STRATEGIES
The Prosecutors' Newsletter

AEQUITAS

Issue #25 • April 2025

Utilizing Eavesdropping Warrants to Successfully Investigate and Prosecute Sex Traffickers

A Practical Guide to a Valuable Tool that Holds Perpetrators Accountable Without Requiring the Testimony of a Victim

Jennifer Dolle and Jennifer Newman[1]

Criminal justice professionals face a variety of challenges when investigating and prosecuting human trafficking cases. One of the most difficult of these challenges to overcome is building cases that allow prosecutors to hold offenders accountable when victims are justifiably too scared or traumatized to participate in an investigation and prosecution. Law enforcement officers should therefore strive to build cases that stand on their own, with or without victim testimony. Whether a victim testifies or not, live and surreptitious interception of offender communications is a way for officers to continue to work a case and collect evidence to build a strong prosecution. When victims do testify, evidence obtained from a wiretap can be crucial to support their credibility before a jury, and in the event that a prosecutor is presenting a case without a participating victim, such evidence may be able to fill in the gaps to prove the charge beyond a reasonable doubt. A wiretap may produce key evidence of a target's role in an organized trafficking scheme or of the guilt of an actor working alone. They may provide crucial out-of-court statements that can help prosecutors convict a trafficker. Wiretaps may also identify other crimes the trafficker is committing, enabling prosecutors to hold offenders accountable for the full range of their criminal conduct or allowing alternative charges when trafficking offenses are unable to be pursued without victim testimony. This article provides law enforce-

ment officers and prosecutors with an introductory and practical overview of obtaining eavesdropping warrants and utilizing the resulting evidence.

Because of the dynamics and illicit nature of human trafficking, especially in the commercial sex industry, much of the force, fraud, or coercion needed to prove the crime of sex trafficking occurs behind closed doors or over electronic devices and can be difficult to obtain and present at trial without a victim's agreement and testimony.[2] Prosecutions involving wiretaps are highly technical, costly, and labor and time intensive. However if done properly, they are incredibly effective at securing this crucial evidence against traffickers and enable law enforcement officials to hold some of the most violent and manipulative perpetrators accountable without requiring the testimony of victims to stand alone.[3]

OBTAINING AN ELECTRONIC SURVEILLANCE ORDER

Communications that may be Intercepted by a Wire

Intercepted statements, including those that may initially seem benign, may be admissible to prove the element of coercion or the interconnectedness of co-conspirators. While a trafficker may use threats of direct violence, and certainly those would be strong evidence when intercepted on a wiretap, coercion can be significantly more subtle as well.[4] Evidence of coercive behavior may manifest in the form of anything from "check-ins" informing traffickers of their location throughout the day and night, constant directives or questions about money, and emotional manipulation based on false promises.[5] These communications may also provide evidence of debt bondage, deception, or other more subtle tactics.[6] Such communications may not be explicitly threatening, but these statements are evidence of coercive control utilized by traffickers to keep their victims subservient to the trafficker, and courts have found them to be admissible as statements made in furtherance of a conspiracy.[7]

Wiretaps are a unique tool to unveil this type of evidence because they allow law enforcement to surreptitiously intercept real-time (or nearly real-time) communications. They can intercept almost any kind of device, including cell phones, computers, and tablets, and they cover a wide variety of communications between those devices. This might include calls over landlines, cell phones, or Voice Over Internet Phone ("VOIP") calls using various applications that can utilize internet services or cellular data to make calls without a SIM card. A wiretap can also intercept text messages, photographs, or videos sent over text or apps and social media communications through applications such as Facebook Messenger or Instagram (though while calls and texts may be intercepted in real time, investigators may experience some delay in intercepting other social media messages).[8]

The Standard for Obtaining an Electronic Surveillance Order

Because of the highly invasive nature of electronic surveillance, a high standard of proof is required to obtain an eavesdropping warrant.[9] While the exact requirements may vary slightly between jurisdictions, those requirements have some common threads. To begin with, no matter the jurisdiction, investigators must obtain a court order as required by their jurisdiction, sometimes known as an eavesdropping warrant or an electronic surveillance order (ESO).

An extensive investigation is typically required to develop intelligence into a viable warrant application. Under federal law, to grant an eavesdropping warrant a judge must determine the following based on the facts laid out in the application: 1) that there is probable cause to believe that the subject is committing, or is about to commit, an eligible offense; 2) that there is probable cause to believe that communications concerning that offense will be obtained through interception; and 3) that normal investigative procedures have been tried and failed or would be unlikely to succeed if tried.[10] State guidelines tend to follow these federal guidelines, though prosecutors should evaluate their state wiretapping statutes to ensure human trafficking offenses are considered eligible offenses in their jurisdiction if they are seeking a wiretapping warrant under state law.

Eligible Offenses

As discussed in more detail later in this article, a wire application must establish probable cause that the subject is committing an offense that is eligible for a wiretap to be authorized to investigate. A wiretap may not be sought in just any case, as they are generally limited to investigations of only the most serious offenses. Prosecutors should consult the relevant statutes in their jurisdiction to determine what sex trafficking-related crimes are designated as eligible.

For example, designated federal crimes are laid out in 18 U.S.C. § 2516(1) and (3) and include crimes such as 18 U.S.C. § 1591 (sex trafficking of children or by force, fraud, or coercion) and 18 U.S.C. § 2421 and § 2422 (related to transportation for illegal sexual activity and related crimes). Similarly, a wire may be used under 18 U.S.C.A. § 2251, which criminalizes the sexual trafficking of a minor, or 18 U.S.C.A. § 2252A (criminalizing the production or distribution of child pornography).[11] If the facts of the case involve organized crime, a racketeering or money laundering charge may also provide the basis for a wire. Having an eligible offense is only the beginning, however.

Acquiring Proof that Communications Concerning the Eligible Offense Will Be Obtained Through Interception

Investigations that end up using wiretaps require a great deal of traditional police work to establish the potential usefulness of a wire. Officers may identify a target based on an analysis of arrest data, a search warrant on a seized device, a pen register warrant, surveillance, or an interview of a victim, even if they subsequently become unable to participate in the investigation.

As discussed further below, seeking a warrant for a wiretap also means that investigators must have already conducted a thorough investigation and have been unable to develop requisite proof of the crimes. In the context of trafficking and related crimes, this might include (but is not limited to) interviewing possible victims or informants, conducting undercover operations and/or physical surveillance, running vehicle or criminal history checks, conducting records checks on hotels or other premises that might be the site of illicit activity, warrants for financial records, conferring with other precincts or jurisdictions for intelligence, executing search warrants, obtaining a pen register warrant, using GPS warrants, reviewing closed cases involving the same individuals, and listening to any pertinent recorded prison calls.[12] This investigation substantially develops the information that will create the probable cause section of the warrant application. Understanding who a potential investigative target may be communicating with and what general role they may play in the larger criminal conspiracy will arm officers to be better able to articulate why a wire is legally justified and practically useful in their case.

> A pen register warrant allows investigators to be more efficient while on their wire (and more effective at minimization) by allowing them to conduct research into the numbers that their target commonly communicates with so that they can better identify who the suspect is speaking to. A pen register can usually be obtained by warrant from a cell phone's service provider and will give investigators a report of what numbers are being called from a particular phone. Similarly, a trap and trace order tracking incoming calls to a phone may be a technique that will provide officers with key information needed to obtain a wiretap order. A pen register showing who the target is communicating with may be a critical piece of evidence in obtaining an ESO; Officers may otherwise have a difficult time demonstrating that a wire will intercept the material communications without providing some basis of evidence for who the target is communicating with.

If, after pursuing all the appropriate and relevant investigative steps, the investigation has not yielded sufficient evidence to prosecute the perpetrators of the offense, law enforcement and prosecutors should analyze whether investing further resources into obtaining an eavesdropping warrant is appropriate.

Exhausting Normal Investigative Means

Under federal law, an application for an ESO must indicate that "normal investigative procedures have been tried and failed or would be unlikely to succeed if tried."[13] Generally, this requires officers to have tried general areas of investigation or be able to articulate why such an avenue would be impossible or fruitless. Such avenues might include (but are not limited to) interviewing victims and informants, conducting undercover operations, physical surveillance of properties suspected to be involved in the offense, running vehicle or criminal history checks, using GPS warrants, obtaining a pen register warrant for the phone of any investigative targets, reviewing closed cases involving the same individuals; and monitoring jail calls, to name but a few avenues by which police work might uncover evidence of criminal wrongdoing on the part of an investigative target. However, this does not mean investigators must pursue avenues they expect will not bear evidentiary fruit. As one Tenth Circuit court held, exhausting normal investigative means might include:

"(1) standard visual and aural surveillance; (2) questioning and interrogation of witnesses or participants (including the use of grand juries and the grant of immunity if necessary); (3) use of search warrants; and (4) infiltration of conspiratorial groups by undercover agents or informants. In addition, if other normal investigative techniques such as pen registers or trap and trace devices have not been tried, a similar explanation must be offered as to why they also would be unsuccessful or too dangerous."[14]

In another Tenth Circuit case, a court found that agents had exhausted their normal investigative means by conducting surveillance of a target and indicating that further visual surveillance would not produce more evidence of the suspected offenses, utilizing confidential informants to collect as much information as possible before noting that they were unable to breach the inner circle of the criminal conspiracy they were investigating; and noting that further attempts to cultivate witnesses might alert the target to the fact that they were under investigation.[15] Similarly, agents reasonably explained their choice to not use grand jury investigation, grants of immunity, or search warrants, believing that the risk that witnesses would lie to the grand jury, claim their Fifth Amendment privilege, or inform principal suspects of the investigation outweighed modest potential evidentiary gains in the case, and that search warrants were not reasonably likely to produce physical evidence of the verbal communications at the heart of the extortion investigation.[16] Similarly, a Ninth Circuit case found that the government's argument that it would not be feasible to obtain an informant or embed an undercover officer deep enough into a drug trafficking organization to yield evidence of wrongdoing was sufficient to show they had exhausted normal investigative means where they had already worked with low-level informants within the organization and engaged in visual surveillance.[17]

Prosecutors are not, however, restricted to seeking a warrant only to make out the bare elements of their charges, or prohibited from seeking a wire when they have minimally sufficient evidence to convict an offender: in *U.S. v. Millner*, the Eighth Circuit reviewed a wiretap that the Drug Enforcement Agency set up to investigate the defendant for trafficking cocaine.[18] The defendant moved at trial to suppress some of the evidence that had been obtained during the execution of the warrant, claiming that the federal government had already had enough evidence to prosecute him, and therefore the continuing wiretaps did not meet the "necessity" requirement. The court agreed that the government had sufficient evidence to prosecute the defendant but was entitled to continue its surveillance to uncover the full scope of the defendant's criminal activity and uncover any other potential targets in their investigation. Another Eighth Circuit case held: "[i]f law enforcement officers are able to establish that conventional investigatory techniques have not been successful in exposing the *full extent* [emphasis added] of the conspiracy and the identity of each co-conspirator, the necessity requirement is satisfied."[19]

Practical Office Considerations

As an investigation into a possible sex trafficking case unfolds and law enforcement or prosecutors come to realize that traditional law enforcement methods have

been exhausted, they may want to consider whether a wiretap is appropriate. Some factors to consider in determining whether a case is appropriate for an eavesdropping warrant include: 1) the size of the organization (a case involving a large criminal enterprise, for example, may be more likely to have a wiretap identify more targets and reveal evidence of criminal wrongdoing, and may be a more attractive target given limited resources), 2) the level of violence in the known criminal activity, 3) the impact prosecution will have on the community, 4) the resources of the jurisdiction,[20] and 5) what charges the prosecutor's office might be able to file and prove without obtaining an eavesdropping warrant.[21]

Whenever a wiretap is being considered, each of these considerations should be carefully weighed on a case-by-case basis to ensure that office resources are being effectively utilized to successfully prosecute these serious offenses.

LEGAL REQUIREMENTS TO FOLLOW WHEN ACTIVE ON A WIRE

Eavesdropping warrants are highly technical to work with. It is imperative to follow all relevant statutes and case law when applying for and executing such a warrant, both to ensure that prosecutors and law enforcement are not running afoul of personal privacy rights, as well as to avoid the risk that any convictions obtained from that information might be jeopardized on appeal. While wiretaps are successful due in no small part to the groundwork of officers who are on the wire, such a warrant can only be approved by a chief prosecutor in the jurisdiction. This means that from the inception, a wiretap must involve law enforcement and prosecutors as equal partners to succeed. It is important that prosecutors and investigators assigned to the case agree upon procedures to be followed during the existence of the wire that will ensure the integrity of the evidence obtained by the warrants.[22] These procedures must be discussed in detail before intercepting any communications and must include instructions on the role of the monitors (including the importance of minimization, which is discussed in greater detail below), the role of field teams conducting concurrent physical surveillance, what to do in case of an emergent situation such as one involving imminent harm to a victim or other community member, and the immediate reporting of other relevant criminal activity that is discussed over the wire but not an enumerated crime in the warrant.

Minimization Requirements

Perhaps the most important requirement associated with wiretaps is ensuring that no investigator enters the wire room to monitor a line without understanding what communications they are authorized by the warrant to intercept and the procedures they must follow to avoid listening to communications they are not authorized to intercept. This process is called "minimization" because it describes procedures designed to minimize the intrusion on the privacy of those individuals whose communications are intercepted. Reviewing courts will analyze the government's actions to determine whether the investigator's efforts to minimize were "reasonable under the circumstances."[23] Specific policies will differ depending on the jurisdiction, but monitors must make the effort to intercept only those communications related to the crimes authorized in the warrant. This typically entails a procedure called "spot-checking," whereby an investigator must stop listening to an interception if it is not authorized but can resume listening for brief periods at fixed intervals to determine whether the conversation has returned to a discussion of criminal activity. In addition, any privileged communications must be minimized. Failure to comply with minimization instructions could result in the exclusion of critical evidence obtained from other calls on the wire.[24] Ensuring that every investigator has detailed information about the key details of the case, the individuals involved, and the specific type of evidence sought is extremely helpful to ensure that minimization procedures are followed.

It is appropriate to listen to calls that mention crimes other than those enumerated in the authorizing warrant,[25] but an application for a retrospective amendment to the warrant must be made to the authorizing judge as soon as is practicable.[26] Under federal law, warrants are authorized for no longer than thirty days;

any applications for extensions of the warrants must be made before the expiration of the active warrant and must comply with all the same legal requirements.[27] In addition, the authorizing judge or pertinent statute may require progress reports to be filed with the court at intervals throughout the existence of the eavesdropping warrants.[28]

The Prosecutor's Role in Wiretap Investigations

Prosecutors should be involved in the decision to seek a wiretap, as it will be crucial for them to work with officers to set and maintain policies surrounding minimization, evaluate evidence to determine when they have enough evidence to conclude the investigation, and set policies surrounding when it is appropriate to intervene if community or victim safety is threatened.

Investigators and prosecutors should communicate daily to stay current on any issues that need to be addressed and to evaluate the evidence being gathered through the eavesdropping warrants. It is imperative to come down off the wire if the communications are not yielding the evidence sought in the warrants. Sealing orders must be obtained from the court whenever interceptions are ceased on any line for any reason to ensure the integrity of the evidence obtained through the authorizing warrant.[29] Unsealing orders can and should be sought in a timely fashion with a showing of good cause or in the interest of justice to comply with discovery obligations and to use the evidence in court.[30] In addition, notice of the existence of the warrants must be provided to the defendant within a specific time frame after arraignment.[31] There are discovery requirements of disclosure to the defendant to use the evidence at trial, but there are also notice requirements as to other intercepted parties on the wire.[32] Prosecutors will be responsible for discovery associated with the wire once the time comes for trial and will need to be involved in the process to ensure that all crucially inculpatory material is handed over to the defense and that all discovery obligations regarding exculpatory evidence are also properly fulfilled.

Wiretaps are expensive in terms of staff hours, equipment, and money.[33] These investigations can be incredibly difficult to conduct in jurisdictions where these resources are limited; prosecutors may be pivotal in interfacing with other agencies and jurisdictions to identify partners to work with to obtain the resources needed to conduct a wiretap. This may include assisting in establishing a collaborative agreement or Memorandum of Understanding (MOU) between two jurisdictions regarding their respective roles and responsibilities, taking on a leadership position as the jurisdiction that intends to try the case, or facilitating information-sharing guidelines.

Prioritizing Victim Safety

A primary consideration while running a wire is always public and victim safety. Prosecutors and law enforcement should anticipate that an electronic surveillance warrant will yield evidence of ongoing criminality and must be prepared to weigh the danger to the victim or the public against the evidence being obtained from the wire. That duty to public safety is always paramount to the goal of building a case, but this constant vigilance is tempered with the humility of understanding what risks prosecutors and law enforcement can abate through their intervention.

There are two categories of potential harms to consider. There are potential harms caused to identified and unidentified victims by the ongoing human trafficking offenses being surveilled, and there are potential harms to trafficking survivors and others in the community resulting from other criminal acts that come to the attention of law enforcement while monitoring the wiretap. Traffickers commit co-occurring crimes: they assault survivors, possess weapons, and rob, steal, and defraud other members of the public. Traffickers also associate with other criminals who sometimes talk about crimes that are not directly related to the sex trafficking conspiracy being investigated on the wire. All parties to the wire execution should be on the same page about when the team will intervene and prevent a crime from occurring. Law enforcement often allows narcotics transactions to occur without intervention while monitoring a wire, but individuals, not drugs, are sold in a human trafficking case, and the human cost to those victims is significant, making each transaction a potential incident in which

law enforcement must intervene. The agencies leading the investigation need to give serious consideration to what will trigger a swift intervention of some form, and they should agree upon a common understanding before "going up" on the wire (the colloquial term sometimes used by investigators to describe the process of electronic surveillance). Intervention may be more likely to be necessary in a situation where someone being exploited in the commercial sex industry is a minor (which implicates mandatory reporting requirements and creates a different level of obligation on the part of investigators) or if someone is being actively assaulted or physically harmed while officers listen. However, there may be some gray areas: for example, whether the team will intercede upon learning about a commercial sex transaction where the potential victim is an adult, and investigators have no evidence of coercion. Not all scenarios can be anticipated, but many can, and it is important to set clear boundaries as to when action must be taken and provide discretion to intervene when exigent necessity arises.

Maintaining the Secrecy of the Wire

While active, only the staff directly involved in obtaining the ESO and monitoring the resulting wiretap should know about the existence of the wiretap and the ongoing investigation into its target or targets. It is of the utmost importance for the quality of the evidence obtained that the target is not alerted to the fact that they are under surveillance, lest they take countermeasures to obfuscate their criminal conduct from surveilling officers.

However, there is always a chance that an intervention designed to protect the safety of the public or a particular victim might cause an investigative target to realize that they are under surveillance. However, even if an arrest is made, law enforcement rarely has reason to disclose the existence of a wiretap in the initial encounter or until a subsequent decision is made to terminate surveillance. It may be possible to intervene without alerting the target to the existence of a wire or a complex investigation: for example, if the wire revealed a minor was being trafficked into the commercial sex industry on a particular street, law enforcement might coordinate with patrol units to do a sweep of the entire street and shut down activity there while appearing to be a "random" crackdown on illicit activity. Whether or not that is possible may wholly depend on the circumstances and nature of the harm being done to the victim. Law enforcement encounters are not uncommon for traffickers and survivors. If there is a documented legal basis for police action, a simple pretext may maintain the viability of the surreptitious wire investigation. A vigilant but creative approach to intervention may avoid the premature disclosure of the investigation to targets if intervention is necessitated. Awareness should also be given to continuing risks to other victims if the investigation is compromised earlier than would be optimal.

If intervention is warranted to actively prevent harm to the community, dealing with the crisis must be done quickly. However, assessing the subsequent status of the investigation and the viability of the wire should be done with cool heads and a careful examination of the circumstances. Such a decision need not be made at the same time as a critical intervention to save a life or prevent the exploitation of a minor. However, some of these situations may be foreseeable enough for investigators and prosecutors to contemplate policies and procedures surrounding them before initiating the surveillance.

TAKEDOWN PLANNING AND CONSIDERATIONS

Many considerations go into planning the conclusion of the eavesdropping warrants once the evidence necessary to prove sex trafficking and related crimes has been obtained. Search warrants should be drafted for any pertinent locations, vehicles, digital devices (such as phones or computers), social media accounts, or persons, and any other jurisdictions that may be affected should be notified. Protective orders should be drafted pertaining to any evidence obtained through the eavesdropping warrants where necessary to ensure the safety of individuals or to maintain the integrity of another related investigation.

Victim safety remains crucial at this stage. If victims are still engaged with the traffickers, the takedown of

the case may be traumatic for them. There should be designated investigators at the scene who are familiar with the case and are trained in how to interact with victims compassionately and in a trauma-informed manner. In a case where law enforcement has engaged in a wiretap, law enforcement usually has much more information than they might ordinarily have about the trafficker, which will allow them to anticipate the offender's tactics and respond accordingly. This includes ensuring that officers are familiar with trauma-informed and victim-centered practices, are collaborating with appropriate service providers, and have qualified interpreters if needed. Any investigators tasked with conducting interviews should have specialized training around trauma-informed interviews and have a plan to conduct interviews at a neutral and safe location. This includes ensuring that officers have a plan for communicating with victims who are not English speaking, either by including officers who can speak the same language as the victims or by working with community services to ensure that investigators can fully and appropriately communicate with any recovered victims.[34] Services must be immediately available. This support should be in the form of service providers, social workers, and medical personnel[35] who can assist as soon as it is safe and practicable.[36] Any statements made by victims to law enforcement at this time should be carefully noted and disclosed in accordance with local laws, whether they contain key inculpatory details or exculpatory information (such as minimization or denial of the offense). A takedown rarely goes as planned but ensuring that meaningful attempts are made to support the victims is essential.

UTILIZING WIRETAP EVIDENCE AT TRIAL

Wiretap evidence can be technical and voluminous, and as a result, it can be difficult to present at trial without extensive preparation and planning. Prosecutors should prepare with officers well in advance of trial – or potentially even in advance of coming off or even starting the wire so that the officers know which officers will testify, what information they can and will be expected to testify to, and how the assigned prosecutor intends to lay out the evidence that is collected on the wiretap. This preparation should happen as early as possible with as much detail as possible, as officers will almost certainly need to take notes and document any details that they will be expected to testify to at trial. Prosecutors should also be prepared to litigate motions surrounding the admissibility of statements obtained while monitoring a wiretap in advance of trial to ensure that the resulting testimony runs smoothly.

Discovery

Wiretaps produce a considerable amount of evidence, often in the form of lengthy audio or video recordings and extensive accompanying transcriptions. The federal rule governing the procedure for a wiretap requires the contents of any wire, oral, or electronic communication intercepted to be recorded on tape or another comparable device if possible.[37] These recordings must be made available to the judge who signed the ESO immediately upon the expiration of the order; such recordings do not, however, need to be immediately turned over to the defense.[38] If an order sealing the recordings is issued, this may delay when the materials must be turned over, but the law requires that prosecutors must ultimately disclose all evidence obtained by the wire that they intend to use in their case in chief and any exculpatory information that may have been overheard during the course of surveillance.[39] In the interest of preserving a case on appeal, prosecutors should generally assume that all recordings must be turned over to the defense unless there is a genuine privacy interest that merits requesting a protective order[40] from the court regarding certain recordings. Any recordings that are not turned over provide an opportunity for the defense to claim that the government is concealing evidence, and prosecutors may or may not correctly identify evidence as exculpatory if it requires contextual information only defense counsel is aware of to identify it as being exculpatory.

Other potential paperwork created during the wiretap process may not be discoverable; some courts have found that minimization instructions, progress reports, and any boilerplate materials used by agents to obtain an ESO are not discovery that a defendant is entitled to.[41] Prosecutors, however, should consider whether there is a genuine reason to hold back these items in discov-

ery; the trend in most criminal jurisdictions has been to expand what is considered discoverable,[42] and items such as minimization instructions and other protocols are fertile ground for defense challenges to the validity of the wire – and the basis for a defense motion to suppress – and exclude critical evidence. With that understanding, these documents should be prepared with the assumption that they might be disclosed by court order, if not with the intention to do so from the outset.

Prosecutors should ensure that before surveillance on a wiretap begins, they are prepared to organize the voluminous discovery obtained by the wiretap for their use at trial and comply with the specific discovery requirements of their jurisdictions. They should also anticipate the associated logistical issues with passing such voluminous discovery; the originals will need to be presented to the court and sealed,[43] though prosecutors can request that they and an investigator maintain working copies to continue investigating. How such recordings are maintained presents further logistical considerations: does the prosecutor have the electronic storage space required for the recordings? Must the prosecutor procure equipment for the defense to pass what could rise into terabytes worth of data? The longer a wiretap has been active and the greater the number of investigative targets, the more pressing those considerations become, and they should be part of any initial considerations of seeking an ESO. Delays in handing over evidence could cause a trial to be further delayed as defense counsel will require more time to analyze the discovery themselves.[44]

Foundation

Admissible evidence must still have some foundation before it can be heard by the trier of fact. That foundation must establish evidence sufficient to "support a finding that the item is what the proponent claims it is."[45] The general standard among the circuits is that to introduce evidence collected on a wiretap, the government must produce "clear and convincing evidence of authenticity and accuracy" of the recordings obtained.[46]

To meet the requirements of Federal Rule of Evidence 901, prosecutors should consider calling a wire room supervisor or other officer involved in overseeing the wire and setting up the surveillance.[47] This officer can lay the foundation for the system and minimization practices and will be able to swear to the accuracy, completeness, and unaltered nature of all copies of transcripts or other intercepted communications that are offered into evidence at trial. They will also be able to authenticate recordings of intercepted communications, subject to their relevance at the time that they are offered into evidence. This person would then also need to establish the accuracy and reliability of the system's time and date stamps, and the source and recipient information[48] recorded for all calls.[49]

Individual case officers who monitored the wire may also be called to identify specific voices based on their personal knowledge or to provide additional evidence regarding how individuals in contact with their targets were identified. For example, an undercover agent conducting physical surveillance of a subject might conduct a surreptitious call to a target and watch as they pick up the phone to establish who was in possession of the phone connected to the number recorded in the wiretap materials. Such a practice avoids having to wait for a target to be identified by voice after an interview (which they may decline after arrest).

Admissibility

The admission of any recordings of a charged offender in a human trafficking conspiracy will be governed by Federal Rule of Evidence 801, or its local equivalent, as non-hearsay statements of a party opponent.[50] As long as investigators are able to identify the offender's voice and provide the foundation that the speaker is the offender, prosecutors should be able to successfully admit any recordings featuring the statements of the charged offender. Any intercepted communications between a trafficker and their victim should be able to be offered under this exception.

However, it may be that there are statements made during calls involving co-conspirators, both charged and uncharged, who are not parties to the action in which the prosecutor is seeking to admit them. This could include the conversations between an unidentified conspirator who transported a victim, and the

victim – or threats made at the behest of the charged trafficker by a third party, or statements from one victim to another regarding their mutual involvement in criminal activity at the direction of their trafficker, none of which would then be statements of a party opponent. Instead, such statements would need to be offered under Federal Rule of Evidence 801(d)(2)(3), regarding statements of a co-conspirator to a party opponent in furtherance of a conspiracy.[51]

Statements of a co-conspirator of a party opponent in furtherance of a conspiracy are treated by the Federal Rules of Evidence essentially the same as those of a party opponent. They are not considered testimonial,[52] and are not hearsay when offered by an opposing party. To offer a statement under this rule, the government must demonstrate by a preponderance of the evidence that a conspiracy involving the declarant and non-offering party existed and that the statement offered was made in furtherance of that conspiracy.[53] This is generally true whether or not the co-conspirator is charged or even identified – and can be true even when the co-conspirator is the victim in the case.[54] Most relevant and probative statements intercepted on a wire between traffickers or between traffickers and their victims will fall into this category. While victims should not be considered co-conspirators for purposes of charging (or threatening to charge), prosecutors should be prepared to articulate for the legal purpose of admissibility that specific victim statements qualify as statements by a co-conspirator.

Proof of an ongoing conspiracy to commit trafficking and related crimes requires some independent evidence other than the content of the statements themselves, such as observations from physical surveillance,[55] arrests for prostitution, online prostitution advertisements, financial records, emails, or recorded jail calls.[56] However, the content of the statements (such as communications discussing the logistics of those engaged in the commercial sex trade) can be a crucial part of the analysis, and the independent evidence supporting a conclusion that a conspiracy exists need not be substantial.[57] In addition, this independent evidence does not itself need to be criminal – for example, a conspirator's presence at an agreed-upon location established in the underlying statement could be considered sufficient independent evidence that a conspiracy existed and that the conspirator was acting in furtherance of it when they made the statement about going to that location.[58]

Many intercepted communications will easily fit this requirement that the statements be made in furtherance of the sex trafficking conspiracy. For example, conversations about money, clients, locations of "dates", and threats of violence should be admissible, as they directly relate to the criminal acts charged and involve the logistics and planning of those crimes.[59]

CONCLUSION

The utilization of eavesdropping warrants is a technical, labor, and time-intensive process and requires dedicated resources to execute properly. Despite this, they are favorable investigative techniques because these warrants yield incredibly persuasive evidence. They enable law enforcement to bring traffickers to justice and prevent further victimization of others without the assistance of uncooperative victims. In addition, communication between traffickers about their operations obtained through electronic surveillance can help identify other perpetrators and victims that otherwise may have remained unknown. Perhaps most importantly, this evidence is corroboration of a victim's exploitation, and it may help persuade a reluctant or scared victim to testify knowing that the jury will not be relying solely on their testimony. In the best-case scenario, a wiretap may provide an investigative team with time to continue to investigate an initial allegation while building a relationship with potential victim-witnesses to bolster their confidence in the investigators and feel comfortable testifying at trial, knowing that this additional evidence will support their testimony. Evidence obtained through wiretaps can mitigate misconceptions surrounding victim behavior and help ensure justice for victims by providing objective direct or circumstantial evidence of the events victims are testifying about. In this manner, prosecutors and law enforcement who appropriately utilize wiretaps may seek justice in cases where an offender's wrongdoing might otherwise never be brought into the light of day.

ENDNOTES

1 Jennifer Dolle is a former Attorney Advisor with AEquitas. Jennifer Newman is a Senior Associate Attorney Advisor with AEquitas. This article was adapted from the draft article Jennifer Dolle, *UTILIZING EAVESDROPPING WARRANTS TO SUCCESSFULLY INVESTIGATE AND PROSECUTE SEX TRAFFICKERS: A Practical Guide to a Valuable Tool that Holds Perpetrators Accountable Without Requiring the Testimony of a Cooperative Victim*, (2021) (on file with AEquitas). Other AEquitas staff who contributed to this article include Jane Anderson, Senior Attorney Advisor; Lou Longhitano, Attorney Advisor; and Holly Spainhower, former Senior Associate Attorney Advisor.

2 Due to end-to-end encryption and the purposeful inability of companies to be able to obtain evidence from locked devices, more traditional techniques, such as search warrants on seized devices or communications stored by telecommunications or social media companies, are becoming less fruitful. While evidence obtained by eavesdropping warrants is also affected by these changes, voice calls and other types of messages, such as those from an iPhone to an Android, can still be intercepted.

3 While this article focuses primarily on the utility of wiretaps in a sex trafficking case, these considerations may also be crucial in labor trafficking investigations when deciding whether and how to utilize a wiretap to obtain evidence.

4 Depending on the nature of the evidence of coercion, a prosecutor may consider whether a victim behavior expert in human trafficking would be an appropriate witness to help contextualize the actions of the offender and responses of the victim. For more information, *see*: webinar by IACP, Jane Anderson, and Miiko Anderson, *Prosecution Foundations: Educating the Judge and Jury About the Realities of Human Trafficking*, AEquitas, (uploaded November 1, 2023) https://www.youtube.com/watch?v=gWt78Z_qjEg

5 AEquitas, Wendy Barnes, Keisha Head, and Toolsi Meisner, *Being Trafficked: What Prosecutors Need to Know About the Life,* 22 Strategies in Brief, (June 2023) available at https://aequitasresource.org/wp-content/uploads/2023/07/Being-Trafficked-—-What-Prosecutors-Need-to-Know-About-the-Life.pdf

6 Webinar by Jennifer Dolle and Sgt. Nick Odenath, *Tapping into Offender Accountability: Using Wiretapping in State-Level Human Trafficking Cases,* AEquitas (April 11, 2023) https://www.youtube.com/watch?v=qy0F_mM5CQg.

7 *See, e.g.*, *United States v. Purcell*, 967 F.3d 159 (2d Cir. 2020) (holding that the communications between the defendant and his victims, including the imposition of rules like forcing victims to call him "daddy," and apprise him of their location regularly were also in furtherance of his sex trafficking conspiracy).

8 Dolle and Odenath, *supra* note 6.

9 18 U.S.C. § 2518 lays out the requirements in detail for obtaining an eavesdropping warrant.

10 18 U.S.C. § 2518 (3). Prosecutors should consult statutes in their jurisdiction, but it is important to note that state laws cannot be less protective of privacy than federal laws. *See, United States v. Mckinnon*, 721 F.2d 19 (1st Cir. 1983).

11 18 U.S.C. § 2516(c)

12 Dolle and Odenath, *supra* note *6.*

13 18 U.S.C. § 2518(3).

14 *United States v. Garcia*, 232 F.3d 1309 (10th Cir. 2000).

15 *United States v. VanMeter*, 278 F.3d 1156, 1164 (10th Cir. 2002).

16 *Id*.

17 *United States v. Motley*, 89 F.4th 777 (9th Cir. 2023).

18 *United States v. Milliner*, 765 F.3d 836 (8th Cir. 2014).

19 *United States v. Jackson,* 345 F.3d 638, 644 (8th Cir.2003).

20 A jurisdiction with fewer man hours and less equipment to conduct a wire may consider whether there are partners in other state or federal jurisdictions who could work together with them on an especially critical case to ensure that they can successfully conduct a wire if needed.

21 Dolle and Odenath, *supra* note *6.*

22 This is not an exhaustive list of issues that may arise while on a wire. This is intended to call attention to some of the more common legal requirements and should be consulted only in addition to established procedures within a prosecutor's office or jurisdiction.

23 *United States v. Apodaca*, 820 F.2d 348, 350 (10th Cir. 1987) (Citing *Scott v. U.S.*, 436 U.S. 128 (1978) to hold that the proper approach for evaluating compliance with the minimization requirement, like evaluation of all alleged violations of the Fourth Amendment, is objectively to assess the agent's or officer's actions in light of the facts and circumstances confronting him at the time without regard to his underlying intent or motive).

24 *See, e.g., State v. Kraft*, 301 So.3d 981, (Fla. Dist. Ct. App Ct. App. 2020) (in a case where the court found that officers on a wire failed to minimize their intrusion into calls with innocent parties, the court held that exclusion of all evidence obtained on the wire – not just the recordings pertaining to the innocent parties – was the appropriate remedy).

25 *United States v. Couser*, 732 F.2d 1207 (4th Cir. 1984) (holding that discovery of nontargeted offenses not named in the warrant for the wiretap is to be analyzed under the "plain view" doctrine).

26 18 U.S.C. § 2517(5).

27 18 U.S.C. § 2518(5).

28 18 U.S.C. § 2518(6); and *see, e.g.*, N.Y. Crim. Pro. § 700.50.

29 18 U.S.C. § 2518(8).

30 *Id.*

31 Notice requirements vary by jurisdiction. Federal law (18 U.S.C. § 2518) dictates that notice must be given within 90 days. In contrast, New York State requires notice within 10 days of arraignment (N.Y. Crim. Pro. § 700.70).

32 18 U.S.C. § 2518(8)(d).

33 *Wiretap Report 2022*, United States Courts, https://www.uscourts.gov/statistics-reports/wiretap-report-2022#:~:-text=The%20expenditures%20noted%20reflect%20the,the%20average%20cost%20in%202021 (finding that in 2022, the average monetary cost of running a wiretap was 106,123$. A single 30-day investigation in a West Texas case involving a federal wiretap in an illegal drugs investigation totaled $3,015,576.).

34 Webinar by AEquitas and Esperanza United, *Beyond Language Access: Confronting Bias & Implementing Strategies to Ensure Justice in the Prosecution of Sexual Violence, Domestic Violence, Stalking, and Human Trafficking Involving Survivors from Latine Communities,* AEquitas, (September 28, 2023), https://www.youtube.com/watch?si=VeErq78_YhzdDfIb&v=DnYqCwcg5gQ&feature=youtu.be.

35 Webinar by Jane Anderson and Kim Nash, *A SANE Approach to Human Trafficking Cases*, AEquitas, (October 27, 2022), https://www.youtube.com/watch?v=PUnydnh-rEk

36 For more information on partnerships with community victim service providers as an essential component of responding to cases involving sexual violence, see: Webinar by Jane Anderson, *Collaboration is Key: Working with Victim Service Professionals,* AEquitas (November 14, 2022) https://www.youtube.com/watch?v=ywe1mPcJd_w&themeRefresh=1

37 18 U.S.C. § 2518(8)(d).

38 *See United States v. Orozco*, 630 F. Supp. 1418 (S.D. Cal. 1986) (holding that while section 2518(8)(d) requires that an evidentiary inventory must be sent to the defense within 90 days of the conclusion of surveillance under a wiretap, prosecutors could seek an extension on a showing of good cause to postpone providing such notice to the defense, and that such an extension did not create grounds to exclude evidence obtained on a wiretap).

39 *Id*.

40 *See, e.g*., *In re Applications of Kansas City Star*, 666 F.2d 1168, 1175-76 (8th Cir. 1981) (observing that the district court order which barred defendant and his attorneys from disclosing wiretap materials was "highly appropriate considering the 'privacy of other people' " and noting that the good cause requirement of the statute called for consideration by the courts of the privacy interests of third parties which might be affected by the disclosure).

41 *See, e.g*., *United States v. Chimera*, 201 F.R.D. 72 (W.D.N.Y. 2001) (holding that the defendants were not entitled to discovery of minimization instructions provided to agents assigned to operate and monitor wiretaps and eavesdrop devices or discovery of "boilerplate" materials and draft applications used by the government in its applications to the court for wiretap and eavesdropping orders).

42 Darryl K. Brown, *Discovery*, in 3 Reforming Criminal Justice: Pretrial and Trial Processes, 147 (Erik Luna ed., 2017), https://law.asu.edu/sites/default/files/pdf/academy_for_justice/7_Reforming-Criminal-Justice_Vol_3_Discovery.pdf.

43 § 2518(8)(a) and *McMillan v. United States*, 558 F.2d 877, 878 (8th Cir. 1977).

44 *United States v. Keith,* 61 F.4th 839 (10th Cir.), cert. denied, 144 S. Ct. 420, 217 L. Ed. 2d 234 (2023) (holding that the voluminous nature of the discovery in the associated wiretap case could have created a speedy trial basis for appeal for the defendant, had he successfully objected to the delays caused by discovery issues during the trial process).

45 Fed. Rule Evid. 901

46 *United States v. Knohl*, 379 F.2d 427, 440 (2d Cir.), *cert. denied*, 389 U.S. 973 (1967); *see also United States v. Ruggiero*, 928 F.2d 1289, 1303 (2d Cir.), cert. denied sub nom., *Gotti v. United States*, 502 U.S. 938 (1991).

47 *See e.g*., *United States v. Cortellesso,* 663 F.2d 361 (1st Cir.1981) (where supervising agent testified to the procedure followed by the F.B.I. with respect to the intercepted communications, his presence at the initial test of the equipment, his personal preparation of the transcripts from the tapes, and his custody of the original logs and tape recordings, he provided sufficient foundation for the accuracy of the collected recordings, and it was not necessary to call the individual agents who conducted the actual monitoring to testify).

48 This could include phone numbers, but in the expanding digital age would also refer to usernames in any applications used to make VOIP calls or other application-based communication, internet protocol addresses, or other identifying information associated with the intercepted communication.

49 If this information is not established by a wire room supervisor, the prosecutor will need to place the actual monitor of that call on the stand to establish that after the fact.

50 Fed. R. Evid. 801(d)(1)

51 Fed. R. Evid. 801(d)(2)(e)

52 *Giles v. California*, 554 U.S. 353, 374 n.6 (2008) (suggesting that "an incriminating statement in furtherance of the conspiracy would probably never be testimonial").

53 *Bourjaily v. United States*, 483 U.S. 171, (1987)

54 *People v. Brown*, 14 Cal. App. 5th 320, 221 Cal. Rptr. 3d 854 (Ct. App. 2017) (holding that the statute prohibiting the prosecution of victims did not preclude such victims from being considered uncharged co-conspirators under the co-conspirator exception to the hearsay rule).

55 This is just one instance where physical surveillance in connection with real-time interception of electronic communications in the wire room can be incredibly important to authenticating and admitting evidence at trial.

56 *See United States v. Sudeen,* 434 F.3d 384, 390 (5th Cir.2005) (holding that the content of a statement may be considered as part of the analysis used to establish the existence of the conspiracy and the defendant's involvement therein, but there must also be independent evidence establishing the factual predicates for Rule 801(d)(2)(E)); and see *Bourjaily* 483 U.S. at 180 (holding that "[w]e think that there is little doubt that a co-conspirator's statements could them-

selves be probative of the existence of a conspiracy and the participation of both the defendant and the declarant in the conspiracy" in light of the subsequent actions of the declarant, which was arriving in the agreed upon location and receiving the drugs that had been the subject of the statements being offered.)

57 *United States v. Stein*, 985 F.3d 1254, 1269 (10th Cir. 2021).

58 *See, e.g., United States v. Roth*, 736 F.2d 1222 (8th Cir. 1984).

59 *See, e.g., United States v. Foard* 108 F.4th 729 (8th Cir. 2024) (holding that where a defendant's text messages to minors identified as sex trafficking victims indicated he had transported them to and from locations at which they were exploited, they were in furtherance of the sex trafficking conspiracy he was charged with participating in).

60 18 U.S.C. § 2518(3).

61 *United States v. Garcia*, 232 F.3d 1309 (10th Cir. 2000).

62 *United States v. VanMeter*, 278 F.3d 1156, 1164 (10th Cir. 2002).

63 *Id*.

64 *United States v. Motley*, 89 F.4th 777 (9th Cir. 2023).

65 *United States v. Milliner*, 765 F.3d 836 (8th Cir. 2014).

66 *United States v. Jackson,* 345 F.3d 638, 644 (8th Cir.2003).

67 A jurisdiction with fewer man hours and less equipment to conduct a wire may consider whether there are partners in other state or federal jurisdictions who could work together with them on an especially critical case to ensure that they can successfully conduct a wire if needed.

68 Dolle and Odenath, *supra* note *6.*

69 This is not an exhaustive list of issues that may arise while on a wire. This is intended to call attention to some of the more common legal requirements and should be consulted only in addition to established procedures within a prosecutor's office or jurisdiction.

70 *United States v. Apodaca*, 820 F.2d 348, 350 (10th Cir. 1987) (Citing *Scott v. U.S.*, 436 U.S. 128 (1978) to hold that the proper approach for evaluating compliance with the minimization requirement, like evaluation of all alleged violations of the Fourth Amendment, is objectively to assess the agent's or officer's actions in light of the facts and circumstances confronting him at the time without regard to his underlying intent or motive).

71 *See, e.g., State v. Kraft*, 301 So.3d 981, (Fla. Dist. Ct. App Ct. App. 2020) (in a case where the court found that officers on a wire failed to minimize their intrusion into calls with innocent parties, the court held that exclusion of all evidence obtained on the wire – not just the recordings pertaining to the innocent parties – was the appropriate remedy).

72 *United States v. Couser*, 732 F.2d 1207 (4th Cir. 1984) (holding that discovery of nontargeted offenses not named in the warrant for the wiretap is to be analyzed under the "plain view" doctrine).

73 18 U.S.C. § 2517(5).

74 18 U.S.C. § 2518(5).

75 18 U.S.C. § 2518(6); and *see, e.g.*, N.Y. Crim. Pro. § 700.50.

76 18 U.S.C. § 2518(8).

77 *Id.*

78 Notice requirements vary by jurisdiction. Federal law (18 U.S.C. § 2518) dictates that notice must be given within 90 days. In contrast, New York State requires notice within 10 days of arraignment (N.Y. Crim. Pro. § 700.70).

79 18 U.S.C. § 2518(8)(d).

80 *Wiretap Report 2022*, United States Courts, https://www.uscourts.gov/statistics-reports/wiretap-report-2022#:~:text=The%20expenditures%20noted%20reflect%20the,the%20average%20cost%20in%202021 (finding that in 2022, the average monetary cost of running a wiretap was 106,123$. A single 30-day investigation in a West Texas case involving a federal wiretap in an illegal drugs investigation totaled $3,015,576.).

81 Webinar by AEquitas and Esperanza United, *Beyond Language Access: Confronting Bias & Implementing Strategies to Ensure Justice in the Prosecution of Sexual Violence, Domestic Violence, Stalking, and Human Trafficking Involving Survivors from Latine Communities,* AEquitas, (September 28, 2023), https://www.youtube.com/watch?si=VeErq78_YhzdDfIb&v=DnYqCwcg5gQ&feature=youtu.be.

82 Webinar by Jane Anderson and Kim Nash, *A SANE Approach to Human Trafficking Cases*, AEquitas, (October 27, 2022), https://www.youtube.com/watch?v=PUnydnh-rEk

83 For more information on partnerships with community victim service providers as an essential component of responding to cases involving sexual violence, see: Webinar by Jane Anderson, *Collaboration is Key: Working with Victim Service Professionals,* AEquitas (November 14, 2022) https://www.youtube.com/watch?v=ywe1mPcJd_w&themeRefresh=1

84 18 U.S.C. § 2518(8)(d).

85 *See United States v. Orozco*, 630 F. Supp. 1418 (S.D. Cal. 1986) (holding that while section 2518(8)(d) requires that an evidentiary inventory must be sent to the defense within 90 days of the conclusion of surveillance under a wiretap, prosecutors could seek an extension on a showing of good cause to postpone providing such notice to the defense, and that such an extension did not create grounds to exclude evidence obtained on a wiretap).

86 *Id*.

87 *See, e.g., In re Applications of Kansas City Star*, 666 F.2d 1168, 1175-76 (8th Cir. 1981) (observing that the district court order which barred defendant and his attorneys from disclosing wiretap materials was "highly appropriate considering the 'privacy of other people' " and noting that the good cause requirement of the statute called for consideration by the courts of the privacy interests of third parties which might be affected by the disclosure).

88 *See, e.g., United States v. Chimera*, 201 F.R.D. 72 (W.D.N.Y. 2001) (holding that the defendants were not entitled to discovery of minimization instructions provided to agents assigned to operate and monitor wiretaps and eavesdrop devices or discovery of "boilerplate" materials and draft applications

used by the government in its applications to the court for wiretap and eavesdropping orders).

89 Darryl K. Brown, *Discovery*, in 3 Reforming Criminal Justice: Pretrial and Trial Processes, 147 (Erik Luna ed., 2017), https://law.asu.edu/sites/default/files/pdf/academy_for_justice/7_Reforming-Criminal-Justice_Vol_3_Discovery.pdf.

90 § 2518(8)(a) and *McMillan v. United States*, 558 F.2d 877, 878 (8th Cir. 1977).

91 *United States v. Keith,* 61 F.4th 839 (10th Cir.), cert. denied, 144 S. Ct. 420, 217 L. Ed. 2d 234 (2023) (holding that the voluminous nature of the discovery in the associated wiretap case could have created a speedy trial basis for appeal for the defendant, had he successfully objected to the delays caused by discovery issues during the trial process).

92 Fed. Rule Evid. 901

93 *United States v. Knohl*, 379 F.2d 427, 440 (2d Cir.), *cert. denied*, 389 U.S. 973 (1967); *see also United States v. Ruggiero*, 928 F.2d 1289, 1303 (2d Cir.), cert. denied sub nom., *Gotti v. United States*, 502 U.S. 938 (1991).

94 *See e.g.*, *United States v. Cortellesso,* 663 F.2d 361 (1st Cir.1981) (where supervising agent testified to the procedure followed by the F.B.I. with respect to the intercepted communications, his presence at the initial test of the equipment, his personal preparation of the transcripts from the tapes, and his custody of the original logs and tape recordings, he provided sufficient foundation for the accuracy of the collected recordings, and it was not necessary to call the individual agents who conducted the actual monitoring to testify).

95 This could include phone numbers, but in the expanding digital age would also refer to usernames in any applications used to make VOIP calls or other application-based communication, internet protocol addresses, or other identifying information associated with the intercepted communication.

96 If this information is not established by a wire room supervisor, the prosecutor will need to place the actual monitor of that call on the stand to establish that after the fact.

97 Fed. R. Evid. 801(d)(1)

98 Fed. R. Evid. 801(d)(2)(e)

99 *Giles v. California*, 554 U.S. 353, 374 n.6 (2008) (suggesting that "an incriminating statement in furtherance of the conspiracy would probably never be testimonial").

100 *Bourjaily v. United States*, 483 U.S. 171, (1987)

101 *People v. Brown*, 14 Cal. App. 5th 320, 221 Cal. Rptr. 3d 854 (Ct. App. 2017) (holding that the statute prohibiting the prosecution of victims did not preclude such victims from being considered uncharged co-conspirators under the co-conspirator exception to the hearsay rule).

102 This is just one instance where physical surveillance in connection with real-time interception of electronic communications in the wire room can be incredibly important to authenticating and admitting evidence at trial.

103 *See United States v. Sudeen,* 434 F.3d 384, 390 (5th Cir.2005) (holding that the content of a statement may be considered as part of the analysis used to establish the existence of the conspiracy and the defendant's involvement therein, but there must also be independent evidence establishing the factual predicates for Rule 801(d)(2)(E)); and see *Bourjaily* 483 U.S. at 180 (holding that "[w]e think that there is little doubt that a co-conspirator's statements could themselves be probative of the existence of a conspiracy and the participation of both the defendant and the declarant in the conspiracy" in light of the subsequent actions of the declarant, which was arriving in the agreed upon location and receiving the drugs that had been the subject of the statements being offered.)

104 *United States v. Stein*, 985 F.3d 1254, 1269 (10th Cir. 2021).

105 *See, e.g.*, *United States v. Roth*, 736 F.2d 1222 (8th Cir. 1984).

106 *See, e.g.*, *United States v. Foard*, 108 F.4th 729 (8th Cir. 2024) (holding that where a defendant's text messages to minors identified as sex trafficking victims indicated he had transported them to and from locations at which they were exploited, they were in furtherance of the sex trafficking conspiracy he was charged with participating in).