—in population, jobs, and money. It has exposed, predictably, the seedy underbelly of those promising advances: resource shortages, young men with money to burn, and a veritable buffet of vices to spend it on.

In the course of the Bakken's rapidly-expanding influence, the U.S. Attorney's Office (USAO) for the District of Montana, along with its sister offices in surrounding states, witnessed and addressed first-hand the rise of the Bakken criminal element, which has brought everything from a prolific vein of pure methamphetamine from Mexico to thoughtless environmental crimes committed by those who cut corners in the name of profit. Montana is a land of layered borders—both seen and unseen. With Canada to the immediate north and seven federally-recognized reservations throughout the state, the Bakken has underscored the need for cross-jurisdiction efforts to combat the ripple effect of a sudden increase in population and crime. This article is written with the intention of explaining this new wave of challenges brought about by the Bakken. It will explore its criminal impact on the community and address ways to enforce federal law in the face of increasingly evolved and international criminal forces in the region.

II. The borderlands of Montana

The sheer breadth of Montana's acreage, combined with the geography of its seven federally-recognized Indian tribes, produces a complicated and challenging jurisdictional picture. When our office was first contacted about writing an article for the Borders issue, my first question was, "Which border?" One hand is hardly enough to count the number and types of borders that Montana is host to. To the north is the Canadian border. Move a little south, and you are at the border of Glacier National Park and the borders of four federally-recognized tribes. Move to the east, and you are nearing the invisible borders of the Bakken. A bit farther south are Montana's largest city, Billings, and two reservations—Crow and Northern Cheyenne. This article focuses on the impact of the Bakken on the other "border" country in Montana, and on how those clashing borders have produced a new breed of legal and investigative circumstances.

A. Indian Country borders

The District of Montana and its sister districts are home to numerous federally-recognized tribes. As a result, prosecutors instantly face unique legal issues based on the geography and borders of the reservation communities. Federal prosecutors who work in what is known statutorily as "Indian Country" often must prove, as elements at trial, that a defendant is an "Indian Person" and that the events

constituting the crime occurred on reservation land. Assistant U.S. Attorneys in districts with federally-recognized tribes occupy a unique place in federal prosecutions, charging felonies such as murder, sexual abuse, assaults, kidnappings, and burglaries that occur on the reservation. These crimes, charged either vis-à-vis 18 U.S.C. §§ 1152 or 1153, constitute two types of jurisdictional charges that are contingent upon whether the victim or defendant is an "Indian Person." The decision to prosecute under § 1152 is also contingent upon whether the defendant has already been punished by the tribal judicial system. Therefore, defendants who commit felony-level crimes in Indian Country often find themselves in federal court charged under § 1152, § 1153, and the corresponding federal felony statute. For example, a defendant who stabs someone may be charged—depending on the defendant's or the victim's Indian Person status—under § 1152 or § 1153, as well as the federal felony statute for Assault With a Dangerous Weapon under 18 U.S.C. § 113(a)(3).

It should be noted, however, that not all crime occurring within a reservation carries the legal responsibility of proving Indian Person status or that the crime occurred in Indian Country. In fact, the Bakken border has rapidly ushered into Montana an unwelcome influx of "big city" crime to otherwise rural communities. With the Bakken's criminal influence, more and more federal indictments based out of Indian Country are crimes of general applicability: drug conspiracies, felons in possession of firearms, and fraud, among others. To prove these offenses, the prosecutor does not have to prove Indian Person status or that the crime occurred on a reservation, because crimes of general applicability apply evenly across the United States, regardless of who commits them or where the crimes occur.

If one were to take a survey of Indian Country federal prosecutors, it would not be a stretch to hypothesize that they have collectively seen more and more cases qualifying for prosecution as crimes of general applicability—cases involving everything from large-scale methamphetamine trafficking and firearm offenses to high-dollar fraud and theft cases. As if this influx of Bakken crime is not alarming enough, the intersection of the Bakken with surrounding borders magnifies the challenges of prosecuting crime in a geographically expansive state.

B. Bakken's invisible borders

Although its parameters lay well below the earth's surface, the reach of the Bakken's criminal influence extends far beyond its oil-bearing innards.

> Between 2005 and 2012, the population in the Williston Basin region—driven by the addition of more than 20,000 jobs—grew an estimated 17 percent. . . . The FBI Uniform Crime Report shows that crimes in the [area] increased 32 percent from 2005 through 2011, and violent crimes (which include murder, aggravated assault, forcible rape and robbery) increased 121 percent.

EXEC. OFFICE OF THE PRESIDENT OF THE UNITED STATES, NAT'L DRUG CONTROL STRATEGY 47 (2014), *available at* http://www.whitehouse.gov/sites/default/files/ondcp/policy-and-research/ndcs_2014.pdf. For example, the Bakken region has experienced a large influx of Outlaw Motorcycle Gangs attempting to establish "ownership" of the territory, facilitating the illegal drug trade and prostitution. *Id.* at 44. Law enforcement intelligence also indicates a rising presence of Mexican drug trafficking organization in the area.

The Bakken is no longer isolated to its natural geography. Its influence has impacted other communities, including native communities, in Montana. Five years ago, very few Montanans would know what the word "Bakken" meant. Today, one would be hard-pressed to find a Montanan who does not know what the word means, or who does not harbor a strong opinion about it.

Even with the influx of crime, the Bakken delivered—and continues to deliver—many positive developments to Montana. For better or worse, sleepy Montana towns have been transformed into man-camps, teeming with six-figure income oil workers, new businesses, packed hotels and restaurants, and

grocery stores that can't keep enough food on the shelves. Those young workers, however, suddenly find themselves with the luxury of excess income.

At this point in the story, highly organized national and international criminals enter the picture. With the arrival of the Bakken, Montana is suddenly a destination of choice for Mexican meth—extremely pure and extremely easy to access. Cartels and other organized criminals have identified the Bakken as the next ripe criminal market. Like any good entrepreneur, dealers looking toward the Bakken are realizing there is a broader, and even more lucrative, Montana market in which to pedal their illegal wares—the surrounding reservations. In Billings a dealer can sell a gram of meth for $100. In the Bakken, he can sell a gram for $150. *Or* he can travel a few hours and sell the same gram of meth for $350 to $400 on a nearby reservation.

Another collateral consequence of the expanding influence of the Bakken is this distribution of extraordinarily pure methamphetamine. The lion's share of methamphetamine indictments from Indian Reservations in Montana are host to charges involving methamphetamine with an over 95 percent purity level. In fact, most Drug Enforcement Administration results routinely return purity levels closer to 98 to 99 percent.

The reverberations of pure meth into Indian Country communities are deeply destructive. In 2013 alone, over 20 babies were born on the Fort Peck reservation with methamphetamine in their systems. Parents disappear from their children's lives to abuse drugs. Burglaries, fueled by an appetite for meth, have increased dramatically in the last two to three years. One weekend in 2013 acutely demonstrated these changes. The Fort Peck Reservation, in the course of one weekend, witnessed a sudden and violent uptick in criminal activity—everything from burglaries to assaults. Once subjects were in tribal custody that weekend, many acted erratically, violently, and exhibited paranoid behaviors. Perplexed jail staff watched as a steady stream of increasingly unhinged subjects were booked. Jail staff hypothesized that a "bad batch of meth" had arrived on the reservation. Ironically, with additional investigation, law enforcement discovered that the cause of the civil and mental unrest was not, in fact, "bad meth," but extremely good meth. Earlier in the weekend, someone began distributing extremely pure meth, something many of its consumers were unaccustomed to.

Much as any entrepreneur would open shop in a new area of town with booming business potential, drug traffickers and other criminals have seized on a unique modern moment in history—the opportunity to sell their poison in a vast area that, by early accounts, seemed unburdened by the concepts of law and order. It's Montana, right?

Wrong. Within the last 21 months, the USAO for the District of Montana has prosecuted approximately 120 Bakken-related drug cases, roughly 80 percent of which are methamphetamine-related. Another estimated 100 indictments are anticipated in the coming year. Those indictments and projected numbers involve drug offenses only, and do not even include the myriad of non-drug offenses, including fraud and environmental and violent crime cases with ties to the Bakken.

The remainder of this article is devoted to outlining successful law enforcement and prosecutorial responses to Bakken crimes. Though they might not come in the same form as the oil boom, sudden criminal influxes like that experienced in the Bakken can instruct other districts as to what works and does not work when a shift in criminal activity demands an adjusted law enforcement and prosecutorial response.

III. Solutions for the 21st century

If the Gold Rush metaphor for the Bakken doesn't strike a chord, consider the comments of retired General David Petraeus after the former CIA director visited the area's oil patch communities. "He (Petraeus) said, 'You know, this kind of looks like a war zone.' " Associated Press, *Petraeus compares Bakken oil patch to 'war zone,'* BILLINGS GAZETTE (Sept. 26, 2014), *available at* http://billings

gazette.com/news/state-and-regional/montana/petraeus-compares-bakken-oil-patch-to-war-zone/article_36d28b49-515b-5878-9c25-be9fcc29feae.htm. The law enforcement response to the Bakken, in many ways, has been to mobilize much like an army's response in a violent war zone. Money and resources must be marshalled quickly, and coordinated efforts require funding, political support, and community understanding.

The groundwork for Montana's response to the Bakken in Indian Country was established as early as 2009, when the USAO for the District of Montana implemented a strategic plan with the goal of enhancing communication, prosecutions, and law enforcement response to violent and sexual crimes in Indian Country. As part of the strategic plan, federal prosecutors in Montana have been travelling to their assigned reservations once a month, at minimum, to staff cases, discuss law enforcement and victim issues, and engage in subject-specific meetings related to high-frequency crimes on the reservation. The first of those teams is called the Multidisciplinary Team, which focuses on sexual crimes against children in Native communities. These meetings, typically held once a month, involve federal and tribal prosecutors, federal and tribal law enforcement personnel, psychologists, social workers, and victim advocates, among others. A master list of cases is kept and discussed each meeting. In 2013, the same type of team was developed for adult sexual assaults and is called the Sexual Assault Response Team. This team also meets once a month to review adult sexual assault cases and collaboratively staff cases and discuss issues as they arise. The team tracks and staffs cases from the time the crimes are committed through the entire prosecution and sentencing process.

Beyond the positive effect this collaboration has on individual cases, its broader, long-term effect is immeasurable. Working relationships between team members are built across time and consistent face-to-face interactions. The trust and mutual respect that develops guide and inform later discourse and disagreements between members of the group. At the end of the day, regardless of the outcome, tribal and federal partners move forward with a joint mission, knowing that team members believe in the collective mission of enhancing the public safety and well-being of the community. These relationships result in candid conversations and solution-building. The strategic plan implemented in Montana has transformed the law enforcement landscape in Indian Country. The Federal Government is no longer a faceless voice at the other end of a telephone call. With frequent communication between Indian Country partners, prosecutors are better able to get ahead of criminal trends in the community, including anticipating the ways the Bakken has changed the criminal enterprise on reservations.

Recent federal funding flowing into the Bakken region has also helped communities surrounding the Bakken anchor themselves for the impending criminal storm. On August 26, 2014, Associate Attorney General Tony West announced $3 million dollars in grants from the Office on Violence Against Women (OVW) to increase local and tribal capacity to prosecute crimes of violence against women and provide services to victims of sexual assault, domestic violence, and stalking in the Bakken Region of Montana and North Dakota. Of the five groups awarded grants, two are from Montana: the Fort Peck Assiniboine and Sioux Tribes and the Montana Coalition Against Domestic and Sexual Violence. The Assiniboine and Sioux Tribes of the Fort Peck Indian Reservation will also receive a 3-year $450,000 grant to support the salary, travel, and training costs of a tribal prosecutor, who will be cross-designated to serve as a tribal Special Assistant U.S. Attorney in the USAO for the District of Montana.

OVW's Bakken Region special initiative launched in April 2014 and is the first large-scale project targeting resources to support the expansion of services to victims of sexual assault, domestic violence, and stalking, as well as aid the local criminal justice system in responding to these crimes in the Bakken region. With Department of Justice (the Department) funding, these grantees will be able to enhance responses to domestic violence, dating violence, sexual assault, and stalking, and expand mental health assistance, advocacy, legal assistance, prevention education, sexual assault forensic examiner programs, Sexual Assault Response Teams, and law enforcement training. The grants are part of the Department's ongoing commitment to protecting women from violence and strengthening the capacity of communities to respond to domestic and sexual violence.

In April 2012 the USAOs for the Districts of Montana and North Dakota convened a law enforcement strategy session in Glasgow, Montana, to address the exponential rise in Bakken region crime. Glasgow is located near the far northeastern border of Montana at the edge of the Bakken boom. More than 150 federal, state, local, and tribal law enforcement personnel from Montana, North Dakota, and Canada attended the meeting. Its focus was to develop and implement a cohesive law enforcement strategy to combat organized crime in the Bakken region.

Project Safe Bakken's mission is to synchronize the law enforcement efforts between federal, state, local, and tribal law enforcement entities. The purpose is to detect, disrupt, and dismantle organized criminal enterprises that distribute illegal drugs and commit other crimes in the Bakken region. To that end, law enforcement, including the U.S. Attorneys for Montana and North Dakota, the Attorney Generals for Montana and North Dakota, the Drug Enforcement Agency (DEA), the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Bureau of Indian Affairs, the U.S. Border Patrol, the U.S. Marshals Service, the Environmental Protection Agency Criminal Investigation Division, the Department of Homeland Security, the Montana Division of Criminal Investigation (MDCI), and the North Dakota Bureau of Criminal Investigations, have joined forces to share intelligence and combat crime in the Bakken region and affected communities, including the Fort Peck and Fort Berthold Indian Reservations. The National Guard assists these efforts by providing intelligence support, including collection, analysis, and dissemination of intelligence data.

Collaborative efforts, however, are not immune to difficulty. A task force's composite parts are, after all, human. Project Safe Bakken has demonstrated and addressed such difficulties, which include gaining cooperation from both state and federal colleagues, limited investigative resources in remote parts of the country, the sheer distance to be traveled to reach an investigative site, and political opposition against federal involvement. Some of these challenges are born from the reality that the Bakken has generated tremendous revenue for the area. In the eyes of some, regulation, enforcement, and prosecution will put a damper on the business and regional success ushered in by the Bakken. The remaining challenges are natural. From Montana's capital, Helena, it takes more than seven hours of driving to reach the edge of the Bakken area which, coincidentally, still places the driver in Montana.

Task force efforts are, therefore, even more critical in the face of the dual challenge of manmade and natural obstacles. These collaborative efforts apply to a range of cases and produce a myriad of benefits. With increased communication between invested parties, investigators and prosecutors can determine whether there may be violations in more than one program, resulting in increased charging options and flexibility. With the Bakken extending across multiple jurisdictions, Project Safe Bakken also enhances law enforcement's ability to weed out criminal activity that may occur in one or more jurisdictions. Single acts in one jurisdiction may not look criminal when viewed as an isolated event. However, if subjects are evaluated and investigated across jurisdictions, the big picture may reveal a broad criminal scheme that is wholly illegal when viewed against the subject's criminal backdrop. Lastly, early coordination among law enforcement helps avoid missed investigative opportunities and creates a better prosecutorial result at the end of the day.

Between Montana and North Dakota, the Bakken has given birth to over 450 federal prosecutions —from drugs and guns to fraud and human trafficking—in the last 2 years alone. The cases are significant and so are the sentences. Take, for example, Tomas Alvarado and Eliseo Lopez Martinez, sentenced to 30 and 27 years, respectively, for trafficking over 90 pounds of methamphetamine into Montana in a 6-month period. Law enforcement searches in the case also yielded 16 firearms, including handguns, shotguns, and rifles (including two semi-automatic, SKS assault-style rifles). The prosecution of Alvarado and Martinez was part of Project Safe Bakken, and was the result of the collaborative efforts of at least eight different investigative entities, including the FBI, DEA, MDCI, the ATF, various drug task forces based in Billings, Billings Police Department, Yellowstone County Sheriff's Department, the Montana Highway Patrol, and the Idaho State Police. Press Release, Salt Lake City Div., Fed. Bureau of

Investigation, Tomas Alvarado and Eliseo Lopez Martinez Sentenced in U.S. District Court (Oct. 21, 2013).

The story of Alvarado and Martinez is startling by any account, yet it represents just the tip of the iceberg of a larger Bakken tale: out-of-state "entrepreneurs" descending on a market ripe for criminal and financial gain. No corner of the Bakken is immune from this human greed, including Montana's most renowned quality—its vast natural allure and geography. Enter Mike Campa and Steven Carpenter, two out-of-state "entrepreneurs" who stole more than $670,000 from over 50 elderly and otherwise vulnerable individuals across the United States with a telemarketing scheme touting fictional oil investment opportunities. The defendants then applied their ill-gotten riches to fund lavish vacations to St. Thomas, Hawaii, and the Dominican Republic. The fraudulent telemarketing scheme operated from 2006 until the summer of 2012, when federal agents shut it down. Campa and his associates promised investors that they had oil and gas leases with the prospect of production and refining on the Fort Peck Indian Reservation. The group sold interests in the promotion to investors from all over the United States. In truth, Campa's leases were never valid (for failure to follow procedural requirements), and to the extent they were available, they were cancelled in 2007. Press Release, U.S. Attorney's Office for the Dist. of Mont., U.S. Dep't of Justice, Bakken Oil Lease Telemarketer Mike Campa Sentenced to 30 Years Without Parole (Jan. 30, 2014).

As an example of the mechanics of the fraud, a victim received the following email, titled "Montana Oil," from Carpenter.

> [E]ach $30,000.00 investment will entitle you to a 1% ownership in US Oil and Gas and all income generated on the Ft. Peck Indian Reservation. Each percentage will also include income generated by all oil and natural gas, our drilling rigs, a 20,000 bpd refinery, pipelines and other land leases. You will recoup your initial investment within 120 days of completion and monthly checks thereafter of at least 5 percent. Upon receipt of your funds, payable to U.S. Oil and Gas, we will file your name with the Bureau of Land Management in Montana, and they will in turn forward you the necessary paperwork and contacts. Attached is our official letter of intent and other documents. Check out this confidential report . . . Thankyou (sic) for your Trust and Confidence. We look forward to sharing our success with you. Steve Carpenter.

Id.

On February 17, 2012, a person who suspected he may have been a victim of the Campa/Carpenter oil and gas scheme made a referral to the U.S. Department of the Interior's Office of Inspector General. On March 1, 2012, a phone call was made to Steve Carpenter that was monitored by federal agents. During the phone call, Steve Carpenter assured the investor that there was "zero chance" that the investor would lose the money that had been committed to the investment with U.S. Oil and Gas, LLC, the company to which the lease belonged. *Id.* Carpenter told the investor that "everything was going perfect" with U.S. Oil and Gas and the Fort Peck investment. *Id.* Carpenter advised that he was going to have a conference call on March 5, 2012, with the Fort Peck Tribe in order to finalize everything so that the drilling could begin.

As an example of the collaborative investigative efforts born from the Bakken, the FBI and Department of the Interior's Office of Inspector General initiated a joint undercover investigation of Steve Carpenter, Mike Campa, Suzette Gal (his wife), and Andras Gal (his son) in April 2012. The undercover agent (UA), posing as a watercraft broker from South Carolina willing to invest in the oil and gas project at Fort Peck, arranged to meet Carpenter in person to deliver a $43,000 check. The two men met in a hotel room in Yorba Linda, California, in August 2012. Their meeting was video and audio recorded by FBI agents. During that meeting, Carpenter told the UA that the project was on the cusp of fruition and that he had received $158 million dollars in loan commitments from banks in Central and South America.

Carpenter assured the UA that he had three rigs on site and that he was working closely with the Bureau of Land Management, the Bureau of Indian Affairs, and the local tribes.

Immediately after the meeting, FBI agents arrested Carpenter. Campa, Suzette Gal, Andras Gal, and Krisztian Gal were arrested later that day. Between October 2009 and May 25, 2012, the Fort Peck oil and gas schemes (Domestic Energy Solutions and U.S. Oil and Gas) garnered the defendants approximately $673,406 in monies from investors. All four were charged. Campa pleaded shortly before the trial of his wife and adult sons. He was sentenced to 30 years in prison and $5,175,406 in restitution. Steve Carpenter, who had a criminal history for committing telemarketing fraud dating back to the early 1990s, was convicted on all counts and sentenced to 188 months in August 2013. Suzette Gal was convicted and sentenced to 10 years in prison in August 2013. Andras Gal was convicted on all counts and sentenced to six years in prison. In December 2013, Krisztian Gal, who was convicted of conspiracy to commit fraud, was sentenced to five years in prison. All have appealed their convictions.

In a statement to the press U.S. Attorney Mike Cotter stated:

> This sentence puts an end to Mike Campa's chances to prey on others. Telemarketing fraud is a uniquely deplorable crime—from the sophistication and thought it requires to construct and execute to the vulnerability of the people it targets. Campa's victims included the elderly looking for a chance to pass along a nest-egg to their children and the desperate caring for a sick loved one or facing foreclosure. People like Mike Campa and Steve Carpenter feed on hope and live on other peoples' dreams—enjoying the high-life while condemning their victims to poverty.

Id.

The Campa/Carpenter case was part of a large-scale Montana-based U.S. Attorney's Office project called The Guardians, which capitalized on the successes and concept of intra-agency collaboration. Abandoning the traditional model of "You work your case and I'll work mine," several agencies committed themselves to long-term mutual cooperation. In the case above, the FBI collaborated with the Department of the Interior, as well as tribal law enforcement contacts, to successfully bring justice to the community and the victims the defendants so callously robbed.

These collaborative techniques, unsurprisingly, translate to other types of cases, including the investigation of environmental crimes, which often slip under the Bakken radar as a result of the vast Montana geography and challenging political climate. As recently as September 2014, a Kalispell, Montana, man pleaded guilty in federal court to 11 felony counts, including false statements, defrauding the United States, and violating the Safe Drinking Water Act. The defendant, Nathan Garber, operated a saltwater disposal well near Dickinson, North Dakota. The well received "produced water" constituting "brine and other wastes" commonly referred to as "saltwater." Press Release, U.S. Attorney's Office for the Dist. of Mont., U.S. Dep't of Justice, Operator of Saltwater Disposal Well Pleads Guilty to Multiple Felony Charges in Connection With Operation of the Well (Sept. 26, 2014). In the Bakken, that term covers a wide array of drilling waste fluids, including hydraulic fracturing fluid, which is water combined with chemical additives such as biocides, polymers, and "weak acids." *Id.* The Environmental Protection Agency has emphasized that the water is often saltier than seawater and can "contain toxic metals and radioactive substances." *Id.* According to the offer of proof, Garber admitted to conspiring with others to commit illegal acts. Garber injected saltwater into the well without first having state authorities in North Dakota witness a test of the well's integrity. Garber also violated a 2012 order from the state to stop injecting until a well integrity test was done. When questioned by the state, Garber made false statements by claiming these injections never occurred.

The well failed a pressure test in February 2012. Nevertheless, Garber continued to inject saltwater, even though he knew the well did not have integrity and thus posed an increased risk of contaminating ground water. Garber also moved a device that is intended to maintain the integrity of the

well and ensure wastewater does not escape into surrounding soil and groundwater. Garber then gave false information to a state inspector regarding the depth of the device. A search warrant revealed that the device had been moved upward and the saltwater had subsequently been injected into the well until a state employee shut down the well. The Garber investigation was the result of the combined efforts of the U.S. Environmental Protection Agency's Criminal Investigation Division and the North Dakota Industrial Commission. These state-federal joint investigations represent a common and successful means of ensuring environmental criminal activity does not fall through the cracks.

IV. Conclusion

As illustrated above, the Bakken has simultaneously brought out the best and worst in human nature. It has demanded all divisions of law enforcement to recalibrate their resources and techniques. The lessons of the Bakken—face-to-face interactions, cross-jurisdictional and agency investigation teams, outside-the-box charging techniques, and the willingness to go the extra mile(s) (literally)—readily translate to the evolving criminal enterprises across America's districts. The techniques and lessons from these early years of the Bakken represent only the beginning of the area's adapting response to this new Gold Rush. It is estimated that the Bakken will continue to yield oil for, at a minimum, another 20 years. The District of Montana and its sister districts will continue battling the criminal forces that saturate the Bakken in order to prevent the past from repeating itself. ❖

ABOUT THE AUTHOR

❑ **Laura Weiss** is an Assistant U.S. Attorney in Helena, Montana. She has prosecuted violent crimes on the Blackfeet, Fort Peck, Fort Belknap, and Rocky Boy's reservations, as well as fraud, gun, drug, and wildlife cases throughout Montana. Ms. Weiss has served as an Assistant U.S. Attorney in Montana since September 2010. ✠

Email Memorandum Regarding Gangs and the Border

Stewart M. Young
Assistant United States Attorney
District of Utah

TO: Sweet.Justice@usdoj.gov (AUSA and New Liaison to Border Gang Task Force)

FROM: Pros.E.Cuter@usdoj.gov (Senior Litigation Counsel and Liaison to Border Gang Task Force)

DATE: November 1, 2014

RE: A Welcome and Thoughts/Ruminations on the Border Gang Task Force

---

Dear Ms. Justice,

I want to welcome you to the Border Gang Task Force and provide some of my collected thoughts during my eight years of working with this task force. I hope you'll indulge a "seasoned" (old) prosecutor's perspective on how to work most effectively with the agents on this task force and how to make the most of your limited time and resources. Of course, all advice is free, and you definitely get what you pay for. But, for what it's worth, I hope that some of what I write may be helpful.

I. The border gang prosecutor's toolbox

As an Assistant U.S. Attorney (AUSA) in a border district, one must acknowledge the myriad problems and opportunities that come with certain locational priorities. Along with the crush of cases for most AUSAs (some mundane, some exciting), the issue of gang connections, gang violence, and gang activities often permeates a large amount of federal crime. Many border prosecutors will often come across gang-related criminal activity or gang-affiliated targets and defendants in their career. Accordingly, taking a walk through the plethora of resources available for prosecuting such gang-affiliated individuals and targets can be instructive.

As you begin working on this Border Gang Task Force, you will find that "big" and "small" cases alike can make a difference. Some prosecutors seek "big" indictments, using the Racketeer Influenced and Corrupt Organizations Act (RICO), the Violent Crimes in Aid of Racketeering statute (VICAR), or larger-scale drug conspiracies (including conspiracy, 21 U.S.C. § 846). Those types of cases are terrific if you have the prosecutorial resources, the agent support, and the Department of Justice (DOJ) and U.S. Attorney's office support to prosecute them. RICO and VICAR are great tools to take down larger-scale organizations and conspiracies encompassing many local border gangs. Indeed, using these types of statutes and charges against groups like La Eme (Mexican Mafia), MS-13, La Familia, Barrio Azteca, Texas Syndicate, and other larger-scale and Mexican drug cartel-connected groups generally can have a great local, and often national, impact. It has become clearer over time that a number of the local border gangs have ties, sometimes direct, to these types of organizations. Accordingly, by using resources and assistance from DOJ's Narcotics and Dangerous Drugs Section or its Organized Crime and Gang Section, one can effectively dismantle, disrupt, and destroy larger-scale border gangs with larger-scale indictments. DOJ provides a number of helpful resources relating to these types of cases, and I recommend you become familiar with them as you begin your career as part of the Border Gang Task Force. For example, manuals for federal prosecutors working on cases involving RICO or VICAR are

available at http://www.justice.gov/criminal/foia/docs/2009rico-manual.pdf and http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/vcar.pdf, respectively.

There are also a number of resources more widely available relating to gang activities in this district, throughout the United States, and even internationally. I urge you to peruse these resources so that you can "talk the talk" with your agents, cooperators, and targets. Additionally, given the proximity to the border, it is important to be familiar with the research and intelligence on the Mexican drug cartels and organizations. Some of them are more academic than others, but the more information you consider and absorb, the better your ability to dismantle, disrupt, and attack the various gangs in this District. Some of these resources are provided below:

- Los Zetas and La Familia Michoacana Drug Trafficking Organizations (DTOs) by Albert De Amicis, *available at* https://www.ncjrs.gov/pdffiles1/234455.pdf.
- The MS-13 and 18th Street Gangs: Emerging Transnational Gang Threats? by Celinda Franco, *available at* http://fas.org/sgp/crs/row/RL34233.pdf.
- Gangs in Central America by Clare Ribando Seelke, *available at* http://fas.org/sgp/crs/row/RL34112.pdf.
- Mexico's Drug Cartels by Colleen W. Cook, *available at* http://fas.org/sgp/crs/row/RL34215.pdf.
- International Drug Control Policy: Background and U.S. Responses by Liana Sun Wyler, *available at* http://fas.org/sgp/crs/row/RL34543.pdf.
- Mexico's Drug Trafficking Organizations: Source and Scope of the Violence by June S. Beittel, *available at* http://fas.org/sgp/crs/row/R41576.pdf.
- Southwest Border Violence: Issues in Identifying and Measuring Spillover Violence by Kristin M. Finklea, *available at* http://fas.org/sgp/crs/homesec/R41075.pdf.
- Southwest Border Gang Recognition by Sheriff Sigifredo Gonzalez, Jr., *available at* http://www.senate.state.tx.us/75r/senate/commit/c640/wtpdf/1108-SigifredoGonzalez-2.pdf.

Additionally, DOJ provides helpful resources on gangs in the U.S. Attorneys' Bulletin every few years. I recommend reading these when they are published in order to be familiar with case studies from other districts, to understand the discussions on useful strategies for prosecutions and investigations, and to absorb other helpful and interesting tidbits. Three issues are provided by the DOJ's Office of Legal Education, Executive Office for United States Attorneys:

- Gang Prosecutions, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab6203.pdf.
- Gang Issues, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5604.pdf.
- Gangs, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5403.pdf.

Finally, the National Gang Center is a very helpful resource, and I recommend becoming familiar with the information it can provide at http://www.nationalgangcenter.gov/.

While I know you'll get up to speed on these resources, I want to share a few of my "small picture" thoughts, as well. I believe a good gang task force prosecutor strives for the larger prosecutions, but also uses the "smaller" prosecutions that can make as big a difference, to dismantle, disrupt, and disable the local border gangs. So, I want to focus on these types of prosecutions that can truly affect gang leadership, gang membership, and the quality of life for the folks living in gang-infested territory. These types of prosecutions include firearms violations, criminal alien and alien smuggling, human trafficking, identity theft, bulk cash smuggling, and the gang enhancement statute.

A. Firearms prosecutions

One vitally important tool in the border prosecutor's toolbox is the use of firearms-type prosecutions. Such prosecutions are generally codified at 18 U.S.C. § 922, which currently regulates firearms trafficking. Oddly enough, the term "trafficking" does not appear in the Gun Control Act except when referring to "drug trafficking." *See* 18 U.S.C. §§ 924(c)(1), 924(h), 929 (2014). The bread and butter of the border gang prosecutor in the firearms arena will be Possession of Firearms (and Ammunition) by Prohibited Persons, codified at 18 U.S.C. § 922(g) (generally referred to as "felon in possession"). Your task force agents will often bring cases to you involving some gang-affiliated target that has just been caught with a weapon, and it will be your job to determine whether such a prosecution makes sense vis-à-vis office resources, evidence, potential sentence, and any other concerns. These are generally easy cases as long as one can prove the possession of the firearm, and I recommend filing them if you feel the requisite prison sentence will aid in the disruption or dismantling of the gang's activities.

Additionally, § 922 criminalizes a number of other activities relating to firearms, including (with certain caveats) being "engage[d] in the business of importing, manufacturing, or dealing in firearms, or in the course of such business to ship, transport, or receive any firearm in interstate or foreign commerce." 18 U.S.C. § 922(a)(1)(A) (2014). This provision makes it illegal for "any importer, manufacturer, [or] dealer . . . to ship or transport in interstate or foreign commerce any firearm to any person other than" a licensed firearm trafficker. *Id.* § 922(a)(2). (The term "licensed trafficker" is not a definitional term in the statute. It is merely a descriptive term for purposes of this email for a person who is a "licensed importer, licensed manufacturer, licensed dealer, or licensed collector." *Id.* For these exceptions, I like to use the term "legal trafficker" or "licensed trafficker."). Thus, the statute criminalizes the transport or receipt of any firearm purchased or obtained in another state, as well as the transfer, sale, or trade of a firearm to another person who does not reside in the state where the transferor resides. *See id.* § 922(a)(3), (5). Finally, the "lie-and-buy" statute—another staple of firearms prosecutions—criminalizes the "acquisition or attempted acquisition of any firearm" by knowingly making "any false or fictitious" statements to acquire a firearm. *Id.* § 922(a)(6). This provision criminalizes both lying to procure a firearm for oneself and the lie itself. Finally, § 922 criminalizes other activities by licensed traffickers, including the disposition or sale of any firearm to any person who is under indictment, has been convicted of a felony, is a fugitive from justice, abuses narcotics, or is an alien unlawfully present in the United States. *Id.* § 922(d)(1)–(3), (5). Section § 922(d)(5) also criminalizes sales to an alien that has a non-immigrant visa, which is a little less likely in our scenarios.

As you can guess, § 922 is a cornucopia of prosecutable offenses relating to local border gangs. Anytime a gang member is trying to transport weapons across state lines (including to Mexico), § 922 is available. Anytime a gang member tries to procure a firearm through a friend's or a significant other's purchase (a lie-and-buy), § 922 is available. And, while some of the border gang members may not have the criminal records to warrant a felon in possession charge, they may possibly be charged based on their immigration status (or non-immigrant status, as the case may be). Thus, § 922 will be very useful as part of the Border Gang Task Force prosecutor's toolbox.

While on this Border Gang Task Force, you will rely a great deal on liaisons from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) when investigating firearms cases. However, the ATF is not necessarily the sole agency responsible for focusing on firearms trafficking. While the ATF has primary responsibility, Homeland Security Investigations (HSI) (like its predecessor, Immigration and Customs Enforcement, and its predecessor, the U.S. Customs Service) is responsible for enforcing U.S. export laws, including "enforcing laws related to the export of military items and dual-use goods." *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-709, FIREARMS TRAFFICKING: U.S. EFFORTS TO COMBAT ARMS TRAFFICKING TO MEXICO FACE PLANNING AND COORDINATION CHALLENGES, 11, n.6 (2009). HSI has historically promoted public awareness of firearms trafficking to Mexico, but it generally does not engage in law enforcement efforts similar to those of the ATF. The Customs and Border

Protection (CBP) or Border Patrol liaisons can also play a role in helping to intercept southbound illicit firearms at the border and assist in the prosecution of gang-related individuals trying to send firearms southbound to the cartels. Nevertheless, it is important to note that the current legal regime for firearms trafficking offenses focuses solely on "dealing in firearms," and our U.S. Criminal Code lacks an effective "trafficking in firearms" statute that might be more helpful. *See* Stewart M. Young, *Going Nowhere "Fast" (or "Furious"): The Nonexistent U.S. Firearms Trafficking Statute and the Rise of Mexican Drug Cartel Violence*, 46 U. MICH. J. L. REFORM 1, 8, 18 (2012) (discussing extraterritoriality and U.S. domestic firearms trafficking laws). Nevertheless, § 922 provides a myriad of responses to any gang-affiliated targets that engage in possession, use, or trafficking of firearms. It should be consulted early and often in your career as part of the Border Gang Task Force.

B. Criminal alien and alien smuggling prosecutions

The Border Gang Task Force has two terrific HSI agents, as well as two Border Patrol (BP) agents, who provide terrific support for targeting criminal aliens and alien smuggling relating to border gangs. Given the proximity to the border, a majority of the gangs have non-citizen participants that may have been deported previously. Some of the gangs also engage in assisting the Mexican cartels and other alien smuggling organizations by providing stash houses, transport services, and other material support. Accordingly, it is important to work with these agents to effectively target the activities of these border gangs. Both the HSI agents and the BP agents provide wonderful resources relating to understanding alienage and smuggling issues that might be brought to the attention of the Border Gang Task Force. While some prosecutors may disdain these prosecutions under 8 U.S.C. § 1326 (deported alien found in the United States) or 8 U.S.C. § 1324 (alien smuggling), I particularly enjoy these because they are generally very easy to prosecute and often very effective at dismantling or disrupting local border gangs.

As you get to know the gangs in this Border District, you will begin to see that the majority of gang leadership, and some of the most concerning gang member targets, do not have legal status within the United States. If any of these targets have been deported by an immigration judge, and depending on their criminal record, they can receive substantial prison time for being a deported alien who has returned to the United States. *See* 8 U.S.C. § 1326 (2014). Working effectively with the HSI and/or BP agents on the Border Gang Task Force can make your life much easier because they can provide the appropriate documentation necessary to file the requisite charges under § 1326. And, at least in our district, those § 1326 cases often go to trial, so you'll definitely get plenty of trial experience. Nevertheless, for the most part, these § 1326 cases are incredibly easy to prove: Was the person deported? Do we have the right deport and the paperwork? Did he or she come back? As such, especially if the target subject has an aggravated felony and a hard deport, the sentences can range upwards to 57 months or more. And a 57-month federal prison sentence on a target gang subject that has an extensive criminal history can be quite the deterrent for other members of the gang. Remember, dismantling and disruption of the local border gangs is an important part of the equation, and the criminal alien program can play a vital role in that arena.

The same is true for prosecutions under the alien smuggling statute, § 1324. Your HSI and BP agents can offer terrific agent support in these cases, including the wrangling of material witnesses, providing intelligence on the smuggling operations, and furnishing the needed litigation support. A number of the border gangs engage in alien smuggling by providing alien stash houses in the area, as a way station for the smuggled persons until they are smuggled to their ultimate destination. These stash houses are often kept in deplorable conditions, and the gang members may engage in other criminal behavior by preying on the smuggled aliens who are waiting at these stash houses. Becoming familiar with the issues involved in these types of cases will be important. There are sometimes violent activities (including rapes, beatings, and threats) or extortive conduct that may also fall within the federal rubric. But, remember to work closely with your local District Attorney (DA) contact on the Border Gang Task Force as well, because he or she may be able to get higher state sentences for some of the gang member's

conduct. A close working relationship with both the agents in this arena, as well as the local DA representative, will ensure that the maximum "bang for your buck" can be maintained, while also ensuring that justice is done.

DOJ provides terrific resources to get a handle on criminal immigration and alien smuggling issues. The more familiar you are with these resources and the more practice you have with them, the easier it will be for you to "talk the talk" with the Border Gang Task Force agents. I recommend becoming as familiar as you can with the main DOJ resources available.

- Immigration Primer by the U.S. Sentencing Commission, *available at* http://www.ussc.gov/sites/default/files/pdf/training/primers/Primer_Immigration.pdf.

Other publicly available resources are also helpful to become familiar with the issues surrounding criminal alien and alien smuggling issues, along with the programs targeting those issues.

- Interior Immigration Enforcement: Programs Targeting Criminal Aliens by Marc R. Rosenblum and William A. Kandel, *available at* http://fas.org/sgp/crs/homesec/R42057.pdf.
- Border Security: Immigration Inspections at Port of Entry by Lisa Seghetti, *available at* http://fas.org/sgp/crs/homesec/R43356.pdf.

Given the plethora of gang activity relating to both the criminal alien statute and the alien smuggling statute, familiarity with §§ 1326 and 1324 is necessary and useful, and those statutes should also be consulted early and often in your career as part of the Border Gang Task Force.

C. Human trafficking prosecutions

Recently, border gangs have become more heavily involved in the trafficking in persons, rather than merely engaging in alien smuggling for profit or assisting certain cartels and large-scale alien smuggling organizations. Some gangs' activities have started to merge into the exploitation of minors or other vulnerable populations, often (and usually exclusively) for sexual activity. A number of border gangs have begun to exploit younger women and minors as prostitutes, usually against their will, in order to serve the gang's clients or the gang members. As the proliferation of the use of the Internet for this activity continues to rise, a number of these border gangs have become more technologically savvy and use numerous Web sites to advertise the services of these sexually exploited minors.

While the FBI and other agencies are heavily involved in investigating and prosecuting human trafficking and sexual exploitation crimes, your Border Gang Task Force agents often will be involved in gathering intelligence and other useful information about the border gangs' activities in this arena. If you or your agents ever come across these types of activities, it is valuable to contact the Internet Crimes Against Children AUSA in this District to assist you with this type of prosecution. While these prosecutions are very effective, they are also very taxing and tough for the victims. Using kid gloves is advised, but these are also among the most worthwhile prosecutions to undertake. Given the generally high penalties, including some available mandatory minimums, I would recommend being familiar with these types of operations in order to effectively disrupt, dismantle, and disassemble some of the local border gangs in this District.

Additionally, there are a number of open source and DOJ-sourced materials available to become more familiar with the issues relating to human trafficking.

- Trafficking in Persons: International Dimensions and Foreign Policy Issues for Congress by Liana Sun Wyler, *available at* http://fas.org/sgp/crs/row/R42497.pdf.
- Sexual Exploitation Crimes Against Children by the DOJ's Office of Legal Education, Executive Office for United States Attorneys, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5905.pdf.

D. Identity theft prosecutions

Local border gangs are also becoming more and more adept at *their* version of white collar crime. While most border gangs are not running Ponzi schemes, commodities trading scams, or mortgage fraud, they are increasingly engaging in identity theft for profit. Generally codified at 18 U.S.C. §§ 1028 and 1028A, the identity theft statutes allow for prosecution of persons that take another person's identity and use it to commit fraud or illegally obtain assets. It can include taking someone's name, driver's license, social security number, or another financial instrument number (such as a credit card number). Gangs have begun to engage in these types of activities in greater numbers, given the ease and availability of such identifiers (including by theft of mail or home break-ins). While not as prevalent or easy as some of the crimes identified above, these types of activities sometimes occur within the alien smuggling context, as well (including the use of certain stolen identifying information to provide fake documents to other persons). The DOJ has aggressively attacked identity theft on a number of levels and has also provided resources to improve the understanding of how to use these statutes.

- Identity Theft by the DOJ's Office of Legal Education, Executive Office for United States Attorneys, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5602.pdf.

Understanding these statutes and how gang members engage in identity theft to improve the gang's resources will be beneficial to your tenure as part of the Border Gang Task Force.

E. Bulk cash smuggling prosecutions

Given that a number of local border gangs engage in substantial work either for Mexican drug trafficking organizations or for criminal enterprises such as the Mexican Mafia or La Familia, it is also clear that these groups need methods to send their profits from drug trafficking and other criminal exploits back across the border. As such, a number of local border gangs engage in bulk cash smuggling or money laundering, which can be prosecuted under 31 U.S.C. § 5332 and 18 U.S.C. § 1956, respectively. At least as of 2008, the National Drug Intelligence Center estimated that between $8 and $24 billion of bulk currency was smuggled out of the United States and south to Mexico, representing the proceeds of drug trafficking. *See U.S. Obligations Under the Merida Initiative: Hearing Before the Subcomm. on the Western Hemisphere of the H. Comm. on Foreign Affairs*, 110th Cong. 38 (2008) (statement of Anthony P. Placido, Assistant Administrator and Chief of Intelligence, Drug Enforcement Administration, U.S. Department of Justice), *available at* http://archives.republicans.foreignaffairs.house.gov/110/40659.pdf. Additionally, to aid in the bulk cash smuggling investigative effort, the Drug Enforcement Administration (DEA), along with Customs and Border Protection (CBP) and the Bureau of Alcohol, Tobacco, Firearms and Explosives, has sought to "develop a robust license plate reader program . . . to develop intelligence that identifies and interdicts conveyances being used to transport firearms and bulk cash that are moving south into Mexico from the United States." *Id.* at 36. Furthermore, HSI has put together a National Bulk Cash Smuggling Center to gather intelligence and investigate and disrupt bulk cash smuggling activities, both domestically and abroad.

As part of the Border Gang Task Force, DEA, CBP, and HSI agents on the Task Force can work together (with your help) to yield numerous large scale bulk cash seizures and to disrupt gang operations, as well as cartel operations. As your Border Gang Task Force agents gather street-level intelligence relating to the movement of southbound cash, they can work with CBP and HSI at the border to intercept the cash. Such "southbound operations" are incredibly effective when used in conjunction with local intelligence, and often can be walled off effectively to provide prosecutorial opportunities without exposing significant informant work.

Outbound operations have increased greatly over the past several years, given federal interest in the southwest border. Former Border Czar and former CBP Commissioner, Alan Bersin, reported to Congress that "[o]utbound currency seizures nationwide . . . increased [in Fiscal Year 2009] 74 percent,

surpassing $57.9 million." *See CBP Commissioner Bersin Testifies on Outbound Operational Efforts, Technology and Partnerships to Combat Southwest Border Violence: Hearing Before the Subcomm. on Homeland Security of the H. Appropriations Comm.*, 111th Cong. (2010) (statement of Alan Bersin, Commissioner, U.S. Customs and Border Protection), *available at* http://www.cbp.gov/about/congressional-resources/testimony/bersin-border-violence. Given the addition of more CBP officers and new technology to the ports of entry, including the implementation of CBP's License Plate Reader program, "southbound operations" have been increasingly effective at identifying and stopping the flow of southbound cash. Additionally, beginning in 2009, CBP created the Outbound Programs Division to target not only the outbound flow of currency, but also the outbound flow of firearms, stolen vehicles, and fugitives, for which Congress provided approximately $47 million to CBP. Thus, the mechanisms for targeting southbound bulk cash smuggling are in place to work effectively with the intelligence provided by Border Gang Task Force agents, all of which will aid in thwarting gang activity.

While bulk cash smuggling is still king, prepaid debit card use has expanded in the money laundering world and threatens the status quo. The Financial Crimes Enforcement Network has taken a "hands-off regulatory approach to prepaid cards," even though a "growing realization [exists] here and abroad that prepaid debit cards and similar devices represent a significant and growing money laundering threat." *See* Courtney J. Linn, *One-Hour Money Laundering*, 8 U.C. DAVIS BUS. L.J. 138, n.195–96 (2007) (analyzing 18 U.S.C. § 1960 that criminalizes conducting a money transmitting business without a requisite state license). At least one commentator has questioned whether these prepaid debit cards fit within the definition of "money" in 31 C.F.R. § 103.23 (which requires the filing of currency or money instrument reports for transnational transactions of more than $10,000) and 31 C.F.R. § 103.11(h) and (u) (which defines "currency" and "money instruments," respectively). *See id.* at n.207. Given that these cards do not appear to be a demonstrable form of currency or a monetary instrument, some target defendants charged with smuggling large amounts of money on these prepaid cards may claim that they are "therefore not subject to the currency and monetary instrument reporting (CMIR) requirements." *Id.* at n.196. Accordingly, this is an area wherein an enterprising Border Gang Task Force prosecutor could pave the way for new thoughts and ideas on how to prosecute these types of smuggling transactions. While some believe that the way these prepaid debit cards are defined "makes them an excellent alternative to currency as a device for avoiding punishment and forfeiture for CMIR and bulk cash smuggling violations," *id.*, the case law surrounding these transactions is young enough for a good AUSA to help the courts develop theories of prosecution. Becoming familiar with these statutes, and looking for ways to use them against local border gangs will be a useful tool in your border crime arsenal.

II. Gang enhancement statute

Generally, I have not found the gang enhancement statute as useful as a number of the charges and statutes discussed above. Found at 18 U.S.C. § 521, the gang enhancement statute provides for an increase by up to 10 years in the maximum penalties for certain underlying offenses. The underlying offenses must be committed by the defendant(s) with the intention of furthering the activities of the gang or to maintain or advance their position within the gang. Akin to RICO and VICAR prosecutions, the prosecutor is tasked with proving the existence of the gang, which may be helpful in providing evidence to the jury about the gang's activities, methods, and goals.

The use of the gang enhancement statute provides for increased maximum penalties, but it may not provide much utility in RICO, VICAR, and drug cases. It might be useful in conjunction with some of the statutes discussed above if they were described in 18 U.S.C. § 521 as underlying offenses. Unfortunately, the statute includes only controlled substance offenses or "[f]ederal felony crime[s] of violence," which generally have a relatively high maximum sentence anyway (or a mandatory minimum). Thus, a number of the other charges and statutes discussed above are not included as underlying offenses for the gang enhancement statute. At least one commentator has questioned the statute's constitutionality in light of more recent Supreme Court precedent, so it is important to continually monitor recent Court

rulings if you find yourself using this statute. *See, e.g.*, Jennifer E. Fleming, *Your Honor, I Seen Him With That Gang: The Constitutionality of the Federal Criminal Street Gang Statute in the Wake of* Apprendi v. New Jersey, 18 WM. & MARY BILL RTS. J. 249, 267 (2009). Additionally, several commentators have addressed state-related gang enhancement statutes, and their commentary on these statutes may be instructive in how to effectively (or ineffectively) use the federal gang enhancement statute. *See, e.g.*, Martin Baker, *Crips and Nuns: Defining Gang-Related Crime in California Under the Street Terrorism Enforcement and Prevention Act*, 40 MCGEORGE L. REV. 891, 892 (2009); Erin R. Yoshino, *California's Criminal Gang Enhancements: Lessons from Interviews With Practitioners*, 18 REV. L. & SOC. JUST. 117, 117–119 (2008). While I have not seen the utility of § 521 as much in my practice, it is important to understand the statute, its contours, and its ramifications in case it comes in handy for one of your future prosecutions.

III. Conclusion

Ms. Justice, I really look forward to working with you more closely on the Border Gang Task Force. I have also heard that many of the Border Gang Task Force agents are eager to work with you, given your terrific reputation from your work in the General Crimes Unit over the past several years. I hope you didn't find this email too overwhelming or ill-formed; I just want to share some of my thoughts on working with our Border Gang Task Force and provide you with some of the things that have worked for me in this position over the last several years. Feel free to chat with me further about any questions, comments, or concerns you might have going forward.

All the best and good luck,

Pros E. Cuter
Pros E. Cuter
Senior Litigation Counsel
U.S. Attorney's Office❖

ABOUT THE AUTHOR

❑**Stewart M. Young** currently serves as an Assistant U.S. Attorney in the District of Utah. Prior to joining the Utah office, Mr. Young served as a tenure-track law professor at the University of Wyoming College of Law and as an Assistant U.S. Attorney in the Southern District of California. In San Diego, he served as one of the Assistant U.S. Attorney-liaisons for both the North County Gang Task Force and the Major Mexican Narcotics Trafficking Task Force. ✠