The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. KALEB COLE, Defendant.	No. CR20-032 JCC MOTION TO SUPPRESS EVIDENCE *Evidentiary Hearing Requested* *Oral Argument Requested* Note on Motion Calendar: August 27, 2021

I. RELIEF REQUESTED

Defendant, Kaleb Cole, by his undersigned attorney, moves this Court to suppress at trial, pursuant to the Fourth Amendment to the United States Constitution and Franks v. Delaware, 438 U.S. 154 (1978), all items of evidence seized by law enforcement pursuant to a search of Mr. Cole's alleged residence located at 1218 Oxon Run, Montgomery, Texas. The Court should suppress this evidence because the affidavit for the warrant authorizing the search 1) at least recklessly omitted information material to the determination of probable cause, which rendered the affidavit insufficient to support probable cause to search the home and 2) even as written failed to establish probable cause to search the home.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

II. FACTS

For a number of years prior to the institution of charges in the case the Federal Bureau of Investigation ("FBI") investigated an organization called Atomwaffen, of which Mr. Cole is an alleged member. They employed a confidential informant ("CI") as part of the investigation and paid him handsomely. The government has informed defense counsel that the CI in this case has worked as an informant for the FBI for approximately the past sixteen years. Since 2003, he has been paid over $140,000 for this work. More importantly, the CI has been paid $78,133.20 plus an expense advance of $4,378.60, since February 7, 2018, which almost entirely coincides with his work on the investigation into Mr. Cole and Atomwaffen.

The CI is a convicted felon and currently owns and operates a publishing company that distributes white supremacist writings. The CI began his long career as a professional informant in exchange for consideration regarding his sentence on a federal conviction for possession of a firearm with an obliterated serial number and an unregistered silencer. He has continued this work for pay.

This informant was the source of almost all of the information implicating Mr. Cole in the alleged criminal activities underlying this case. On February 24, 2020, FBI Special Agent Casey Villareal submitted an application for a warrant to search Mr. Cole's alleged residence in Montgomery, Texas. See Exhibit 1 (application, affidavit and warrant). The affidavit in support of the application described a plot to create and send threatening posters to Jewish people and people belonging to racial minority groups. The bulk of the application, as it pertained to Mr. Cole's alleged involvement in criminal activity, described communications over an app called Wire between a group of alleged co-conspirators. See Exhibit 1 at 17 – 28. The affiant asserted that Mr. Cole was a member of this group and that he used a moniker consisting of a string of

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

symbols to communicate within the app. Id. at 18. The affidavit does not explicitly state that this information came from the CI but defense counsel, on information and belief, believes that there is no other potential source. The affidavit does not contain information specifically implicating Mr. Cole in the alleged plot other than the information provided by the CI.

The affidavit refers to the existence of the CI by noting in a couple of places that information came from "confidential human source (CHS) reporting." See Exhibit 1 at 15, 17. The affidavit does not provide any details about how the CI came to possess the information included in the affidavit. It likewise does not include any information about the scope of the CI's current or prior work as an FBI informant or track record in this capacity. The affidavit is essentially silent regarding the CI other than noting generally that he provided some information regarding the investigation. It certainly does not acknowledge, or even allude to, the fact that the CI is a paid informant and convicted felon.

The magistrate who reviewed the warrant application was unaware of the source of the incriminating information contained within the document, the relevant missing facts that were not included in the document, or the magnitude of the affiant's failure to establish the CI's credibility, and therefore issued the warrant as requested. The search of the home conducted pursuant to the warrant uncovered potentially incriminating evidence.

III. SUMMARY OF ARGUMENT

The Court should suppress on two separate bases all evidence seized from the residence during the execution of the search warrant.

First, the search of the residence was unlawful because the affidavit submitted in support of the warrant depended entirely on a conclusion of the affiant that was not supported by underlying facts, and as such failed to establish probable cause for the warrant to issue. In

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

particular, the warrant affidavit described a multitude of actions taken, and statements made, by someone in Wire chats employing a user-name consisting of a string of symbols. The affidavit simply identified Mr. Cole as the user of this moniker without providing any basis for the affiant's conclusion that the user was Mr. Cole, which is far from self-evident as described below. And, other than statements associated with the person using the symbol string moniker, the affidavit contained almost no information associating Mr. Cole with criminal activity. Because the affidavit did not contain sufficient information to establish probable cause to search Mr. Cole's alleged residence absent the unsupported conclusion, the search based on the warrant supported by the faulty affidavit was illegal, and the fruits thereof should be suppressed.

Second, even if the Court finds that the warrant affidavit as written provided probable cause for the search, the Court should nonetheless suppress the fruits of the search because the warrant affiant recklessly omitted information necessary to the probable cause determination, in violation of Franks v. Delaware. Specifically, the affiant completely failed to include any information supporting the credibility of the confidential informant ("CI") in this case or put the issuing magistrate on notice of the existence of issues that reflect negatively on the CI. This type of failure constitutes a material omission in in the warrant affidavit. And, in this case, because essentially all of the information supporting probable cause for the warrant to issue came from the CI, when that information is removed from consideration as part of this Court's evaluation of the validity of the warrant, as it must be under Franks, insufficient information remains to support a finding of probable cause. The Court should suppress the fruits of the warrant on this basis as well.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

IV. ARGUMENT

A. The search warrant application failed to establish probable cause that evidence of a crime would be found in the residence.

The Court should suppress the fruits of the search of the residence because the affidavit submitted in support of the warrant depended entirely on a conclusion of the affiant that was not supported by underlying facts and therefore failed to establish probable cause.

The Fourth Amendment generally requires that police officers obtain a warrant based on probable cause to justify a seizure and search. Terry v. Ohio, 392 U.S. 1, 20 (1968). In order to establish probable cause, an affidavit must establish that there is a fair probability that contraband or evidence of a crime will be found in a particular place. Illinois v. Gates, 462 U.S. 213, 238 (1983). Probable cause determinations are to be made by viewing the "totality of the circumstances" set forth in the affidavit. Id. In reviewing the validity of a search warrant, a court is limited to the information and circumstances contained within the four corners of the underlying affidavit. United States v. Stanert, 762 F.2d 775, 778, amended by, 769 F.2d 1410 (9th Cir. 1985).

"Conclusions of the affiant unsupported by underlying facts cannot be used to establish probable cause." United States v. Underwood, 725 F.3d 1076, 1081 (9th Cir. 2013)(citing United States v. Cervantes, 703 F.3d 1135, 1139-40 (9th Cir. 2012) (affording little if any weight to detective's conclusory statement that, based on his training and experience, the box in defendant's possession came from a suspected narcotics stash house)).

In the instant case, while the warrant affidavit provides details about the activities of someone who was alleged to be Mr. Cole, it does not provide any detailed information allowing the magistrate to make an independent determination that the person who made the communications in question was in fact Mr. Cole. The affidavit simply stated, without support, that the user of the symbol string moniker was Mr. Cole. See Exhibit 1 at 18. And this is

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

something that may not have stood out to the magistrate who issued the warrant, as the magistrate may well have thought that such a conclusion was clear and was based on evidence in the government's possession, such that it did not rise to the level of importance that a detailed description of the underlying data was necessary. But this was not the case.

It is not entirely clear even to this day what the government's basis is for attributing this moniker to Mr. Cole. The government has not obtained any subscriber information regarding the moniker, or information connected to IP addresses using the moniker, or digital devices connected to both the moniker and Mr. Cole. It appears that the source of the government's belief may be the CI. See Exhibit 1 at 17. If this is the case, the affidavit nonetheless fails to provide any detail about the source of the information other than "CHS reporting." Id. This is not the kind of detailed information that allows a magistrate to make an independent determination about whether the facts in the affidavit are sufficient to provide probable cause for a search. See Underwood, 725 F.3d at 1081.

The affidavit contains nothing particular about why or how the CI identified Mr. Cole as the user of the symbol string moniker. And that was a fact crucial that was crucial to the probable cause determination in this case. Without that fact, although the affidavit establishes probable cause that **someone** committed a crime, it fails to establish probable cause that **Kaleb Cole** did so. The search warrant which was issued in reliance on this premise therefore did not comport with the requirements of the Fourth Amendment.

Where evidence is obtained in violation of the Fourth Amendment, the remedy is suppression of the fruits of the unlawful search. See Wong Sun v. United States, 371 U.S. 471, 484 – 85 (1963). Consequently, because the warrant affidavit issued in this case was unsupported by probable cause the fruits of the unlawful search of the residence should be suppressed.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

B. The Court should suppress the fruits of the search under *Franks v. Delaware*.

The Court should suppress the fruits the search on an alternative basis as well- that the affidavit for the warrant at least recklessly omitted information material to the determination of probable cause, in violation of Franks v. Delaware, 438 U.S. 154 (1978).

In Franks, the Supreme Court held that a defendant has a constitutional right, after the *ex parte* issuance of a warrant, to challenge the truthfulness of statements made in the search warrant affidavit. Material omissions as well as false statements are subject to challenge. United States v. Stanert, 762 F.2d 775, 781, amended by 769 F.2d 1410 (9th Cir. 1985). When a defendant makes a preliminary showing that (1) the affidavit contains intentionally or recklessly false statements or omissions and (2) the affidavit cannot support a finding of probable cause without the allegedly false information, then s/he is entitled to a hearing to determine the validity of the warrant. Franks, 438 U.S. at 171-72. The defendant need not present clear proof that misrepresentations were deliberate or reckless in order to obtain a Franks hearing; all that is needed is a substantial showing. United States v. Gonzalez, Inc., 412 F.3d 1102, 1111 (9th Cir. 2005).[1] The fact that probable cause existed and could have been established in a truthful affidavit will not cure a Franks error. Baldwin v. Placer County, 418 F.3d 966, 971 (9th Cir. 2005) (citing United States v. Davis, 714 F.2d 896, 899 (9th Cir. 1983) (under Franks, "the fact that probable cause did exist and could have been established by a truthful affidavit does not cure the error.")).

[1] At the hearing, the defendant must show, by a preponderance of the evidence, that the statements or omissions were made either deliberately or with reckless disregard for the truth. United States v. Davis, 663 F.2d 824, 831 (9th Cir. 1981).

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

1. The warrant affidavit contains material omissions that can only be characterized as deliberate or reckless.

In order to establish meet the requirements of the first prong of the Franks test, the defense must show that 1) the affiant for the warrant made either a material false statement or a material omission in the warrant affidavit, and 2) the statement or omission was made intentionally or recklessly. The defense can make both showings by establishing that that FBI SA Villareal omitted from the affidavit the fact that the CI was receiving significant consideration from the FBI in exchange for his cooperation against Mr. Cole.

The Ninth Circuit has made clear that law enforcement officers must always disclose in a warrant affidavit whether an informant has an ulterior motive for providing information for a search warrant affidavit. See United States v. Martinez-Garcia, 397 F.3d 1205, 1216 (9th Cir. 2005); United States v. Meling, 47 F.3d 1546, 1553 (9th Cir. 1995). In Martinez-Garcia, the search warrant affidavit failed to disclose that the informant had a pending federal charge and that a deal was made with him to make a favorable recommendation to prosecutors in exchange for his cooperation. Martinez-Garcia, 397 F.3d at 1216. The Ninth Circuit held that "knowingly omit[ting] from the affidavit information related to incentives he provided to [the CI]" satisfied the first prong of the Franks test, i.e. that the defendant made a substantial showing that that law enforcement knowingly omitted material information from the search warrant affidavit. Id.

It is beyond dispute that the affiant failed to include material information in the warrant affidavit. The government has informed defense counsel that the CI in this case has worked for the FBI for approximately the past sixteen years. He began this work in exchange for consideration regarding his sentence on a federal conviction for possession of a firearm with an obliterated serial number and an unregistered silencer. He has continued this work for pay. Since 2003, the CI has been paid over $140,000 for his work with the FBI. More importantly, the CI

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

has been paid $78,133.20 plus an expense advance of $4,378.60 in conjunction with his participation in the investigation in this case. None of this was disclosed in the warrant application, which does no more than generally refer to "confidential human source (CHS) reporting." See Exhibit 1 at 15, 17. This omission was material. See Martinez-Garcia, 397 F.3d at 1216; Meling, 47 F.3d at 1553.

The failure to disclose the benefits offered to the CI cannot be characterized as anything other than intentional or reckless. The affiant provided his bona fides as part of the application, which provides in relevant part:

> I am a Special Agent SA with the Federal Bureau of Investigation (FBI) and have been so employed since April 2008. I am currently assigned to investigate domestic terrorism in the Houston Field Office. My experience as an FBI Agent includes the investigation of terrorism cases where individuals frequently utilize computers and the Internet to coordinate and facilitate various crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures.

Exhibit 1 at 9-10. It is simply not reasonable to believe that a trained FBI agent with over ten years of experience would fail to recognize the importance of information that bears on a CI's incentives to cooperate when submitting an affidavit for a search warrant based almost exclusively on information provided by the CI.

It is common knowledge that criminal informants are, rightly, viewed with suspicion. Criminal informants are, by definition, "cut from untrustworthy cloth and must be managed and carefully watched by the government and the courts to prevent them from falsely accusing the innocent, from manufacturing evidence against those under suspicion of crime, and from lying under oath in the courtroom." United States v. Bernal-Obeso, 989 F.2d 331, 333 (9th Cir. 1993) (evidence that informant attempted to conceal his felony criminal record is exculpatory and thus

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

discoverable under Brady). The use of such informants by the government thus "may raise serious questions of credibility." Id. (quoting On Lee v. United States, 343 U.S. 747, 757 (1952)). Because informants "will stop at nothing to maneuver themselves into a position where they have something to sell, [i]t is no accident that some federal jury instructions regarding an immunized witness warn jurors that such a witness 'has a motive to falsify.'" United States v. Hernandez-Escarsega, 886 F.2d 1560, 1574-1575 (9th Cir.1989). Again, SA Villareal is without doubt well aware of these principles.

The failure to include the information about the CI's incentives is made more egregious by the fact that the warrant application incriminated Mr. Cole based almost solely on the alleged observations of the CI. And it it is further compounded by the fact that the affidavit is misleading in regard to the fact that the source of all of the incriminating information regarding Mr. Cole is in fact the CI. While the affidavit did not explicitly state that all of the information regarding Mr. Cole's statements in the Wire communications (see Exhibit 1 at 17 – 28) came from the CI, it is counsel's understanding that the CI is in fact the source. This is not immediately apparent from the affidavit, which likely served to obscure this red flag from the magistrate who issued the warrant.

The materiality and nature of the omissions from the search warrant affidavit about the CI's motives for providing the information included in the affidavit cannot be classified as mere oversights. See Frimmel Management, LLC v. United States, 897 F.3d 1045, 1052 (9th Cir. 2018) (finding that omissions regarding credibility of informants must have been intentional or reckless given their significance). The defense has shown a reckless material omission in this case.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

2. The warrant affidavit does not survive the redaction of the information from the CI.

Upon the defense making a showing as to the first part of the test (here: showing a reckless omission), the Court then turns to whether the affidavit establishes still establishes probable cause as it should have read. In this case, because the affidavit relied almost solely on the allegations of a confidential informant to provide probable cause that Mr. Cole committed a crime, and because the affidavit provided no information whatsoever establishing the credibility of the informant or information corroborating the informant's claims that Mr. Cole was the person using the symbol string moniker, the affidavit does not overcome the material omissions about the informant's credibility.

In assessing whether information from an informant is sufficient to support a finding of probable cause, courts must evaluate the totality of the circumstances with consideration of the informant's veracity, reliability and basis of knowledge. Illinois v. Gates, 462 U.S. 213, 238 (1983). "'To credit a confidential source's information in making a probable cause determination, the affidavit should support an inference that the source was trustworthy and that the source's accusation of criminal activity was made on the basis of information obtained in a reliable way.'" Frimmel Management, 897 F.3d at 1052 (quoting United States v. Landis, 726 F.2d 540, 543 (9th Cir. 1984)). Courts look to several factors to determine the reliability of information from an informant, including whether the informant has a history of providing reliable information in previous investigations and any prior criminal convictions for crimes of dishonesty. Martinez-Garcia, 397 F.3d at 1216. Courts must also examine whether the informant's information was bolstered by independent police investigation of the tip or corroboration by other confidential informants. Id.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

A comparison of this case to Martinez-Garcia demonstrates why the facts of this case warrant suppression. While the Ninth Circuit did not ultimately find suppression the appropriate remedy in Martinez-Garcia, the factors the court cited as supporting probable cause for the search, despite the reckless omission of information about consideration provided to the CI, illustrate why suppression is called for in this case, as essentially none of those factors are present here. These factors include: the CI had a track record of providing reliable information and had been polygraphed successfully; police surveilled the CI attending a meeting for a planned drug deal; the CI successfully completed a controlled buy of meth from the target of the warrant at another location; other confidential informants confirmed information in the affidavit; DMV records showed that the target lived at the residence; and "insofar as the affidavit indicated that [the CI] had provided information for monetary consideration, it did not characterize his motives as altogether pure." Martinez-Garcia at 1216-17.

In this case, the affidavit established essentially none of the additional facts necessary to overcome the failure to disclose the CI's incentives. First and foremost, the affidavit failed to set forth whether the CI had any track record at all, let alone whether it was a positive record. It further failed to describe how the CI came to possess the information that was included in the affidavit. These are the two key components required for a court to evaluate an informant's credibility. Additionally, no other informants provided any corroboration of the CI's identification of Mr. Cole as the user of the symbol-string moniker, and the government did not independently corroborate this proposition. Essentially, with the CI's credibility eradicated, there is nothing left to support a finding of probable cause for the warrant.

The lack of additional information supporting probable cause dooms the warrant, as failure to disclose in a warrant application the fact that a confidential informant is receiving

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

benefits in exchange for information will invalidate the prior probable cause finding unless there is sufficient additional information in the affidavit to overcome the failure. See Martinez-Garcia, 397 F.3d at 1216-17; Meling, 47 F.3d at 1554-55. For this reason, the Court should hold an evidentiary hearing as a precursor to suppression.

3. The Court should ultimately suppress the fruits of the search.

After the hearing, suppression should result if, after including the including the omitted information in the warrant affidavit, probable cause is lacking. See Franks, 438 U.S. at 171-72. For all the reasons outlined above, after the hearing the defense will ask that the Court suppress all evidence uncovered pursuant to the warrant and any derivative evidence.

C. The good faith exception to the warrant requirement does not apply in this case.

The good faith exception cannot save the warrant issued in this case for two reasons: 1) because the warrant was so lacking in indicia of probable cause that reliance on the warrant was objectively unreasonable, and 2) because the exception does not apply in cases where the magistrate in issuing a warrant was misled by information in the affidavit.

In United States v. Leon, 468 U.S. 897 (1984), the Supreme Court announced a "good faith" exception to the application of the exclusionary rule. Id. at 922–23. This exception provides that the exclusionary rule should not bar the government's introduction of evidence obtained by officers acting in objectively reasonable reliance on a search warrant that is subsequently invalidated. Id. at 918–21. The good faith test is an objective one, and turns on whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization. Id. at 922, United States v. Luong, 470 F.3d 898, 902 (9th Cir. 2006). There are at least four situations in which reliance on a warrant cannot be considered objectively reasonable, and for which the good faith exception therefore cannot apply: (1) when the affiant

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

knowingly or recklessly misleads the judge with false information; (2) when the judge wholly abandons his or her neutral role; (3) when the affidavit is so lacking in indicia of probable cause that official belief in its existence is objectively unreasonable; and (4) when the warrant is so facially deficient that executing officers cannot reasonably presume it to be valid. Luong, 470 F.3d at 902.

The warrant in this case fails in regard to the first and third tests: the affiant knowingly misled the magistrate who issued the warrant, and the affidavit is so lacking in indicia of probable cause that official belief in its existence is objectively unreasonable. These will be addressed in reverse order.

1. The affidavit is so lacking in indicia of probable cause that official belief in its existence is objectively unreasonable.

The test for reasonable reliance is whether the information contained in the affidavit is sufficient to "create disagreement among thoughtful and competent judges as to the existence of probable cause." Leon, 468 U.S. at 926.

In United States v. Underwood, 725 F.3d 1076 (2013), the Ninth Circuit found the good faith exception inapplicable because the warrant affidavit was so lacking in indicia of probable cause that belief in its existence was unreasonable. The only fact supporting the probable cause finding was an observation that the defendant delivered two wooden crates to two co-conspirators in the parking lot of a hardware store. Id. at 1078. There were no other accompanying facts in the affidavit to support an inference that the crates contained drugs or that the defendant knew (or should have known) the crates contained drugs. The affidavit contained an assertion that a DEA agent believed that the crates contained drugs, but did not provide underlying facts that could be used to judge the reasonableness of such belief. Id. at 1086. The court explained that "the

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

affidavit fails to set forth a sufficient factual basis for the conclusion that Underwood was a courier for an ecstasy trafficking organization" and suppressed the evidence.

Under this precedent, the good-faith exception should not be applied to Mr. Cole's case. As discussed above, just as in Underwood, no facts in the warrant affidavit supported a finding of probable cause to believe that Mr. Cole was the person who had committed the crimes discussed in the affidavit. The affidavit contained only an unsupported conclusion that the person discussed in the affidavit was in fact Mr. Cole and did not contain any details on which the magistrate could independently evaluate this assertion. This level of detail is so grossly insufficient to probable cause that reliance on the warrant that issued based on the affidavit was unreasonable. Consequently, the good faith exception cannot save the warrant issued in this case.

2. The exception does not apply in this case because the magistrate was misled by information in the warrant affidavit.

The warrant affidavit in this case contained a material omission regarding the provision of benefits to the CI in exchange for his cooperation with the government's investigation. As such, the Court should reject any argument that the good faith exception applies here. As noted above, in Leon itself the Supreme Court expressly held that the good faith exception does not apply to motions to suppress brought under Franks where the judge was misled by a false or misleading statement. See United States v. Leon, 468 U.S. 897, 923 (1994) ("Suppression therefore remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth."). Thus, it does not apply here.

BLACK & ASKEROV, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
206.623.1604 | Fax: 206.658.2401

V. CONCLUSION

For the foregoing reasons, the defense respectfully requests that the Court grant its motion to suppress all evidence seized during the unlawful search of Mr. Cole's alleged residence located at 1218 Oxon Run, Montgomery, Texas, in this matter.

Respectfully submitted this 13th day of August, 2021.

BLACK & ASKEROV, PLLC

Christopher Black, WSBA No. 31744
Attorney for Kaleb Cole
Black & Askerov, PLLC
705 Second Avenue, Suite 1111
Seattle, WA 98104
Phone: 206.623.1604
Fax: 206.658.2401
Email: chris@blacklawseattle.com

Exhibit 1

AO 93 (Rev. 11/13) Search and Seizure Warrant

Sealed
Public and unofficial staff access to this instrument are prohibited by court order.

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1218 OXON RUN, MONTGOMERY, TEXAS AND
A 2000 FORD FOCUS, WASHINGTON STATE
LICENSE PLATE BJG6073 VIN #1FAFP3637YW420460

Case No. H20-0391M

SEALED

TRUE COPY I CERTIFY
ATTEST:
DAVID J. BRADLEY, Clerk of Court
By Kathleen Murphy
Deputy Clerk

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Texas
(identify the person or describe the property to be searched and give its location):

1218 Oxon Run, Montgomery, Texas and a 2000 Ford Focus, Washington state license plate BJG6073 VIN #1FAFP3637YW420460

In seaching these properties, law enforcement officers shall not have to knock and annouce their presence before entry into the properties.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of the crimes 82261A (Stalking), 844(e) (Mailing Threatening Communications), and 371 (Conspiracy). Evidence to be seized include, but not limited to, all electronics and digital evidence, records of victims and co-conspirators, passwords, and financial records.

See Attachement B.

YOU ARE COMMANDED to execute this warrant on or before March 10 '20 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

NS

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 2-24-20 @ 11:45 am

Judge's signature

City and state: Houston, Texas

Hon. Nancy K. Johnson, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: H20-0391M	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is 1218 Oxon Run, Montgomery, TX, 77316, further described as a single-family home with brown siding, white trim, and a white front door.

The property to be searched is the 2000 Blue Ford Focus, Washington State License Plate Number BJG6073, VIN #1FAFP3637YW420460.

ATTACHMENT B

Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is,

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities.

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism.

4. All stamps, packaging tape, and blank envelopes.

5. All receipts reflecting purchases of stamps, packaging tape, or blank envelopes in January 2020;

6. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल"

7. Digital devices or other electronic storage media and/or their components, which include:

   a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

   b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, optical scanners, desktop computer, laptops computers, tablets and mobile phones;

   c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs,

optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

8. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1218 OXON RUN, MONTGOMERY, TEXAS AND A 2000 FORD FOCUS, WASHINGTON STATE LICENSE PLATE BJG6073 VIN #1FAFP3637YW420460

Case No. H20-0391M

SEALED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

1218 OXON RUN, MONTGOMERY, TEXAS AND A 2000 FORD FOCUS, WASHINGTON STATE LICENSE PLATE BJG6073 VIN #1FAFP3637YW420460. See Attachent A.

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachent B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
2261A, 844(e), and 371	Stalking, mailing threatening communications, and conspiracy

The application is based on these facts:
See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Casey M. Villarreal, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 02/24/2020

Judge's signature

City and state: Houston, Texas

Hon. Nancy K. Johnson, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF: 1218 OXON RUN, MONTGOMERY, TEXAS AND A 2000 FORD FOCUS, WASHINGTON STATE LICENSE PLATE BJG6073 VIN #1FAFP3637YW420460	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Casey M. Villarreal, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following:

   a. Premises known as 1218 Oxon Run, Montgomery, Texas 77316, hereinafter "PREMISES," further described in Attachment A-1, for the things described in Attachment B-1.

   b. 2000 Ford Focus, Washington State License Plate BJG6073, hereinafter "VEHICLE," further described in Attachment A-2, for the things described in Attachment B-2.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since April 2008. I am currently assigned to investigate domestic terrorism in the Houston Field Office. My experience as an FBI Agent includes

the investigation of terrorism cases where individuals frequently utilize computers and the Internet to coordinate and facilitate various crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); and 371 (Conspiracy) have been committed by known and unknown persons. There is also probable cause to search the PREMISES and VEHICLE described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes, as described in Attachment B.

APPLICABLE LAW

5. Title 18, United States Code, Section 2261A provides for criminal penalties for whoever:

> with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
>
> (A) places that person in reasonable fear of the death of or serious bodily injury to a person, . . . described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A).

6. The persons described "in clause (i), (ii), (iii), or (iv) of paragraph (1)(A)" are:

> (i) that person;
>
> (ii) an immediate family member (as defined in section 115) of that person;
>
> (iii) a spouse or intimate partner of that person; or

(iv) the pet, service animal, emotional support animal, or horse of that person.

7. Title 18, United States Code, Section 876(c), provides for criminal penalties for:

> Whoever knowingly so deposits or causes to be delivered as aforesaid, any communication with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to kidnap any person or any threat to injure the person of the addressee or of another

8. Title 18, United States Code, Section 371 prohibits conspiring to commit a federal offense, and taking an overt act in furtherance of the conspiracy.

SUMMARY OF PROBABLE CAUSE

A. Overview

9. The FBI is conducting an investigation into Kaleb James **Cole**, an individual living in Montgomery, Texas. **Cole** is a high-level member and primary producer of propaganda for the Atomwaffen Division (AWD). AWD came to the attention of law enforcement on or about May 12, 2017 when Devon Arthurs was arrested for murdering two of his roommates near Tampa, Florida. Arthurs had been a member of AWD, as were his roommates. After his arrest, Arthurs admitted to the murders of his two roommates and told investigators he had committed the murders after he had converted to Islam and that the murders were his attempt at keeping the members of AWD from committing planned

acts of terror related to the group's ideology. Arthurs claimed AWD had plans to use explosives to damage infrastructure and to use firearms to commit acts of violence.

10. After Arthurs' arrest, another roommate, Brandon Russell, who was the leader of AWD, was encountered by law enforcement at the residence unharmed. In the residence, law enforcement found bomb-making precursor chemicals and hexamethylene triperoxide diamine, a high explosive chemical. Russell admitted the chemicals were his and, on or about May 20, 2017, Russell was charged in a federal criminal complaint in Florida with a violation of Title 26, United States Code, Section 5861(d) (possession of an unregistered destructive device) and Title 18, United States Code, Section 842(j)(unlawful storage of explosive material). In addition to the explosive material inside the residence, law enforcement discovered Nazi paraphernalia and a framed image on the wall in honor of Oklahoma City bomber, Timothy McVeigh.

11. Following the arrest of Russell, AWD selected John Denton, a resident of Houston, Texas, and Kaleb J. **Cole**, aka "Khimaere" or "Khim," a resident of Arlington, Washington, to co-lead AWD in Russell's absence. Members of AWD also formed a relationship with Denver, Colorado resident, James Mason, who is the writer of the book, "Siege," which serves as the basis for AWD ideology. The book, which is a collection of neo-Nazi newsletters authored by Mason, advocates the leaderless resistance and lone offender strategies as a viable means to accelerate the collapse of the system which members of AWD believe to be controlled by Jews.

12. On January 25, 2018, AWD hosted a "Death Valley Hate Camp" in Las Vegas, Nevada, where members trained in hand-to-hand combat, firearms, and created neo-Nazi propaganda videos and pictures of themselves posing with weapons. **Cole** coordinated the camp, beginning planning in early October 2017. **Cole** traveled from Washington State to Las Vegas for the hate camp with another Washington State AWD member, Aidan Bruce-Umbaugh. The two possessed concealed pistol licenses and transported numerous firearms and cases of ammunition to the event. California AWD member Samuel Woodward was expected to be at this hate camp, but could not attend due to being arrested for the murder of Blaze Bernstein, an openly gay Jewish college student.

13. Prior to YouTube removing their pages, AWD posted propaganda videos on two channels called "AWDTV" and "Atomwaffen Division." One of those videos titled "Zealous Operation," depicts a hate camp at Devil's Tower, an abandoned cement factory in Concrete, Washington. Approximately half a dozen AWD members can be seen wearing military style clothing, face masks, and carrying an assortment of long guns, while conducting paramilitary style training and shooting at a gravel pit attached to Devil's Tower. At the beginning of the video, participants state, "*GAS THE KIKES! RACE WAR NOW*!" while the statement is spelled out at the bottom of the screen.

14. On February 23, 2018, *The Seattle Times* published an article discussing AWD, and identifying several of its members nationwide, to include some in Washington State. Photographs, along with personally identifiable information, including home and

work addresses, were included in the article. The article also discussed the application Discord that members used to facilitate communication. According to the article, several thousand pages of Discord chat logs between members were hacked and leaked to the public. After having been identified, several of the AWD members, to include those in leadership positions, deleted their online profiles, quit their jobs, changed residences, and moved to the Swiss-based, encrypted electronic communication service Wire, in an attempt to go dark and avoid detection by law enforcement. **Cole** was one of the AWD members identified in this article.

15. Based on confidential human source (CHS) reporting, on or about September 16, 2018, **Cole** posted a recorded leadership message to AWD members via Wire. In the recording, **Cole** said, "*The matter of these nosy reporters coming into our daily lives, where we work, where we live, where we go in our spare time. We must simply approach them with nothing but pure aggression. We cannot let them think that they can just... that that it's safe for them to just come up to us, and fuck with us. We cannot let them think they are safe in our very presence alone...*" The statement was in response to an incident where journalist AC Thompson confronted Denton at a music festival in Texas for the "*Documenting Hate*" news series.

16. On July 9, 2019, **Cole** was interviewed by the FBI when he was deported from Canada to the United States. During the interview, **Cole** blamed the media for sensationalizing information about AWD and expressed dismay as to why he was targeted

by the media in their stories, and how he was never approached in an attempt to collect accurate information. **Cole** felt the media's reporting of AWD being a threat to the public was "*internet nonsense.*"

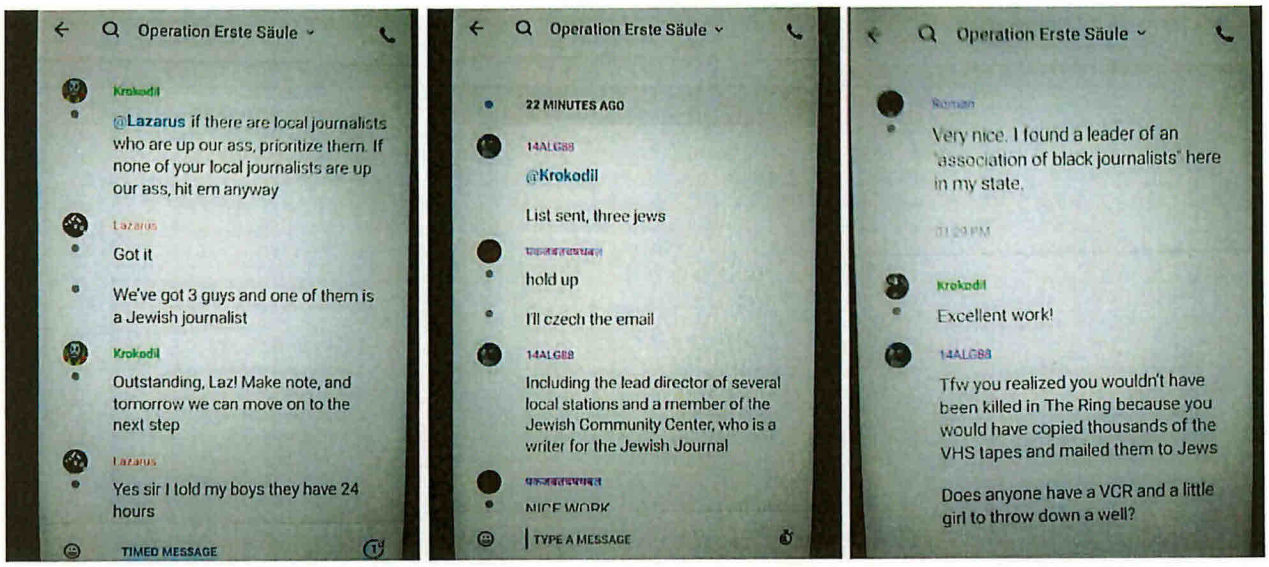
17. In August of 2019, leadership members of AWD attended a "Nuclear Congress" in Las Vegas, Nevada, where members gave presentations, discussed recent events, challenges, plans going forward, and operational security. AWD member Cameron Brandon Shea discussed the importance of keeping identity protected, and how the media continues to be a challenge to AWD.

18. On September 26, 2019, **Cole** was served with an Extreme Risk Protection Order (ERPO) by the Seattle Police Department (SPD). SPD and Arlington Police Department (APD) officers seized nine firearms in **Cole's** possession, as well as a number of milled lower rifle receivers. In the wake of the ERPO service, several news outlets nationwide covered the event. CHS reporting covered Shea, **Cole**, and other AWD members discussing and disparaging the media coverage of the event, with one member suggesting to "*hit back... embarrass the enemy on their own front.*"

19. On November 4, 2019, **Cole** and Bruce-Umbaugh were stopped by law enforcement for speeding in Post, Texas while on their way to meet with Denton, near Houston, Texas. Bruce-Umbaugh was subsequently arrested for 18 USC 922(g)(3) (Possession of a Firearm by an Unlawful User of a Controlled Substance). Law

enforcement seized four firearms and approximately 2000 rounds of ammunition. **Cole** continued to the Houston area to meet with Denton.

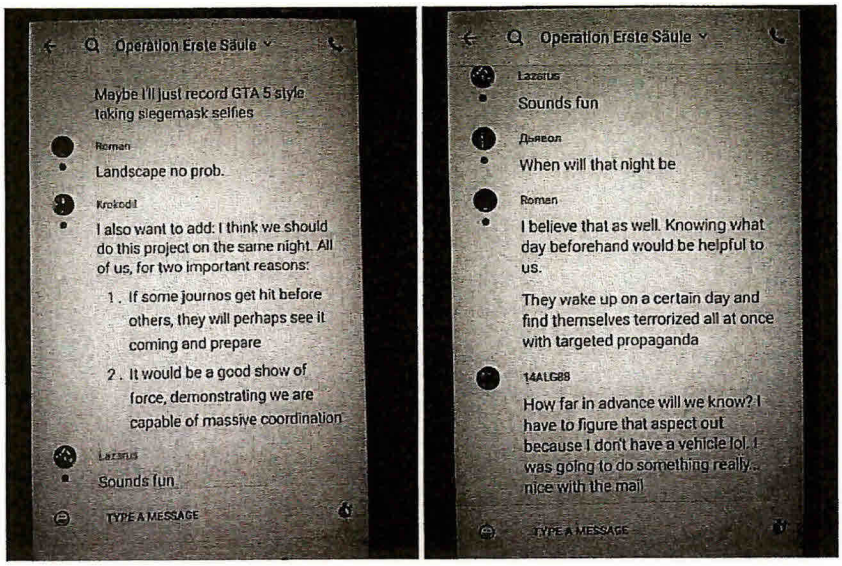
20. Per CHS reporting, in or about November 2019, Shea, using the moniker Krokodil, established a private Wire chat group titled, Operation Erste Saul. Shea invited co-conspirators "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," and "पकजबतचषथबल" to this chat group to collaborate on an effort to target journalists' homes and media buildings. According to Shea, the purpose of the operation was to "*send a clear message that we [AWD] to have leverage over them... The goal of course, is to erode the media/states air of legitimacy by showing people they have names and addresses and hopefully embolden others to act as well.*" Other participants in the chat group included **Cole**, Alexander Gosch, using the handle "14ALG88," a minor using "Lazarus," Johnny Roman Garza using Roman, and others. Shea directed each participant to identify, research, and locate journalists in their area. "Lazarus," reported that his cell had three targets, and one was Jewish. Gosch advised his cell was targeting three Jews. Roman said he found a leader of an association of black journalists in his state. Shea stated that the identification of these targets was "*Excellent work!*" and "*Outstanding.*" Shea wrote that the AWD cells in Florida, California, and Oregon had already acquired approximately 12 targets including home addresses, and that one of the targets was a "*cultural center.*" Shea went on to state that "Khim," [**Cole**] was, "*developing a number of posters that are threatening but not explicitly.*"



21. During this same discussion, Shea requested that co-conspirators email information about the targets to him within 24 hours at the email address atomtvjhfie8hjh4s[@]secmail.pro. Secmail.pro is a Finnish based company known for its privacy and security centric email service. Shea further explained that the information would be placed into custom posters for the targets. **Cole**, using the moniker "पकजबतचषथबल," stated that newer AWD initiates whose identity was not known to the public would carry out "Operation Erste Saule." Shea indicated that he too would participate in carrying out the operation because his identity was not known to the public.

22. On or about December 11, 2019, during a continued discussion to coordinate "Operation Erste Saule," Shea explained that he wanted to coordinate the operation on the same night so journalists would be caught off guard, and to accomplish an effective "*show of force, demonstrating we are capable of massive coordination.*" Roman discussed the intended impact of the coordinated plan was to "*have them all wake up one morning and*

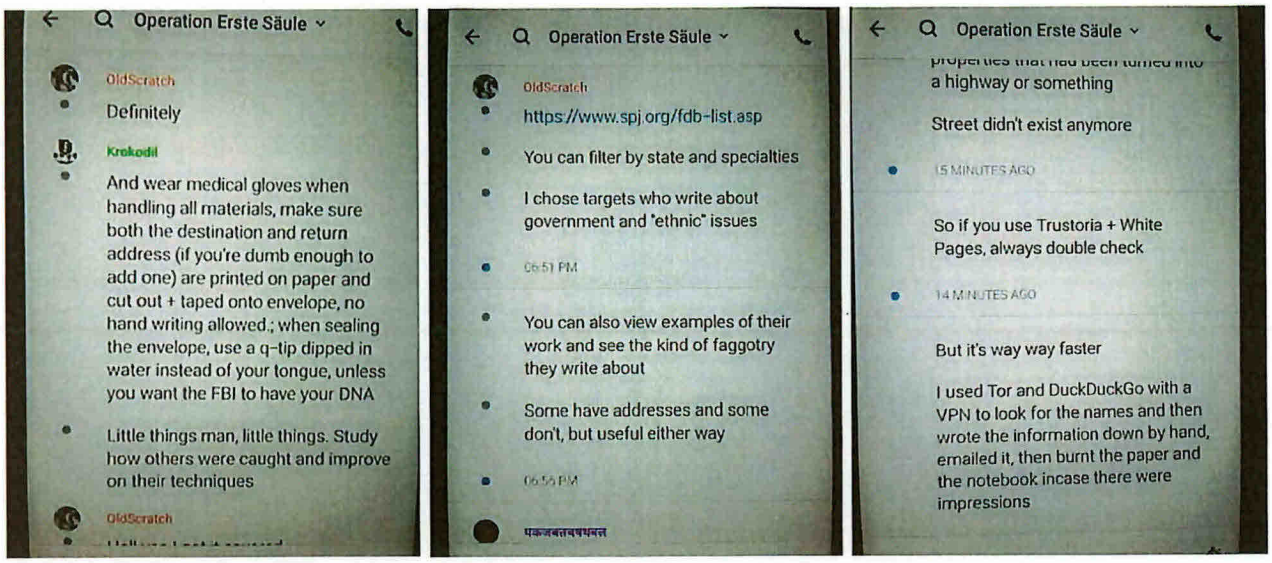
find themselves terrorized by targeted propaganda." **Cole** also suggested buying rag dolls and knives, so one could leave a doll knifed through the head, at their target location.



23. On or about December 11, 2019, during a Wire discussion to coordinate "Operation Erste Saule," **Cole** told his co-conspirators that the group was working on getting more addresses, and the posters. **Cole** suggested that his co-conspirators conduct reconnaissance of their victims' addresses and suggested searching their addresses in Google maps. **Cole** told his co-conspirators to use, "*proper electronic opsec measures*," which I believe describes an intent to anonymize or privatize their actions to avoid law enforcement and obfuscate any activity.

24. On or about December 18, 2019, during a Wire discussion to coordinate "Operation Erste Saule," **Cole** explained that he had addresses from Washington, Oregon, California, Ohio, and Florida. Shea wanted everyone to respond within 48 hours before

moving on to the next stage. Co-conspirators discussed how to print propaganda posters. Shea discussed operational security in terms of buying stamps in another town with cash while wearing a disguise. Shea also recommended using a mailbox with no cameras and to wear medical gloves to avoid prints or DNA. Another AWD member, "OldScratch," recommended using the website [https://www.spj.org/fdb-list.asp], to acquire victim addresses. This URL contains a list of journalists and their contact information for the SOCIETY OF PROFESSIONAL JOURNALISTS. "OldScratch," stated he used this method and "*chose targets who write about government and 'ethnic' issues.*"



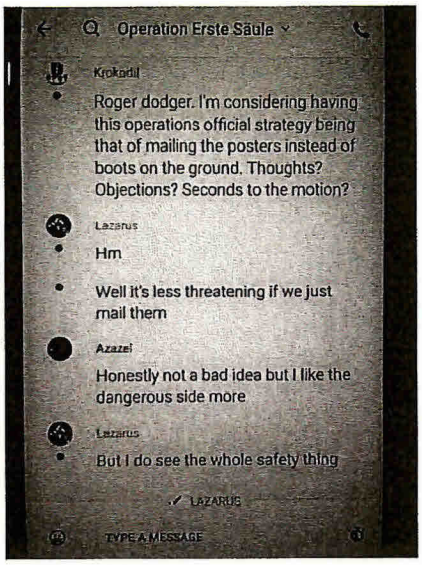
25. On or about December 25, 2019, during a Wire discussion to coordinate "Operation Erste Saule," **Cole** explained that he was going to distribute the posters via "Guerrila Mail" with the subject line, "*prop-run.*" Guerrila Mail is an electronic

communication service that offers temporary, disposable email accounts. On or about December 26, 2019, during a Wire discussion to coordinate "Operation Erste Saule," **Cole** confirmed that everyone in the group had received their propaganda poster. Taylor Ashley Parker-Dipeppe using the moniker "Azazel," provided his email address as xogofi1993[@]mailart.top, and confirmed he was in the same cell as "Lazarus." "Azazel," and "Lazarus," are members of a Florida chapter of AWD. Garza using the moniker Roman asked when they were going to execute the operation. Shea, **Cole**, and "Azazel," continued discussion to coordinate a date to execute "Operation Erste Saule."

26. On or about December 27, 2019, during the Wire discussion to coordinate "Operation Erste Saule," Shea and the group decided to execute the operation on January 25, 2020. **Cole** wanted AWD members to take video of their activities. Roman said "*scoping my places on maps right now*." "OldScratch," indicated one of his targets was in a gated community. Roman then discussed using a disguise such as wearing construction gear to blend in, or to execute the operation at night. Shea discussed using his bicycle to avert being detected by license plate readers. Roman stated how the operation was going to deliver a "*nationwide scare*."

27. On or about January 6, 2020, during a Wire discussion to coordinate "Operation Erste Saule," Shea stated his cell was, "*air tight... ready to go...*" Members again discussed the coordination of the operation and opinions on conducting the operation entirely via the mail. "Lazarus," stated "*it is less threatening if we just mail them.*"

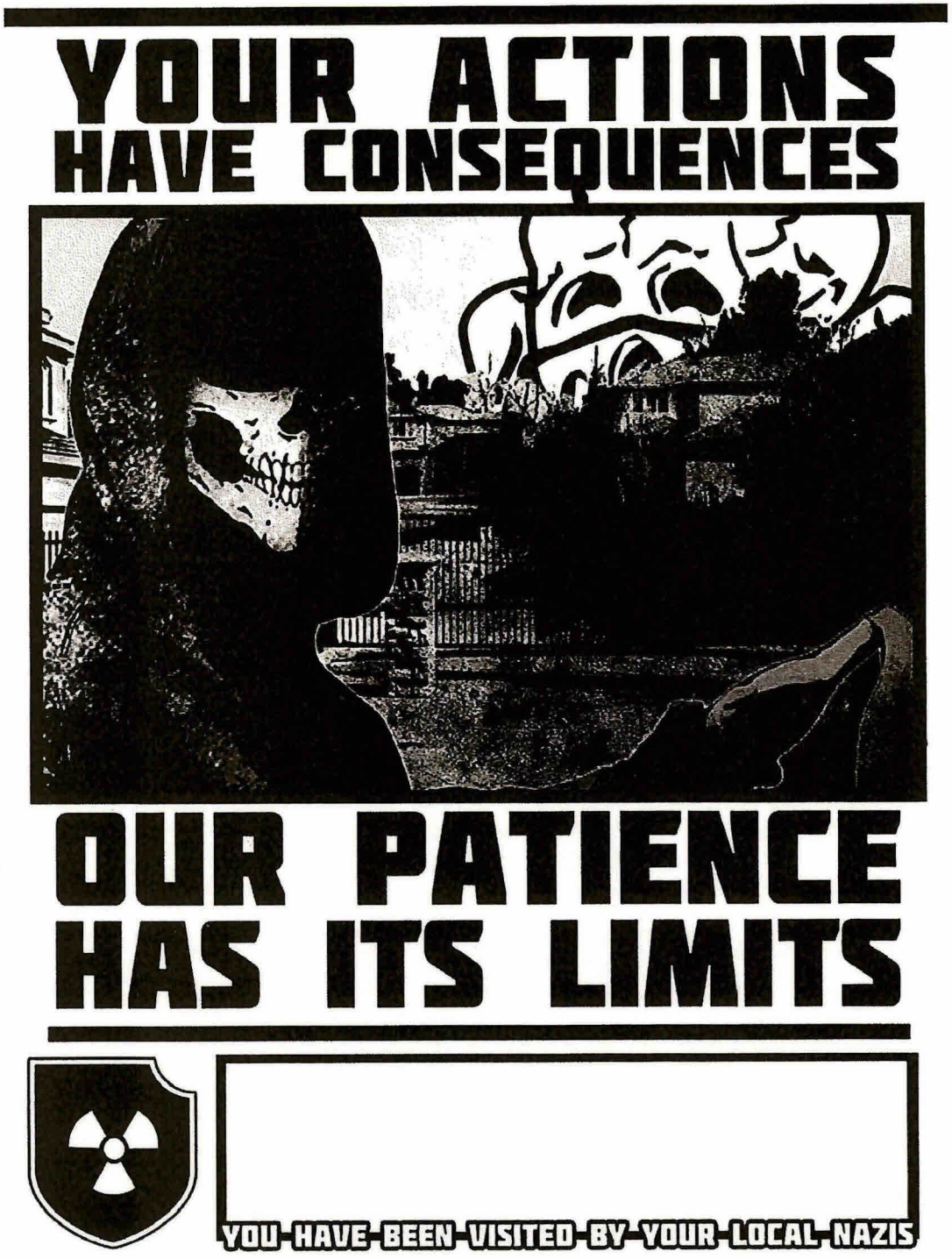
"14ALG88," had previously stated *"I plan on doing something really nice with the mail."* Shea and others ultimately decided to stay with "*boots on the ground*" at some locations and mailing them to the riskier target locations. Shea emphasized operational security, stressing the importance of not getting caught and remaining invisible to law enforcement.



28. **Cole** referenced multiple times in the chat group that he was the individual designing and creating the posters. On or about December 26, 2019, **Cole** stated he "*sent the posters out*" and that he had been "*having issues with my linux machine.*" Based on my training and experience, I understand a "linux machine" to be a personal computer utilizing the linux operating system. The posters sent to the group were directed to be mailed or posted to the home addresses of targeted journalists. All three of the posters contain threatening statements and insinuations, indicating the targets are under surveillance and

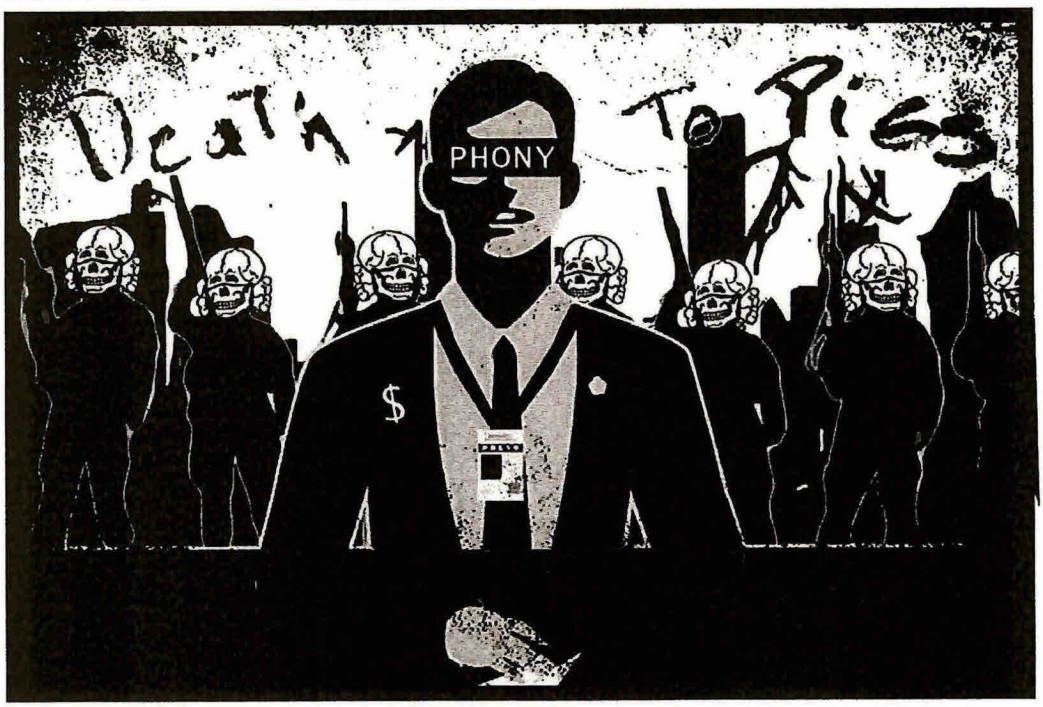
at risk from AWD and contain a blank area at the bottom designated for placement of the specific target address.

29. Based upon the group's own statements, **Cole**'s prior statements about media intimidation, and the nature of the "Operation Erste Saule" as explained by Shea, I believe **Cole**, Shea, and co-conspirators intend for the following posters, produced by **Cole**, to intimidate their respective targets, and given the nature of the prospective targets and the circumstances of "Operation Erste Saule" as outlined by Shea, these posters would cause fear, intimidation, and substantial emotional stress of their respective targets. The posters are attached hereto and made a part hereof by this reference.


YOUR ACTIONS
HAVE CONSEQUENCES
OUR PATIENCE
HAS ITS LIMITS
YOU-HAVE-BEEN-VISITED-BY-YOUR-LOCAL-NAZIS


WE ARE
WATCHING
WE ARE NOONE
WE ARE
EVERYONE
WE KNOW
WHERE YOU LIVE
DO NOT FUCK WITH US
YOU HAVE BEEN VISITED BY YOUR LOCAL NAZIS

TWO CAN PLAY AT THIS GAME



THESE PEOPLE HAVE NAMES AND ADDRESSES

YOU-HAVE-BEEN-VISITED-BY-YOUR-LOCAL-NAZIS

30. On or about January 7, 2020, Shea stated to his co-conspirators: "*If we are arrested later in connection to the operation, but they can't prove we specifically did it, fedwaffen's open sourcing of the AW brand name gives us plausible deniability…And since we have JM's [Mason] disavowal of fedwaffen on the website, saying we disavow illegal action, that further helps our point that fedwaffen was behind this.*" It is known to investigators that "fedwaffen" is a reference to a faction of unknown individuals who have in recent months, posted AWD videos and propaganda online, claiming to be AWD. However, this new unsanctioned faction and all its communications were disavowed by Mason and members of the real AWD.

31. On or about January 22, 2020, Shea informed all participants the chat group was going to be dissolved shortly. **Cole** stated "*All I can say is get a few good video clips if you can.*" Shea then reminded everyone to not get caught, and if they do, plead the 5th amendment and remind their lawyers of the "fedwaffen" defense enumerated above. The Wire chat group was subsequently closed.

B. The Events of January 25, 2020 and Following Days

1. Washington State

32. On January 25, 2020, law enforcement conducted surveillance of Shea and observed him driving his vehicle to Redmond, Washington, and park in a Target parking lot. Shea then changed into a grey hoodie, stocking cap, and a surgical facemask. Shea proceeded to walk across the street into a Fred Meyer store where he purchased a book of

Santa Claus stamps and packaging tape with cash. Based on my training, experience, and knowledge of the investigation, I believe Shea was obfuscating his appearance, consistent with the operational security measures mentioned above.

33. On January 29, 2020, the FBI was contacted by C.I., a Seattle reporter who has reported on AWD, and M.C., the director of the Anti-Defamation League's Pacific Northwest Regional Office.[1] Both had received posters in the mail. C.I. received the poster that is titled, "Two Can Play At This Game," and included C.I.'s name, his home address, and his cell phone number. M.C. received a poster titled, "Your Actions Have Consequences," and included M.C.'s home address. The envelopes in which the posters arrived were both addressed by affixing cut-out, printed addresses with packaging tape, akin to the procedure Shea described in above in paragraph 26. The envelopes also both included Santa Claus stamps.

34. On February 5, 2020, the Seattle Police Department was contacted by H.B., who was formerly employed as the director of the Anti-Defamation League's Pacific Northwest Regional Office. H.B. had recently returned from vacation when she opened her mail, and received the poster titled, "We Are Watching" which included M.B.'s name and address at the bottom. The envelope the poster arrived in was postmarked January 27, 2020, and was mailed with a Santa Clause stamp.

---

[1] The Anti-Defamation League's mission is to combat anti-Semitism and other forms of hatred and bigotry.

2. Florida

35. On January 24, 2020, law enforcement conducted surveillance of Taylor Ashley Parker-Dipeppe, who agents had previously identified as being "Azazel." Agents observed Parker-Dipeppe leave his residence, 12171 Cavern Rd, Springhill, Florida 34609 ("hereinafter FLORIDA RESIDENCE") in a white 2014 Hyundai Accent, bearing New Jersey license plate number D76HYX and Vehicle Identification Number KMHCT5AE6EU193326 (hereafter "FLORIDA VEHICLE"). Parker-Dipeppe traveled with a female and was wearing a black t-shirt, jeans, and boots.

36. The two arrived at a Goodwill Springhill Super Store in Spring Hill, Florida. They purchased a tan baseball hat, a hooded sweatshirt, yellow in color with what appeared to be black lettering on the front, and a pair of black sunglasses. The two then visited the Spring Hill Walmart. They purchased a pack of Gorilla Tape mounting tape squares. Parker-Dipeppe paid for both transactions using a debit card ending in 9799.

37. On January 25, 2020, Parker-Dipeppe and the female were observed leaving the FLORIDA RESIDENCE at approximately 8:30 p.m. The FLORIDA VEHICLE traveled towards Tampa and arrived at an apartment complex in Tampa. Parker-Dipeppe dropped off the female and picked up a male in Saint Petersburg, Florida.

38. Agents observed Parker-Dipeppe and the male entering a Saint Petersburg Walmart late in the evening. The male purchased a TT sweater and black Avia pants. Both Parker-Dipeppe and the male exited the Walmart and then drove back to Tampa.

39. Agents then observed Parker-Dipeppe and the male drive to a Tampa residence. The two affixed a poster to the front of the residence, immediately below a bedroom window. The two then ran back to the FLORIDA VEHICLE and drove away. The poster had been affixed using mounting tape squares, *i.e.*, the same type of tape that Parker-Dipeppe had purchased at Walmart.

40. The poster was the "We Are Watching" poster that is identified above. The poster included the name and home address of V.C., a Florida news reporter who was born and raised in Puerto Rico.

41. V.C. did not live at the residence. It appears that Parker-Dipeppe and the male had the wrong address. L.H., who is of African descent, lived at the residence with her father and minor child. L.H. saw the poster.

3. Arizona

42. On January 25, 2020, law enforcement conducted surveillance of Johnny Roman Garza, also known as Roman, in the Queen Creek, Arizona area. Garza was picked up by Patrick Kraft in a maroon Ford Taurus, bearing Arizona license plate 851TLX (hereafter "KRAFT ARIZONA VEHICLE"). Shortly after midnight, the KRAFT ARIZONA VEHICLE was parked near an apartment complex in Phoenix, Arizona where the leader of the Arizona Association of Black Journalists resided. At least one of the vehicle occupants exited the vehicle. The occupant returned to the vehicle, and the vehicle proceeded to the residence of M.B., who is the Editor in Chief of Arizona Jewish Life

Magazine. Both Garza and Kraft were observed fleeing from the direction of M.B.'s residence to the vehicle. The two left the scene, and Kraft dropped Garza off at his residence.

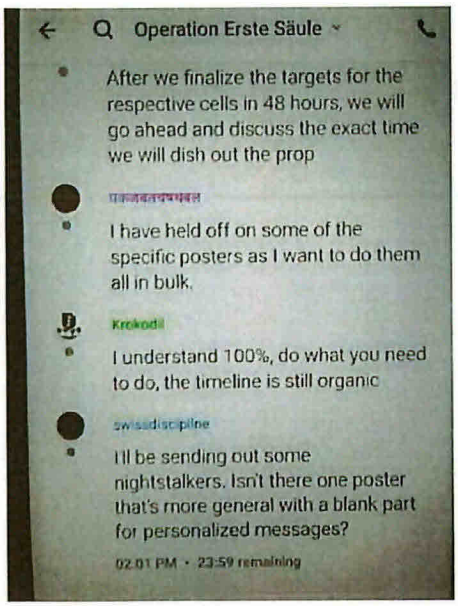
43. M.B. found a poster titled, "Your Actions Have Consequences" that included M.B.'s name and home address at the bottom. The poster was glued to a bedroom window, on the North side of M.B.'s home.

C. Cole's Involvement and Use of the PREMISES and VEHICLE

44. As discussed herein, the FBI, through its investigation, has identified numerous members of Atomwaffen Division, including **Cole**, who have planned and conspired to implement a targeted campaign with the goal of terrorizing journalists with threatening propaganda.

45. On or about December 4, 2019, Shea, using his online moniker "Krokodil," created the "Operation Erste Saule" private chat group in the WIRE application. Shea then invited **Cole**, along with several other AWD affiliates into the private group. The chat group was established and utilized for the planning and coordination of executing the targeted propaganda campaign.

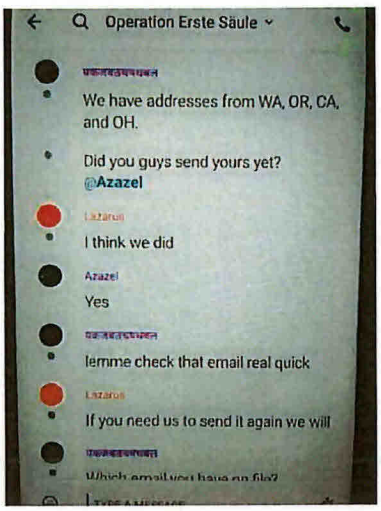
46. A main element of the operation was the production of the threatening propaganda. **Cole** referenced multiple times in the chat group that he was the individual designing and creating the posters. On or about December 26, 2019, **Cole** stated he "*sent the posters out*" and that he had been "*having issues with my linux machine.*" Based on my training and experience, I understand a "linux machine" to be a personal computer utilizing the linux operating system. Additionally, on or about December 18, 2019, **Cole** answered a question regarding a poster design by stating, "*I left it blank mostly for input of addresses.*" Based on my training and experience, individuals designing digital posters, would utilize a personal computer equipped with a software program designed to aid in the production of graphic material. The posters sent to the group via the internet, were directed



to be mailed or posted to the victims' home addresses. All three of the posters contain

threatening statements and insinuations, indicating the targets are under surveillance and at risk from AWD and contain a blank area at the bottom designated for placement of the specific target address.

47. Another element of "Operation Erste Saule" is the utilization of email to compile names and addresses of individuals the operation intends to target. On or about December 11, 2019, **Cole** responded to messages referring to addresses by stating, *"lemme check that email real quick."* Based on my training and experience, individuals check email



through an internet connection on electronic devices, such as personal computers.

48. Based on observations during surveillance, Agents observed **Cole** consistently residing at the PREMISES. On December 23, 2019, CHS reporting indicates **Cole** applied for work at an office in Conroe, TX. Conroe, TX is approximately 20 minutes by vehicle from the PREMISES. On January 9, 2020, an undercover employee (UCE) met with **Cole** and Denton at the PREMISES. The UCE was greeted by Denton in a Ku Klux

Klan robe. Both **Cole** and Denton were observed later wearing Ku Klux Klan robes. Based on the UCE's observations, **Cole** is residing on the couch in the living room of the PREMISES. A folding table is set up next to the couch, holding many of **Cole's** belongings, including two laptop computers, and a large television being used as a monitor connected to a desktop computer.

49. On January 25, 2020, a court-authorized electronic tracking device was affixed to **Cole's** VEHICLE. Based on a review of the location data collected by the device, the VEHICLE is regularly parked in front of the PREMISES overnight and on weekends. The VEHICLE leaves the PREMISES on weekdays at approximately 5:15AM CST, and travels to **Cole's** known place of employment, Medivators, 3150 Pollok Drive,

Conroe, Texas 77303. **Cole** leaves work at approximately 2:00PM CST. Surveillance last observed **Cole** on February 14, 2020, leaving work at 2:00PM CST, eventually returning to the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

50. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES or in the VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

51. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES or in the VEHICLE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not

actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

52. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of

the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES or in the VEHICLE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation,

thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions

about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to commit stalking over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for

evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

53. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

54. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

55. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

AFTERHOURS AND NO KNOCK WARRANT

56. A CHS was at the PREMISES in June 2019, and at that time observed an AK style rifle, two AR style rifles, a 12 gauge shotgun and two other rifles (type unknown). On February 17, 2020, **Cole** and Denton left the PREMISES in **Cole's** vehicle and drove to Academy Sports

and Outdoors in Conroe, Texas. Surveillance video observed **Cole** and Denton walking to the firearms section of the store and selecting multiple items for purchase. **Cole** purchased gun cleaner and a tactical rifle sling such as is commonly used on an AK or AR rifle. Denton purchased gun cleaner, gun oil, a Sig compact red dot scope, an angle mount for the scope, an AR gun cleaning kit and six 20-count boxes of 5.56 mm ammunition. Based on my training and experience, I know 5.56 mm ammunition can be used in a variety of firearms, including AK and AR style rifles. The same rifles previously observed in the PREMISES by the CHS.

57. Given the violent nature espoused by the Atomwaffen Division, the paramilitary training and large cashes of explosives found at the search of the Florida Atomwaffen residence, and the firearms and ammunition known to be in Denton's residence, the Affiant is concerned for the safety of law enforcement members executing the search warrant. Additionally, there are two other individuals at this residence, one of who will be arrested on a criminal complaint from the Eastern District of Virginia. Additionally, **Cole** will be arrested on a criminal complaint out of the Western District of Washington. The Affiant wants to ensure all occupants of the residence are at the PREMISES when the search warrant is executed so that none will remain fugitives. The Affiant therefore requests that this warrant be allowed to be executed at any hour of the day and that the agents be able to serve the warrant without first announcing their presence.

CONCLUSION

58. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and VEHICLE described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

59. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Casey M. Villarreal
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 24, 2020:

Hon. Nancy K. Johnson
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 1218 Oxon Run, Montgomery, TX, 77316, further described as a single-family home with brown siding, white trim, and a white front door.

The property to be searched is the 2000 Blue Ford Focus, Washington State License Plate Number BJG6073, VIN #1FAFP3637YW420460.

ATTACHMENT B

Property to be Seized

Documents (in whatever form) relating to violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); 245 (Federally Protected Activities); and 371 (Conspiracy), that is,

1. All documents relating to attempts to locate the home addresses of any members of the media, the Anti-Defamation League, persons who identify as Jewish, or ethnic minorities.

2. All documents relating to the Atomwaffen Division, including members of the group;

3. All documents containing swastikas, other Nazi symbols, or other symbology related to white-supremacist violent extremism.

4. All stamps, packaging tape, and blank envelopes.

5. All receipts reflecting purchases of stamps, packaging tape, or blank envelopes in January 2020;

6. All documents containing the monikers "Krokodil," "Lazarus," "14ALG88," "Azazel," "Roman," "Swissdiscipline," "OldScratch," or "पकजबतचषथबल"

7. Digital devices or other electronic storage media and/or their components, which include:

   a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

   b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, optical scanners, desktop computer, laptops computers, tablets and mobile phones;

   c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs,

optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

8. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF	§	
	§	
	§	**CASE NO.**
SEARCH WARRANT FOR	§	
1218 OXON RUN, MONTGOMERY,	§	**SEALED**
TEXAS AND	§	
A 2000 FORD FOCUS, WASHINGTON	§	H20-0391M
STATE LICENSE PLATE BJG6073	§	
VIN #1FAFP3637YW420460	§	

MOTION TO SEAL SEARCH WARRANT APPLICATION AND AFFIDAVIT

The United States of America hereby moves this Court for an order permitting it to application, affidavit, attachments, and motion to seal in the above-captioned proceedings for 180 days. For cause the Government is concerned that that disclosure of the affidavit at this time could potentially result in endangering life or physical safety of individual, flight from prosecution, evidence destruction and tampering, witness intimidation otherwise seriously jeopardizing investigation or unduly delaying trial.

Respectfully submitted,

RYAN PATRICK
UNITED STATES ATTORNEY

STEVEN T. SCHAMMEL
Assistant United States Attorney
United States Attorney's Office
Southern District of Texas
1000 Louisiana St., Ste. 2300
Houston, Texas 77002
Phone: (713) 567-9325

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF	§	
	§	
	§	**CASE NO.**
SEARCH WARRANT FOR	§	
1218 OXON RUN, MONTGOMERY,	§	**SEALED**
TEXAS AND	§	H20-0391M
A 2000 FORD FOCUS, WASHINGTON	§	
STATE LICENSE PLATE BJG6073	§	
VIN #1FAFP3637YW420460	§	

ORDER TO SEAL SEARCH WARRANT APPLICATION AND AFFIDAVIT

The United States having moved this Court, for an order to seal the application and affidavit,

IT IS ORDERED, that the search warrant application, affidavit, attachments, and motion to seal in the above-entitled proceedings, shall be under seal and shall not be disclosed for 180 days from the entry of this date.

Signed on this 24th day of Feb, 2020, at Houston, Texas.

Nancy K. Johnson
U.S. Magistrate Judge
Southern District of Texas