NOT FOR PUBLICATION

FILED

JUN 20 2025

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff - Appellee, v. LATONIA SMITH, Defendant - Appellant.	No. 24-5419 D.C. Nos. 2:19-cr-00304-WQH-VCF-1 2:23-cv-02083-WQH MEMORANDUM*

Appeal from the United States District Court
for the District of Nevada
William Q. Hayes, District Judge, Presiding

Argued and Submitted May 16, 2025
San Francisco, California

Before: M. SMITH and BRESS, Circuit Judges, and MORRIS, Chief District Judge.**

Defendant-Appellant Latonia Smith appeals the denial of her motion to vacate her conviction and sentence pursuant to 28 U.S.C. § 2255. After Smith's mother was fired, her mother's former supervisor and former employer's counsel

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable Brian M. Morris, United States Chief District Judge for the District of Montana, sitting by designation.

received threatening Facebook messages and letters. Investigators considered Smith a suspect, so they obtained a warrant to seize certain "electronic equipment" and "electronic data storage devices." After Smith assaulted her mother's former employer's counsel, investigators sought a second warrant to seize any firearm used during the assault and any cellphone she may have used to navigate to the victim's residence. But before the new warrant was signed, investigators executed the original warrant and seized Smith's cellphone during the search. Based in part on information stored on the seized cellphone, Smith was convicted of three counts of mailing threatening communications in violation of 18 U.S.C. § 876(c).

Smith filed a § 2255 motion, claiming that her trial counsel were ineffective because they did not move to suppress the cellphone evidence. The district court denied her motion, concluding that Smith had failed to demonstrate that her counsel performed deficiently. Among other things, the district court found that competent counsel could have believed the original warrant authorized investigators to seize Smith's cellphone and was not overbroad.

"When considering a *Strickland* claim based on counsel's failure to bring a suppression motion, 'the relevant question' is whether 'no competent attorney would think a motion to suppress would have failed.'" *Chong v. United States*, 112 F.4th 848, 855 (9th Cir. 2024) (quoting *Premo v. Moore*, 562 U.S. 115, 124 (2011)), *cert. denied sub nom. Tran v. United States*, 145 S. Ct. 1218 (2025).

Pursuant to that standard, Smith has not shown her counsel's performance was constitutionally deficient, so we **AFFIRM**.

1. A competent attorney could have thought the original warrant authorized investigators to seize Smith's cellphone. According to Smith, the original warrant reached only "traditional computer-related equipment associated with word processing and printing, not cell phones." But the warrant's text was much broader. It covered "[c]omputers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications[.]" Cellphones are electronic equipment that can be used to create or transmit threats. That is all the warrant required. Also, the warrant used scanners, digital cameras, and internet access devices as examples of electronic equipment. None of these items is used with computers for word processing and printing. Thus, Smith cannot cabin the warrant's text to devices used for those purposes. Even if she could, cellphones can be used for word processing and printing—as they were here.

Smith's other arguments are unpersuasive. For example, Smith argues that the warrant incorporated the affidavit by reference, and that the affidavit limited the warrant to either "the type of equipment associated with creating letters using a word processing program" or to her "personal computer." Certainly, courts can treat an affidavit as part of a warrant to help cure the warrant's overbreadth or lack

of particularity. *See, e.g.*, *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 699 (9th Cir. 2009). But Smith cites no cases holding that a warrant is otherwise limited to the items specifically flagged in the affidavit, and we do not follow such a "hypertechnical" approach to search-warrant interpretation. *See United States v. Ventresca*, 380 U.S. 102, 109 (1965). Even construing this warrant with reference to the affidavit, a competent attorney could have thought it covered cellphones. The warrant affidavit focused on Smith's computer but never said investigators were interested only in that device. To the contrary, the affidavit said investigators wanted to search the computer "[a]mong other things," and detailed threats that were sent on Facebook, not just those that appeared to be printed from a word processor.

Smith also argues that investigators knew that the first warrant did not cover cellphones, noting that investigators sought a second warrant that explicitly mentioned cellphones. An "[u]lterior motive may be evidence justifying an inference that the search exceeded the scope of the warrant . . . but it is not the determining factor, where the warrant itself was properly issued." *United States v. Ewain*, 88 F.3d 689, 694 (9th Cir. 1996). Because cellphones are "electronic equipment" and can be used to create and send threats, a competent attorney could have concluded that the original warrant covered cellphones—even if the investigators obtained the second warrant because they worried the original one

would not authorize the seizure of Smith's cellphone. Moreover, a competent attorney could have thought the investigators here sought the new warrant to obtain additional evidence about Smith's assault on her mother's former employer's counsel, not to supplement the original warrant.

2. A competent attorney could have thought the original warrant was not overbroad. "When determining whether a warrant which authorizes the seizure of a category of items is overbroad, we consider: (1) whether probable cause existed to seize all items of a category described in the warrant; (2) whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not; and (3) whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued." *United States v. Shi*, 525 F.3d 709, 731–32 (9th Cir. 2008).

First, investigators had probable cause to search all the electronic equipment that Smith could have used to create or transmit threats. The warrant affidavit established probable cause to believe that Smith sent threatening communications via Facebook message and the mail. Although people can certainly send Facebook messages on their computers, they can also do so using their cellphones. Likewise, people can, and do, prepare and print documents on their cellphones rather than their computers—as Smith herself did in this case.

Second, the warrant employed objectively definable terms like "computers," "peripherals," "electronic equipment," and "electronic data storage devices."

Finally, investigators could not have narrowed the set of devices to be seized. Smith told investigators that she had at least one laptop, but nothing suggests investigators did or could know what device or devices Smith used to prepare and send each message.

3. Because we agree with the United States that a competent attorney could have thought the first warrant covered Smith's cellphone and was not overbroad, we need not decide whether a competent attorney would have believed that the good-faith exception, or the inevitable-discovery doctrine, would make the cellphone evidence admissible notwithstanding any defects in the warrant. We also need not decide whether Smith has shown that she was prejudiced because her counsel did not move to suppress the cellphone evidence.

AFFIRMED.

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, v. LATONIA SMITH, Defendant.	Case No.: 2:19-cr-00304-WQH-VCF / 2:23-cv-02083-WQH **ORDER**

HAYES, Judge:

The matter before the Court is the Motion to Vacate, Set Aside, or Correct Sentence pursuant to 28 U.S.C. § 2255 ("Section 2255 Motion"), filed by Defendant Latonia Smith. (ECF No. 307.)

BACKGROUND

On October 29, 2019, United States Postal Inspector Justin Steele submitted an Application for a Search Warrant ("October 29 Application") to United States Magistrate Judge Daniel Albregts seeking to search and seize materials at Defendant's residence in Las Vegas, Nevada. Steele's affidavit accompanying the October 29 Application recounted a series of threatening communications via Facebook and the United States mail received by an employee of Planet Hollywood Resort and Casino ("Planet Hollywood") in Las Vegas, employees of the Fennemore Craig Law Firm in Las Vegas and Reno, and the spouse of a Fennemore Craig employee. These communications included violent and graphic language. For example, a letter received by two Fennemore Craig employees and the spouse of a Fennemore Craig employee on October 1, 2019 began: "Your throat will

be slit you will be recorded as the blood spills from your neck and just as you gasp to take your undeserving final breath three bullets will be placed right through your skull." (ECF No. 313-1 at 000167-68.) This letter continued at length with similar language and included threats to "slaughter[]" the recipients' relatives and friends, and stated that, "[w]hen you least expect it you will beg for your lives and your childrens [sic] lives." *Id*. at 000168. Another letter began, "Congratulations you have just been added to the hit list," and another letter specified that it was a "REAL THREAT." *Id*. at 000165, 000166.

Inspector Steele's affidavit in the October 29 Application asserted that "there is probable cause to believe that Latonia Smith transmitted threatening communications through the internet and through the United States mail, all in violation of Title 18, United States Code, Section 875 and 876," because:

> [T]he threatening communications began shortly after [the Planet Hollywood employee who received the communications] terminated [Annecer] Peruzar's employment with Planet Hollywood; Ms. Smith is the daughter of Ms. Peruzar; the first communication specifically references 'my mother,' the first and subsequent communications reference the same themes of workplace discrimination, wrongful termination, injustice, racism, and abuse by management and/or by [the Planet Hollywood employee]; Ms. Smith filed her own civil action against Caesar's [Entertainment, which owned Planet Hollywood,] and the law firm defending Caesar's, all in connection with Ms. Peruzar's employment litigation; the threatening communications extended to Fennemore Craig attorneys and employees involved in the civil litigation; the communications relate closely in time either to the event of Ms. Peruzar's termination or to the subsequent litigation; and the letters are addressed using the same convention of printing the address separately and affixing it to the outside of the envelope.

(ECF No. 313-1 at 000169.)

On October 29, 2019, Judge Albregts issued a Search and Seizure Warrant ("October 29 Warrant") authorizing the search of Defendant's residence and the seizure of the following:

> All documents relating to the creation or transmission of threats or threatening communications, including documents containing threatening communications.

> Any materials used to create or transmit threats or threatening communications including but not limited to: electronic printers, templates, cardstock, artwork, laminate stock, laminators, and reflective paint.
>
> Computers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to: computers, scanners, color printers, digital cameras, copy machines, internet access devices, and graphic design software.
>
> Any electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives, removable hard drives, removable storage devices (e.g. thumb or flash drives), compact discs or other optical storage devices, and other memory storage devices.
>
> The word "communication" is defined as any means of transmitting and storing information, including, without limitation, electronic signals commonly referred to as e-mail, text messages, instant messages, tweet, voice-mail, voice-messaging, private messages, video calling history, "Friend" requests, status updates; Instagram messages, electronic recordings, or other electronic means of transmitting information, including all associated metadata if stored and/or recorded in an electronic medium.
>
> The word "document" is defined as any information, communication or historical event recorded in any form or medium (paper or electronic), including, without limitation: activity logs, photographs, status updates, comments, "Friend" lists, "Friend" requests, "News Feed information," IP logs, "Neoprint," photographs, "likes," chat histories, gifts, pokes, tags, memoranda, letters, transmittals, notes, compilations, summaries, charts, receipts, invoices, bills, deposit slips, checks (front and back), forms, ledger entries, journal entries, diary entries, calendar entries, database entries, drawings and/or diagrams, and any and all associated metadata associated with information stored and/or recorded in an electronic medium.

Id. at 000189-90. The October 29 Warrant contained detailed "protocol for the electronic data seized pursuant to this Search Warrant," and stated that the warrant must be executed on or before November 12, 2019. *Id*. at 000185, 000191.

On November 1, 2019, Steele submitted an Application to Supplement the October 29 Warrant to United States Magistrate Judge Brenda Weksler ("November 1 Application"). In the accompanying affidavit, Steele stated that, on the evening of October 31, 2019, an attorney employed by Fennemore Craig, who had previously received a threatening communication described in the October 29 Application, was confronted by Defendant at his apartment in Reno. *See id*. at 000210. Steele stated that Defendant was brandishing "a matte black semi-automatic handgun" and entered the attorney's apartment. *Id*. Steele stated that, after a struggle, the attorney ran to a neighbor's apartment, where he called 911. *Id*. at 000211. Steele stated that when the police arrived, Defendant had left the property. *Id*. Steele stated:

> I know from my training and experience that cell phones are used to navigate via GPS. I also know that cell phones register, or ping, on cellular towers when used to navigate, place calls, or even when in passive receive mode. Accordingly, any cell phone used to travel from Las Vegas to Reno, or Reno to Las Vegas, to commit the assault on [the Fennemore Craig attorney] is likely to contain evidence of location monitoring, navigation, or registration on cell phone towers and thus constitute evidence of the Subject Offenses.

Id. The November 1 Application requests authorization to search for and seize "Cellular telephone devices, and any records associated with the use of those Devices," and "Any firearm or ammunition." *Id*. at 000212.

According to a Return completed by Steele, Defendant's residence was searched on November 1, 2019, between 9:32 PM and 10:52 PM. (ECF No. 312 at 000886.) Among the items seized were four cellular telephones, two electronic tablets, a laptop computer, a desktop computer, and a "Glock 17 replica air gun." *Id*.

Two hours after the search of Defendant's residence began, at 11:32 PM on November 1, 2019, Judge Weksler signed a Search and Seizure Warrant ("November 1 Warrant") as requested in the November 1 Application to Supplement the October 29 Warrant. (ECF No. 313-1 at 000205.)

On November 20, 2019, a grand jury returned an Indictment charging Defendant with five counts of Mailing Threatening Communications, in violation of 18 U.S.C. § 876(c). (ECF No. 19.)

After numerous pretrial proceedings, Defendant's case was tried to a jury commencing on April 22, 2021. (ECF No. 215.) At trial, the Government introduced evidence that was extracted from Defendant's iPhone "that was recovered pursuant to th[e] search warrant" executed on November 1, 2019. (*See* Trial Trans. at 22, ECF No. 244.) At trial, Steele testified that there was nothing of evidentiary value found on the other electronic devices seized from Defendant's residence on November 1, 2019, and nothing else seized from Defendant's residence was offered at trial. *Id*. at 71-72. The "Glock 17 replica air gun" recovered from Defendant's residence was not referenced at trial based upon the trial court's grant of Defendant's motion in limine to exclude the evidence. (*See* ECF No. 209, granting ECF No. 187.)

On April 29, 2021, the jury returned a verdict of guilty on all counts in the Indictment. (ECF No. 234.)

On February 3, 2022, Defendant was sentenced to 36 months in the custody of the Bureau of Prisons as to each count, to run concurrently to one another, followed by a three-year term of supervised release. (ECF No. 277.)

On February 10, 2022, Defendant filed a Notice of Appeal. (ECF No. 278.)

On March 15, 2023, the Court of Appeals for the Ninth Circuit issued a Memorandum Opinion affirming the Judgment of conviction. (ECF No. 305; *see also* ECF No. 306 (Mandate of the Court of Appeals).)

On December 15, 2023, Defendant, proceeding pro se, filed the pending Section 2255 Motion. (ECF No. 307.)

On January 24, 2024, the Government filed a Response in opposition to the Section 2255 Motion. (ECF No. 311.)

On February 22, 2024, Defendant filed a Reply, accompanied by an attachment.[1] (ECF No. 312.)

On April 4, 2024, the Government filed a Surreply and new exhibits. (ECF No. 313.)

On June 27, 2024, Defendant filed a Sur-Surreply and new exhibits. (ECF No. 318.)

On July 3, 2024 and July 18, 2024, Defendant filed Motions for Modification of her Sur-Surreply.[2] (ECF Nos. 321 & 323.)

CONTENTIONS OF THE PARTIES

In the Section 2255 Motion, Defendant contends:

> The second warrant [i.e., the November 1 Warrant] was sought precisely because the first warrant [i.e., the October 29 Warrant] did not authorize the seizure of items resembling cell phones. Because the officers seized cell phones without the authority of a judicial warrant, their seizure was unconstitutional and should have been suppressed. Trial counsel's failure to seek to suppress evidence based on a violation of Ms. Smith's Fourth Amendment rights is beyond the pale of an objectively reasonable strategy….
>
> Because there is a reasonable probability that the cell phone evidence would have been suppressed and of a different result at trial had the cell phone evidence been suppresses, trial counsel's failure to move to suppress was prejudicial.

(ECF No. 312 at 1-2.)

In its Surreply, the Government contends:

---

[1] In its Response, the Government asserts that the Section 2255 Motion should be summarily denied because "Smith offers nothing beyond conclusory generalities and she has failed to carry her burden to set forth facts that would entitle her to relief," and "[w]hile Smith's petition does include a notation that reads 'See attached…,' no attachment appears on either the motion filed on the Court's docket, nor the copy served on the government." (ECF No. 311 at 6.) In her Reply, Defendant includes the 22-page attachment that she asserts she "submitted … to the court with the petition" but "appears … was not scanned into the system." (ECF No. 312 at 1.) Upon review of the Court docket, Defendant is correct that she submitted the 22-page attachment with her original Section 2255 Motion, but it was filed by the Clerk of Court under seal at ECF No. 308 and a copy apparently was not served upon the Government at the time. The Court orders ECF No. 308 to be unsealed. The Court considers the attachment filed at ECF No. 308 (and publicly refiled with Defendant's Reply at ECF No. 312) to be part of the Section 2255 Motion and the Government's request to summarily deny the Section 2255 Motion is denied.

[2] Defendant's Motions for Modification of Defendant's Sur-Surreply are granted. (ECF Nos. 321 & 323.)

> Smith's claim rests exclusively on a warrant return which indicates that law enforcement completed a search of her residence before a supplemental search warrant was issued. However, the original warrant authorizing the search of Smith's residence authorized the seizure of "[c]omputers, peripherals, and all other electronic equipment used in connection with creating harassing and threatening communications, including but not limited to:… internet access devices" as well as "[a]ny electronic data storage devices used in connection with harassing and threatening communications." Accordingly, while agents obtained a supplemental in an abundance of caution, Smith's smartphones were properly seized pursuant to the initial warrant, which was issued long before law enforcement executed the search. Smith's counsel was therefore not ineffective for declining to pursue a motion to suppress on these grounds.
>
> Furthermore, review of the warrant return indicates that the agent who seized Smith's personal iPhone, which was the smartphone upon which the government relied at trial, did not participate in the search of the house. Because law enforcement seized the relevant evidence used against Smith at trial pursuant to her arrest, and that arrest itself was pursuant to a warrant, Smith suffered no prejudice from her counsel's decision not to seek to suppress items seized during the search of her home. Smith's claim therefore fails for this independent reason as well.

(ECF No. 313-1 at 2-3 (citations omitted).)

In her Sur-Surreply, Defendant contends that "[t]he iPhone labeled as Defendant's was located inside the home and collected from inside the home with all other items." (ECF No. 318 at 2.) Defendant also contends that "[t]he first warrant would have been overbroad with respect to cell phones." *Id.*; *see also* ECF No. 321 at 1. Defendant also asserts that "the Government planted evidence on her phone after the phone was illegally seized." (ECF No. 318 at 3.)

STANDARD OF REVIEW

A federal prisoner making a collateral attack on the validity of her conviction or sentence must do so by way of a motion to vacate, set aside, or correct the sentence pursuant to 28 U.S.C. § 2255. Section 2255 states:

> A prisoner in custody under sentence of a court established by Act of Congress claiming the right to be released upon the ground that the sentence was imposed in violation of the Constitution or law of the United States, or that

> the court was without jurisdiction to impose such sentence, or that the sentence was in excess of the maximum authorized by law, or is otherwise subject to collateral attack, may move the court which imposed the sentence to vacate, set aside or correct the sentence.

28 U.S.C. § 2255(a). To warrant the granting of relief, the movant must demonstrate the existence of an error of constitutional magnitude which had a substantial and injurious effect or influence on the jury's verdict. *See Brecht v. Abrahamson*, 507 U.S. 619, 637 (1993); *United States v. Montalvo*, 331 F.3d 1052, 1058 (9th Cir. 2003) ("We hold now that *Brecht*'s harmless error standard applies to habeas cases under section 2255, just as it does to those under section 2254."). Such relief is warranted where a movant has shown "a fundamental defect which inherently results in a complete miscarriage of justice." *Davis v. United States*, 417 U.S. 333, 346 (1974); *see also United States v. Gianelli*, 543 F.3d 1178, 1184 (9th Cir. 2008).

Generally, "claims not raised on direct appeal may not be raised on collateral review unless the petitioner shows cause and prejudice." *Massaro v. United States*, 538 U.S. 500, 504 (2003); *see also United States v. Ratigan*, 351 F.3d 957, 962 (9th Cir. 2003) ("A § 2255 movant procedurally defaults his claims by not raising them on direct appeal and not showing cause and prejudice or actual innocence in response to the default."). Claims of ineffective assistance of counsel are an exception and may be raised on collateral review even if they were not raised on direct appeal. *See Massaro*, 538 U.S. at 504 ("[A]n ineffective-assistance-of-counsel claim may be brought in a collateral proceeding under § 2255, whether the petitioner could have raised the claim on direct appeal."); *United States v. Jackson*, 21 F.4th 1205, 1212 (9th Cir. 2022) ("[I]neffective assistance of counsel claims may be brought in collateral proceedings under § 2255.").

RULING OF THE COURT

Defendant contends that her attorneys rendered ineffective assistance by failing to move to suppress evidence derived from her iPhone seized from her residence. There is a two-prong standard for judging a criminal defendant's contention that the Constitution

requires a conviction to be set aside because counsel's assistance at trial was ineffective. *See Strickland v. Washington*, 466 U.S. 668 (1984). First, the defendant must show that, considering all the circumstances, counsel's performance fell below an objective standard of reasonableness. *See id*. at 687-88. In making this showing, the defendant must identify the acts or omissions that are alleged not to have been the result of reasonable professional judgment. *See id*. at 690. The court must then determine whether, in light of all the circumstances, the identified acts or omissions were outside the wide range of professionally competent assistance. *See id*. at 688-90. "When counsel focuses on some issues to the exclusion of others, there is a strong presumption that he did so for tactical reasons rather than through sheer neglect." *Yarborough v. Gentry*, 540 U.S. 1, 8 (2003). "Moreover, even if an omission is inadvertent, relief is not automatic. The Sixth Amendment guarantees reasonable competence, not perfect advocacy judged with the benefit of hindsight." *Id*. at 6.

Second, the defendant must affirmatively prove prejudice. *See Strickland*, 466 U.S. at 691-92. The defendant must show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. *See id*. at 694. A reasonable probability is a probability sufficient to undermine confidence in the outcome. *See id*. The court need not address both *Strickland* requirements if the petitioner makes an insufficient showing regarding just one. *See id*. at 697; *Rios v. Rocha*, 299 F.3d 796, 805 (9th Cir. 2002) ("Failure to satisfy either prong of the *Strickland* test obviates the need to consider the other.").

To assess the two *Strickland* prongs, the Court examines the viability of a potential Fourth Amendment motion to suppress evidence derived from Defendant's iPhone seized from her residence.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause ... and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Courts analyze the "specificity" requirement through "two aspects … particularity and breadth." *United States v. SDI Future Health, Inc.*, 568

F.3d 684, 702 (9th Cir. 2009) (quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 856 (9th Cir. 1991)). "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id*. (quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d at 856-57). "Particularity means that the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize. The description must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized." *Id*. (quotation omitted). "This requirement prevents general, exploratory searches and indiscriminate rummaging through a person's belongings. It also ensures that the magistrate issuing the warrant is fully apprised of the scope of the search and can thus accurately determine whether the entire search is supported by probable cause." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (citations omitted). "However, the level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought. Indeed, warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *SDI Future Health, Inc.*, 568 F.3d at 702 (quotations omitted). In determining whether a warrant is sufficiently particular, courts "consider one or more of the following factors":

> (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.

United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006) (quoting *Spilotro*, 800 F.2d 963).

The Court focuses solely on the October 29 Warrant, because the warrant Return indicates that Defendant's residence was searched prior to the time Judge Weksler granted

the November 1, 2019 Warrant. The October 29 Warrant authorized the seizure of "[c]omputers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to … internet access devices," as well as "[a]ny electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives … and other memory storage devices." (ECF No. 313-1 at 000189.) A "smartphone," such as Defendant's seized iPhone, is a form of a "computer" or "other electronic equipment." The iPhone also is an "internet access device," an "electronic data storage device," and a "memory storage device." For example, the Cambridge Dictionary defines "smartphone" as "a cell phone that can be used as a small computer and that connects to the internet."[3] In *Riley v. California*, 573 U.S. 373, 393 (2014), the Supreme Court stated: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." *See id*. at 379 ("[T]he phone was a 'smart phone,' a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."). Similarly, the Court of Appeals for the Ninth Circuit has equated laptop computers and smartphones for Fourth Amendment purposes. *See United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019) ("The Court's view of cell phones in *Riley* so closely resembles our own analysis of laptop computers in [*United States v.*] *Cotterman*[, 709 F.3d 952 (9th Cir. 2013),] that we find no basis to distinguish a forensic cell phone search from a forensic laptop search."). The Third Circuit specifically has held that cell phones are included in the term "computer hardware" in a warrant. *United States v. Horton*, 638 F. App'x 126, 129 (3d Cir. 2016) ("The warrant, as written, defines 'computer hardware' broadly. Horton does not and cannot argue that his cell phone is not 'computer hardware' as it is defined in the warrant,

[3] *See* https://dictionary.cambridge.org/us/dictionary/english/smartphone.

which includes '*any equipment*' capable of transmitting computer data."). The Court finds that Defendant's seized iPhone fits within the scope of the broad language of electronic equipment authorized to be seized by the October 29 Warrant.

Steele's lengthy affidavit in support of the October 29 Warrant amply demonstrates probable cause to seize the items described in the October 29 Warrant, including Defendant's iPhone. (*See* ECF No. 313-1 at 000160-84.) The October 29 Warrant's description of items to be seized, including the above-quoted language and detailed definitions of "communication" and "document," are adequately tailored to the particular facts and circumstances establishing probable cause described in the affidavit. The October 29 Warrant objectively describes the items to be searched and seized with adequate specificity and sufficiently restricted the discretion of agents executing the search. As was the case in *Adjani*, 452 F.3d at 1148, the October 29 Warrant affidavit adequately limits the search for evidence of "threatening communications." (*See* ECF No. 313-1 at 000160-62, 000171.) Although the October 29 Warrant contains "including but not limited to" language, the context of the warrant limiting officers to searching and seizing materials involving threatening communications being transmitted in the mail or interstate commerce, as described in detail in the affidavit, "adequately limits the scope of the search and thus prevents it from being overbroad." *United States v. Reeves*, 210 F.3d 1041, 1046 (9th Cir. 2000) ("Appellant argues that the inclusion of the words 'may include, but is not limited to' and 'other items' in the search warrant rendered it impermissibly overbroad…. [T]he catch-all phrases of which Reeves complains exist in the context of authorization for a search for 'evidence of the possession, manufacture, and delivery of the controlled substance methamphetamine.' This context adequately limits the scope of the search and thus prevents it from being overbroad.") (citing *United States v. Washington*, 797 F.2d 1461, 1472 (9th Cir. 1986) (finding that a warrant authorizing seizure of "records, notes, [and] documents indicating [the defendant's] involvement and control of prostitution activity including but not limited to, photographs, handwritten notes, ledger books," was not overbroad, because the warrant "effectively tells the officers to seize only items

indicating prostitution activity")). The October 29 Warrant includes a detailed protocol for searching the electronic data seized pursuant to the warrant (*see* ECF No. 313-1 at 000191-95), and "[s]uch specificity increases our confidence that the magistrate judge was well aware of what he was authorizing and that the agents knew the bounds of their authority in executing the search." *Adjani*, 452 F.3d at 1149 n.7. The Court finds that the October 29 Warrant adequately sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not.

The third particularity factor is "whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued." *Adjani*, 452 F.3d at 1148 (quotation omitted). The affidavit supporting the October 29 Warrant describes in detail threatening communications, including three communications to a named Planet Hollywood employee on Facebook and multiple letters containing threatening communications which apparently were generated on word processing programs. The affidavit quotes these threatening communications verbatim and states the exact date on which each communication was received by each named recipient. In light of these specific facts, the October 29 Warrant reasonably authorized law enforcement to search for the enumerated materials in any "electronic equipment used in connection with creating or transmitting threats or threatening communications." (ECF No. 313-1 at 000189.) The Government has adequately shown that it was not able to describe the items to be searched and seized "more particularly in light of the information available to it at the time the warrant was issued." *Adjani*, 452 F.3d at 1148 (quotation omitted).

After considering the relevant factors, the Court finds that the October 29 Warrant is sufficiently particular, not overbroad, and satisfies the Fourth Amendment's specificity requirement. Moreover, even if the warrant were deficient, the Court would find that the good faith exception to suppression applies. The Government has adequately shown that Steele was not "dishonest or reckless in preparing [his] affidavit" and he "harbored an objectively reasonable belief in the existence of probable cause." *United States v. Leon*, 468 U.S. 897, 926 (1984).

Defendant asserts that "[t]he second warrant [i.e., the November 1 Warrant] was sought precisely because the first warrant [i.e., the October 29 Warrant] did not authorize the seizure of items resembling cell phones." (ECF No. 312 at 1.) Defendant relies upon Steele's statement in the November 1 Application that he sought to "expand the list of Items to Be Seized to include any firearms and cellular telephone devices." (ECF No. 313-1 at 000209; *see also* ECF No. 323 at 1.) However, "because our inquiry is an objective one, … we need not be concerned with the state of mind of the officer who executed the warrant." *United States v. Hurd*, 499 F.3d 963, 968 n.5 (9th Cir. 2007) (citing, *inter alia*, *United States v. Ewain*, 88 F.3d 689, 694 (9th Cir. 1996) (holding that an officer's subjective intent is irrelevant to the determination of whether a search is within the scope of a warrant)). "A policeman's pure heart does not entitle him to exceed the scope of a search warrant, nor does his ulterior motive bar a search within the scope of the warrant, where the warrant was properly issued." *Ewain*, 88 F.3d at 694. As discussed above, Defendant's seized iPhone fits within the scope of the electronic equipment authorized to be seized by the October 29 Warrant, regardless of Steele's subjective belief.[4]

---

[4] Even if Steele's subjective belief were relevant, it would not change the outcome of the Section 2255 Motion. A review of Steele's affidavit supporting the November 1 Application illustrates his motivation for seeking to supplement the October 29 Warrant. The affidavit supporting the November 1 Warrant recounts the October 31, 2019, physical confrontation between Defendant—who resided in Las Vegas—and an attorney employed by Fennemore Craig (who had previously received a threatening communication described in the October 29 Application) at the attorney's residence in Reno. (ECF No. 313-1 at 000210-11.) The affidavit states that "any cell phone used to travel from Las Vegas to Reno, or Reno to Las Vegas, to commit the assault on [the Fennemore Craig attorney] is likely to contain evidence of location monitoring, navigation, or registration on cell phone towers and thus constitute evidence of the Subject Offenses." *Id*. at 000211. The affidavit contains no new facts or discussion related to cell phones containing evidence of threatening communications; this subject was covered exclusively (and sufficiently) in the affidavit supporting the October 29 Warrant. Therefore, it is clear from the November 1 affidavit that the motivation for supplementing the October 29 Warrant was not a belief that evidence of cell phones containing evidence of threatening communications was not covered by the October 29 Warrant. Instead, the apparent motivation was to expand the search parameters of the seized cell phone(s) to include "evidence of location monitoring, navigation, or registration on cell phone towers," a subject which was not included in the October 29 Warrant. No evidence of location monitoring, navigation, or cell towers was ultimately introduced at Defendant's trial.

The Court finds that Defendant has failed to demonstrate that her counsel's performance fell below an objective standard of reasonableness or that she suffered prejudice based on counsel's failure to move to suppress evidence derived from Defendant's seized iPhone.

In the Sur-Surreply, Defendant contends for the first time that "the Government planted evidence on [Defendant's] phone." (ECF No. 318 at 3.) The Court does not address the merits of this claim for multiple, independent reasons. First, because Defendant raised this argument for the first time in her Sur-Surreply, the argument is waived. *See Zamani v. Carnes*, 491 F.3d 990, 997 (9th Cir. 2007) ("The district court need not consider arguments raised for the first time in a reply brief.").

Second, Defendant's entire argument on this claim of Government misconduct consists of a single sentence. Defendant offers no details indicating what evidence was purportedly "planted … on her phone," and whether this evidence was introduced at trial. "[B]ald, conclusory or inherently incredible assertions … do not require an evidentiary hearing" when considering a § 2255 motion. *United States v. Howard*, 381 F.3d 873, 879 (9th Cir. 2004); *see also United States v. Rodrigues*, 347 F.3d 818, 824 (9th Cir. 2003) ("[T]he [section 2255] petitioner is … 'required to allege specific facts which, if true, would entitle him to relief.'") (quoting *United States v. McMullen*, 98 F.3d 1155, 1159 (9th Cir. 1996)).

Finally, Defendant has made no attempt to show cause and prejudice for failing to raise this claim of Government misconduct related to "planted evidence" on direct appeal. *See Massaro*, 538 U.S. at 504; *Ratigan*, 351 F.3d at 962. "Where a defendant has procedurally defaulted a claim by failing to raise it on direct review, the claim may be raised in habeas only if the defendant can first demonstrate either 'cause' and actual 'prejudice' or that he is 'actually innocent.'" *United States v. Braswell*, 501 F.3d 1147, 1149 (9th Cir. 2007) (quoting *Bousley v. United States*, 523 U.S. 614, 622 (1998)). Defendant makes no attempt to show actual innocence. *Cf. Ratigan*, 351 F.3d at 965 ("To establish actual innocence, [a petitioner] must now demonstrate in light of all the evidence,

including new evidence that might be introduced by both sides, that it is more likely than not that no reasonable juror would have convicted him.") (quotation omitted). "The 'cause and prejudice' test for excusing the failure to raise a claim on direct appeal will apply, for example, where the claim rests upon a new legal or factual basis that was unavailable at the time of direct appeal, or where 'interference by officials' may have prevented the claim from being brought earlier." *Braswell*, 501 F.3d at 1150 (quoting *Murray v. Carrier*, 477 U.S. 478, 488 (1986)). "If a petitioner succeeds in showing cause, the prejudice prong of the test requires demonstrating 'not merely that the errors at ... trial created a possibility of prejudice, but that they worked to his actual and substantial disadvantage, infecting his entire trial with error of constitutional dimensions.'" *Id*. (quoting *United States v. Frady*, 456 U.S. 152, 170 (1982)). Defendant offers no argument or evidence of what material was allegedly "planted on her phone," why she failed to raise the issue at the time of trial or the subsequent appeal, and how the allegedly "planted" evidence "worked to [her] actual and substantial disadvantage, infecting [her] entire trial with error of constitutional dimensions." *Id*.

Defendant also requests an evidentiary hearing. The Court finds, for the reasons discussed above, that the Section 2255 Motion fails to adequately allege facts which would entitle Defendant to relief, and the Section 2255 Motion and record of the case conclusively shows that she is not entitled to relief.[5] Accordingly, the Court finds that Defendant's claims may be resolved on the record and do not require an evidentiary hearing. *See United States v. Rodriguez-Vega*, 797 F.3d 781, 792 (9th Cir. 2015).

---

[5] There is a factual dispute as to whether the iPhone introduced at trial was found by the agents in a filing cabinet inside Defendant's residence, as asserted by Defendant (*see* ECF No. 318 at 2), or found on Defendant's person as part of a search incident to Defendant's arrest, as asserted by the Government (*see* ECF No. 313-1 at 8). Because the Court finds that the Section 2255 Motion must be denied even assuming the truth of Defendant's assertion about where the iPhone was found, the Court does not conduct an evidentiary hearing to resolve this factual dispute.

A certificate of appealability is authorized "if the applicant has made a substantial showing of the denial of a constitutional right." 28 U.S.C. § 2253(c)(2). To meet this threshold substantial showing, the movant must "demonstrate that the issues are debatable among jurists of reason; that a court could resolve the issues [in a different manner]; *or* that the questions are adequate to deserve encouragement to proceed further." *Lambright v. Stewart*, 220 F.3d 1022, 1025 (9th Cir. 2000) (quoting *Barefoot v. Estelle*, 463 U.S. 880, 893 n.4 (1983)). Courts "will resolve any doubt about whether the petitioner has met the *Barefoot* standard in [her] favor." *Id*. (citation omitted). The Court finds that the *Barefoot* standard has been satisfied as to the claim in the Section 2255 Motion that Defendant's trial counsel rendered ineffective assistance by failing to move to suppress evidence derived from the seized iPhone. A certificate of appealability is granted as to this issue.

CONCLUSION

IT IS HEREBY ORDERED that the Section 2255 Motion is denied (ECF No. 307), the Motions for Modification of Defendant's Sur-Surreply are granted (ECF Nos. 321 & 323), and the filing at ECF No. 308 shall be unsealed.

A certificate of appealability is granted as to the issue of whether Defendant's trial counsel rendered ineffective assistance by failing to move to suppress evidence derived from the seized iPhone.

The Clerk of Court shall enter judgment in Case Number 2:23-cv-02083-WQH. Case Number 2:19-cr-00304-WQH-VCF remains closed.

Dated: July 29, 2024

William Q. Hayes

Hon. William Q. Hayes
United States District Court

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

FILED

SEP 11 2025

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

LATONIA SMITH,

Defendant - Appellant.

No. 24-5419

D.C. Nos.
2:19-cr-00304-WQH-VCF-1
2:23-cv-02083-WQH
District of Nevada,
Las Vegas

ORDER

Before: M. SMITH and BRESS, Circuit Judges, and MORRIS, Chief District Judge.*

The panel unanimously votes to deny the petition for panel rehearing. Judge M. Smith and Judge Bress vote to deny the petition for rehearing en banc, and Judge Morris so recommends. The full court has been advised of the petition for rehearing en banc, and no judge of the court has requested a vote on it. Fed. R. App. P. 40. The petition for panel rehearing and the petition for rehearing en banc are DENIED.

* The Honorable Brian M. Morris, United States Chief District Judge for the District of Montana, sitting by designation.

NICHOLAS A. TRUTANICH
United States Attorney
District of Nevada
Nevada Bar No. 13644
STEVEN W. MYHRE
Assistant United States Attorney
District of Nevada
Nevada Bar No. 9635
501 Las Vegas Blvd. South, Suite 1100
Las Vegas, Nevada 89101
Tel: 702.388.6336 / Fax: 702.388.6418
steven.myhre@usdoj.gov

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN THE MATTER OF THE SEARCH OF: 9748 CANYON LANDING AVENUE LAS VEGAS, NEVADA 89166	Case No. 2:19-mj-818-DJA **UNDER SEAL**

AFFIDAVIT OF JUSTIN STEELE IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Justin Steele, 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 premises located at 9748 Canyon Landing Avenue, Las Vegas, Nevada (hereinafter the "Place To Be Searched"), and to search for and seize the use, fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 875 (Transmitting a Threat in Interstate Commerce) and 876 (Mailing Threatening Communications) (hereinafter also referred to collectively as the "Subject Offenses").

2. I have been a United States Postal Inspector since 2015 and am currently assigned to the Phoenix Division of the United States Postal Inspection Service (hereinafter "USPIS"), External Crimes Team, located in Las Vegas, Nevada. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), authorized to conduct investigations into alleged violations of federal law. I hold a Bachelors' Degree in Chemistry and received federal law enforcement training from the USPIS. I have been trained to conduct, and have conducted, investigations into alleged federal crimes of mail fraud, mail theft, identity theft, credit card fraud, unlawful transportation of contraband, and the transmission of threatening communications. I have also received training and possess experience regarding the use of computers and other electronic devices to effect those crimes.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested Search Warrant and does not set forth all of my knowledge regarding the matters described herein.

4. Among other things, this application seeks a Search Warrant authorizing the seizure of any computers found at the Place To Be Searched in order to search them for evidence of threatening communications. As set out more fully below, the Place To Be Searched is the residence of Latonia Smith, the subject of the Postal Inspection Service's investigation of the Subject Offenses. During an interview with Postal Inspectors in June 2019, Ms. Smith denied any involvement in the Subject Offenses and initially consented to a search of her computer to demonstrate her non-involvement. However, shortly after giving her consent, she withdrew it, claiming that she needed her computer to study for the MCAT. The warrant I apply for today seeks authorization to seize and search that computer for evidence of threatening communications.

SUBJECT OFFENSES

5. The USPIS is conducting an investigation into the Subject Offenses, arising from a number of threatening communications believed to be mailed or transmitted by Latonia Smith, the daughter of a former employee of the Planet Hollywood Hotel and Casino in Las Vegas, Nevada. As described more fully below, there is probable cause to believe that Ms. Smith became angered following the termination of her mother's employment at Planet Hollywood, causing her to send threatening communications to her mother's former supervisor in reprisal for the firing. Later, after related civil lawsuits were filed against Caesar's Entertainment – the parent company of Planet Hollywood – Ms. Smith is believed to have sent threatening communications to lawyers and employees representing Caesar's in those suits.

FACTS ESTABLISHING PROBABLE CAUSE

6. In September 2018, Samantha Radak reported that she began receiving threatening and harassing communications through Facebook shortly after firing an employee at Planet Hollywood Resort and Casino ("Planet Hollywood"), where Ms. Radak worked as a supervisor. Ms. Radak explained that in November 2017, she fired Annecer Peruzar for allegedly taking change from a customer while cleaning the customer's room. Shortly after terminating Ms. Peruzar's employment, Ms. Radak began receiving the threatening and harassing communications, copies of which communications she provided to me and which I describe below.

a. On December 7, 2017, a Facebook user under the name of Medina Sinclair transmitted the following communication to Ms. Radak via Facebook:

> I have to say you fired my mom in the most blatant discriminatory act. My mom works hard and loves her job. She supports us kids at UNLV and would never jeopardize her job over a tip that you can't even buy a Coke with. She worked for the company for more than 3 years with a clean file and you fired her for no reason except racial hatred. She broke no policies, and you did not have any

> ground to suspend or fire her. Instead, you abused the handbook, used unrelated policies, and conspired with a supervisor who hates black people to rid good employee of her job based also on your personal racial bias. There is proof that you singled her out and I hope your upper management shows you more mercy than you showed my mother because I am finding every action that can be taken against this wrongful termination and discriminatory act to ensure my mom gets her job back; I will not stop! Heartless and evil!

b. On December 22, 2017, a Facebook user under the name of Aus Riley, transmitted the following communication to Ms. Radak via Facebook:

> And you're still a racist prick. And all of your racist friends that support you at work are uneducated pricks and puppets. Feel dumb yet after firing minorities and using the excuse that they stole $1?! No! We just have dumb bigoted leaders running this country and running institutions, trying to make decisions that they're incapable of making. Decisions like "hmmm why would my loyal employees steal $1? Let me implement a policy to prevent miscommunications with TIPS and give ALL employees a warning." NO! Your racist ego is the only thing that drives your thought processes because everyone else outside your little "Hitler" circle knows YOU ARE WRONG. Your ego and pathetic need for power won't let you admit that....sad. But to you and every other leader that wants to follow in your footsteps (image of a middle finger) We won't tolerate hate and we'll make sure there's no place in our society for you animals. Probably a racist Trump supporter...pathetic.

c. On March 8, 2018, a Facebook user under the name of Simone Wiley communicated the following to Samantha.Radak:

> Think you were forgotten about. You're very easy to find petty bitch...remember that. We will get the last laugh (laughing while crying emoji)"; "samantha jean radak who lives in rhodes ranch. How's your new place? Dumb bitch.; in life you only live because others allow you to.

7. During the time frame beginning in December 2017 and through August of 2018, Ms. Radak also received 3 letters delivered via U.S. Mail, each letter containing threatening communications. Images of each letter's corresponding postmarked envelope is attached at Exhibit 1. As is apparent from the outside of the envelopes, each letter was sent to the same address: 214 August Course Avenue, Las Vegas, NV 89148, which is the business address for Caesar's Entertainment, the parent company of Planet Hollywood and Ms. Radak's employer.

Only one of the envelopes specifies Ms. Radak as the addressee but, as explained more fully below, the content of each letter appears to address the same issue and appears to be directed at Ms. Radak.

8. As shown in Exhibit 1, the address on each envelope appears to have been printed on a separate sheet of paper, cut out, and then affixed to the outside of the envelope. On two of the envelopes, the same convention appears to have been followed with regard to the return address, which references the Democratic National Convention or "DNC."

9. Each of the letters contained in its corresponding envelope is printed on plain white paper and the words appear to have been generated by using a word processor and conventional electronic printer. The content of each letter is addressed below.

10. The letter contained in the envelope postmarked on December 20, 2017, states as follows:

> No matter how much you (and your little friends) feel like a dictator bitch at work, you're not untouchable cunt. Karma will be waiting around the corner for you. Oh and thanks for the motivation to work ten times harder to make sure we don't have uneducated and hateful pricks like you as leaders over anything but the dumb shit that manages to spew from your mouths. Ta-ta (laughing while crying emoji)

11. The letter contained in the envelope postmarked on May 17, 2018, states as follows:

> You and the racist managers who protect you leave and we will stop we will not stop until racists are out of our workplaces and society
> RACIST

12. The letter contained in the envelope postmarked on August 11, 2018, states as follows:

> You have lived seven months pass the new year
> Yoouu (sic) do not deserve the air you breathe
> We have been kind
> At times Forgiving
> Evil and greed is at the heart of us all

But Those with power should reevaluate their actions
Seek penance fix your ways and actions or you will all die
All
Starting with the head
The very very top first
Mark these words
We have entered a new era
We rule
No one is untouchable
No one
Racist Motherfuckers
Keep fucking with us
ALL WILL REGRET
REAL THREAT
FIX IT
Deadline Monday December 31, 2018: YOU BETTER FIX IT
Pass Along

13. In November 2018, Ms. Peruzar, filed a civil action against Caesar's in Nevada state court, alleging Intentional Tort (fraud/misrepresentation/malice), Employer Defamation, and Intentional Infliction of Emotional Distress. Caesar's retained the law firm of Fennemore Craig to defend the civil suit.

14. In April 2019, Latonia Smith filed a civil action in Nevada state court against Caesar's and others, alleging slander, defamation, intentional infliction of emotional distress, malicious prosecution, abuse of process arising from the termination of Ms. Peruzar. In May 2019, Ms. Smith filed a second lawsuit against the Fennemore Craig law firm in United States District Court, alleging civil conspiracy, slander, defamation, intentional infliction of emotional distress. A Fennemore Craig employee, Shawna Braselton, signed subpoena service orders in connection with the litigation and Attorney Wade Beavers made appearances in these lawsuits on behalf of the Fennemore Craig law firm.

15. On April 25, 2019, the Fennemore Craig firm received two letters contained in a single envelope, mailed to the following addressees: ATTN: SHAWNA BRASELTON OR WADE BEAVERS, 300 E 2ND STREET SUITE 1510, RENO NEVADA 89501. The words

contained in the letters were printed on plain white paper and appear to have been generated from a word processor and accompanying electronic printer. The first letter stated as follows:

> CONGRATULATIONS YOU HAVE JUST BEEN ADDED TO THE HIT LIST
> NO ONE IS WALKING AWAY UNSCATHED
> FROM THE VERY TOP
> TO THE VERY BOTTOM
> P.S. CONGRATES ON YOUR WEDDING SHAWNA. HOPEFULLY YOULL BE AROUND FOR MANY YEARS TO ENJOY IT
> THE PEOPLE HAVE SUFFERED VIOLENCE AND THE VIOLENT TAKE IT BY FORCE
> BEHOLD I WILL BRING EVIL UPON THEM WHICH THEY SHALL NOT BE ABLE TO ESACAPE AND THOUGH THEY SHALL CRY I WILL NOT HEARKEN UNTO THEM
> THIS IS AMERICA

16. The second letter stated as follows:

> NOT A KILLER BUT DON'T PUSH IT
> REVENGE IS THE SWEETEST JOY AND EVERY SINGLE ONE OF YOU WILL MEET IT FACE TO FACE
> NO ONE WILL BE SAFE
> KEEP IT UP SICK BASTARDS
> MOVING UP ON THE HIT LIST
> 6 FEET UNDER OR BURNED
> WHATEVER IS PREFERRED
> THE CULMINATION
> YEARS IN THE PLANNING
> LAW IS JUST A FRIENDLY SOLUTION
> MIDDLE FINGER TO AMERICAN JUSTICE
> MIDDLE FINGER TO AN EYE FOR AN EYE
> IT'LL BE THE END OF LIVES
> EMBODYING THE RAGE OF ALL MASS MURDERERS
> KEEP PUSHING
> DON'T GIVE TWO FLYING FUCKS ABOUT GETTING RID OF ALL SCUM
> FOR GOOD
> WILL NEVER SEE IT COMING
> IT WILL JUST BE LIGHTS OUT
> ALL CAN ANSWER TO WHATEVER FUCKING DEITY WISHED
> OR JUST BURN

17. As with the letters sent to Radak, the address on the outside of the corresponding envelope appears to have been printed on a separate sheet of paper, cut out, and then affixed to

the front of the envelope.

18. On June 11, 2019, another Postal Inspector and I interviewed Latonia Smith at her residence located at 9748 Canyon Landing Ave., Las Vegas, NV 89166. During the interview, Smith denied sending any threatening letters and stated she was being "set up," referring to the lawsuit that she had filed against Caesar's Entertainment. Smith was advised to cease and desist sending the letters and she again denied her involvement. I asked if she would consent to a search of her computer to prove that she was not involved. Smith initially agreed but quickly provided reasons to postpone the surrender of her computer, stating that she needed the computer to study for the MCAT. I gave Smith my business card and asked her to call to set up a time to surrender her computer after she finished her studies. I was never contacted by Smith thereafter.

19. On October 1, 2019, I was contacted by Craig Etem Director of the Fennemore Craig Law Firm in Reno, NV. Etem stated that on September 30, 2019, two (2) employees of Fennemore Craig – Shannon Pierce and Tyre Gray – each received letters through the U.S. mail containing threatening communications. Etem stated that Pearce and Gray had signed affidavits or pleadings in connection with the civil action brought by Smith.

20. One letter was addressed to Pearce at 300 E Second St. Suite 1510, Reno NV 89051, one of the business addresses for Fennemore Craig. The other was addressed to Gray at 300 S 4th St, Suite 1400, Las Vegas NV 89101, also a business address for the law firm. Each of the letters contained in its corresponding envelope is printed on plain white paper and the words appear to have been generated by using a word processor and conventional electronic printer. The content of each letter is addressed below.

21. Both letters contain the same communication as follows:

Your throat will be slit you will be recorded as the blood spills from

> your neck and just as you gasp to take your final undeserving breath three bullets will be placed right through your skull You will be hunted to the ends of the earth young or old You and every blood relative you leave behind you and every friend you have you and every person who speaks to you you and every person who helps you you and every single one of you will suffer and will be slaughtered like less than animals When you least expect it you will beg for your lives and your childrens lives. Everyone around you will die a painful death The marks of your dried tears will be left with your bloodied brain splattered across the floor your body will be fed to the animals and the insects who sit about you Petition the gods to die a different death petition them to grant you mercy in the next life because none will be found in this one and there will be no mercy in your death petition them for some other death than the one that will meet you at the hands of the black and pale horse because when you are caught there will only be suffering the horses have been dispatched jihad has been declared against you the black horse carries scales in his hand the pale horse has a rider and his name is death they will hunt you until they rid you of your place here they will come like thieves in the night and your destruction will come suddenly like labor pains your suns will become black like sackcloth and your moons will become like blood you will stand before the white throne of the gods and they will judge you using the book of life you will be thrown with hades and death into the lake of fire the gods will reward those who bring you to your end through pain and suffering (Arabic symbols)
> You will suffer and die for your sins may the odds of a different death be ever in your favor"

22. On October 1, 2019, Jean Wirthlin received a letter containing the same communication recounted above, which letter was delivered via U.S. Mail to her home at 9947 Coyote Echo Ct., Las Vegas, NV 89166. Wirthlin stated her husband was an attorney with the Fennemore Craig law firm. As with the other letters described above, the address on the corresponding envelope was printed on a separate piece of paper, cut out, and stapled onto the envelope. The letter contained in its envelope was printed on plain white paper and the words appear to have been generated by using a word processor and conventional electronic printer.

23. Based on my training and experience, I know that computers and computer programs, specifically word processing programs, are used to generate letters and threatening communications contained in letters, such as those described above. Communications

generated by computer programs are often stored in storage devices associated with the computer and can be recovered forensically even if they have been deleted from the storage medium. I also know that electronic printers associated with the computer are used to print documents and communications generated on computer programs.

24. Based on the foregoing, I submit that there is probable cause to believe that Latonia Smith transmitted threatening communications through the internet and through the United States mail, all in violation of Title 18, United States Code, Section 875 and 876. As shown above, and among other things, the threatening communications began shortly after Ms. Radak terminated Ms. Peruzar's employment with Planet Hollywood; Ms. Smith is the daughter of Ms. Peruzar; the first communication specifically references "my mother," the first and subsequent communications reference the same themes of workplace discrimination, wrongful termination, injustice, racism, and abuse by management and/or by Ms. Radak; Ms. Smith filed her own civil action against Caesar's and the law firm defending Caesar's, all in connection with Ms. Peruzar's employment litigation; the threatening communications extended to Fennemore Craig attorneys and employees involved in the civil litigation; the communications relate closely in time either to the event of Ms. Peruzar's termination or to the subsequent litigation; and the letters are addressed using the same convention of printing the address separately and affixing it to the outside of the envelope.

PLACE TO BE SEARCHED

25. I further submit that there is probable cause to believe that evidence of the Subject Offenses is likely to be found at the Place To Be Searched as described below and in Attachment A to the Search Warrant, as follows:

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166:

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

26. The Place to Be Searched is the current residence of Latonia Smith as confirmed through independent sources, by driving by and visiting the residence, and by my interview of Ms. Smith.

ITEMS TO BE SEIZED

27. Based on the foregoing, I further submit there is probable cause to believe that located in the Place To Be Searched are the use, fruits, instrumentalities and evidence of violations of Title 18, United States Code, Sections 875 and 876 ("Subject Offenses") as described below and in Attachment B to the Search Warrant.

Indicia of occupancy for 9748 Canyon Landing Ave., Las Vegas, NV, 89166.

Evidence of violations of the Subject Offenses

All documents relating to the creation or transmission of threats or threatening communications, including documents containing threatening communications;

Any materials used to create or transmit threats or threatening communications including but not limited to: electronic printers, templates, cardstock, artwork, laminate stock, laminators, and reflective paint.

Computers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to: computers, scanners, color printers, digital cameras, copy machines, internet access devices, and graphic design software.

Any electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives, removable hard drives, removable storage devices (e.g. thumb or flash drives), compact discs or other optical storage devices, and other memory storage devices.

The word "communication" is defined as any means of transmitting and storing information, including, without limitation, electronic signals commonly referred to as e-mail, text messages, instant messages, tweet, voice-mail, voice-messaging, private messages, video calling history, "Friend" requests, status updates; Instagram messages, electronic recordings, or other electronic means of transmitting information, including all associated metadata if stored and/or recorded in an electronic medium.

The word "document" is defined as any information, communication or historical event recorded in any form or medium (paper or electronic), including, without limitation: activity logs, photographs, status updates, comments, "Friend" lists, "Friend" requests, "News Feed information," IP logs, "Neoprint," photographs, "likes," chat histories, gifts, pokes, tags, memoranda, letters, transmittals, notes, compilations, summaries, charts, receipts, invoices,

bills, deposit slips, checks (front and back), forms, ledger entries, journal entries, diary entries, calendar entries, database entries, drawings and/or diagrams, and any and all associated metadata associated with information stored and/or recorded in an electronic medium.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for and seize documents that might be found in the Place To Be Searched, in any form or medium, including electronic. Accordingly, documents might be found in data stored electronically 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).

29. *Probable cause.* I submit that if a computer or storage medium is found in the Place To Be Searched, there is probable cause to believe those documents and 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."

30. *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 Place To Be Searched 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 communicate threats, 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.

31. *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.

32. *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.

COMPUTER SEARCH PROTOCOLS

33. The USPIS intends to follow the protocols found at Attachment C to the Search Warrant and incorporated herein when conducting a search of any electronic devices found at the Place To Be Searched and included in the Items To Be Seized.

SEALING

34. I further request that the Search Warrant, Supporting Application and Affidavit be sealed until further order of the Court. This is an ongoing investigation involving a crime of violence (communication threats of death or injury) and the public disclosure of the information contained herein at this time may likely compromise the investigation to include: tipping off any perpetrators affording them time to destroy evidence or to abscond; identifying victims of the threats subjecting them to be re-victimization; and revealing the identity of person(s) suspected of committing criminal offenses and subjecting them to public scorn or humiliation before they have been formally charged and afforded due process of law.

CONCLUSION

35. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Items To Be Seized as forth in Attachment B, constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 875 and 876, and are likely to be found at the Place To Be Searched, as described at Attachment A.

/s/
Justin Steele
United States Postal Inspector

Subscribed and sworn to before me on this 29th day of October 2019.

DANIEL J. ALBREGTS
United States Magistrate Judge

ATTACHMENT A

PLACE TO BE SEARCHED

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

ATTACHMENT B

ITEMS TO BE SEIZED

I. **Statutes Violated.**

Potential violations of federal law include: Title 18, United States Code, Sections 875 (Transmission of Threat In Interstate Commerce) and 876 (Mailing Threatening Communications) (also referred to as "Subject Offenses").

II. **Description of Items To Be Seized.**

Evidence of indicia of occupancy for 9748 Canyon Landing Ave., Las Vegas, NV, 89166.

Evidence of violations of the Subject Offenses.

All documents relating to the creation or transmission of threats or threatening communications, including documents containing threatening communications.

Any materials used to create or transmit threats or threatening communications including but not limited to: electronic printers, templates, cardstock, artwork, laminate stock, laminators, and reflective paint.

Computers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to: computers, scanners, color printers, digital cameras, copy machines, internet access devices, and graphic design software.

Any electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives, removable hard drives, removable storage devices (e.g. thumb or flash drives), compact discs or other optical storage devices, and other memory storage devices.

The word "communication" is defined as any means of transmitting and storing information, including, without limitation, electronic signals commonly referred to as e-mail, text messages, instant messages, tweet, voice-mail, voice-messaging, private messages, video calling history, "Friend" requests, status updates; Instagram messages, electronic recordings,

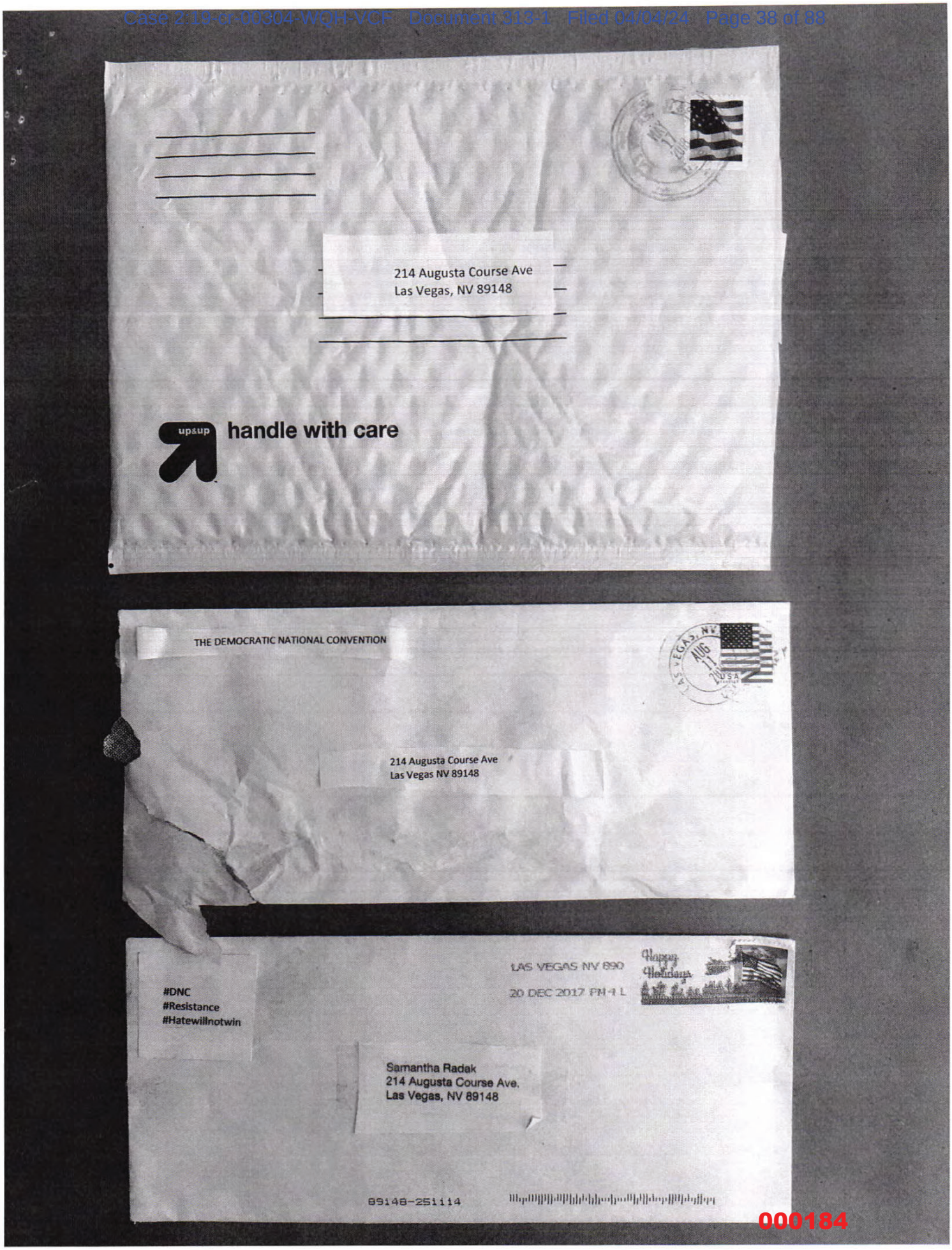
or other electronic means of transmitting information, including all associated metadata if stored and/or recorded in an electronic medium.

The word "document" is defined as any information, communication or historical event recorded in any form or medium (paper or electronic), including, without limitation: activity logs, photographs, status updates, comments, "Friend" lists, "Friend" requests, "News Feed information," IP logs, "Neoprint," photographs, "likes," chat histories, gifts, pokes, tags, memoranda, letters, transmittals, notes, compilations, summaries, charts, receipts, invoices, bills, deposit slips, checks (front and back), forms, ledger entries, journal entries, diary entries, calendar entries, database entries, drawings and/or diagrams, and any and all associated metadata associated with information stored and/or recorded in an electronic medium.

This Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and separately sealed, as though set forth fully herein.

EXHIBIT "1"

EXHIBIT "1"


214 Augusta Course Ave
Las Vegas, NV 89148
up&up
handle with care
THE DEMOCRATIC NATIONAL CONVENTION
214 Augusta Course Ave
Las Vegas NV 89148
#DNC
#Resistance
#Hatewillnotwin
LAS VEGAS NV 890
20 DEC 2017 PM 4 L
Happy Holidays
Samantha Radak
214 Augusta Course Ave.
Las Vegas, NV 89148
89148-251114
000184

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

9748 CANYON LANDING AVENUE
LAS VEGAS, NEVADA 89166

Case No. 2:19-mj-818-DJA

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 _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

See Attachment "A".

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)*:

See Attachment "B".

YOU ARE COMMANDED to execute this warrant on or before 11/12/19 *(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.

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 HONORABLE DANIEL J. ALBREGTS
(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: 10/29/19 4:19 pm

DANIEL J. ALBREGTS
Judge's signature

City and state: Las Vegas, Nevada

HONORABLE DANIEL J. ALBREGTS
Printed name and title

000185

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

Return

Case No.: 2:19-mj-	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

000186

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

000187

ATTACHMENT A

PLACE TO BE SEARCHED

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

ATTACHMENT B

ITEMS TO BE SEIZED

I. **Statutes Violated.**

Potential violations of federal law include: Title 18, United States Code, Sections 875 (Transmission of Threat In Interstate Commerce) and 876 (Mailing Threatening Communications) (also referred to as "Subject Offenses").

II. **Description of Items To Be Seized.**

Evidence of indicia of occupancy for 9748 Canyon Landing Ave., Las Vegas, NV, 89166.

Evidence of violations of the Subject Offenses.

All documents relating to the creation or transmission of threats or threatening communications, including documents containing threatening communications.

Any materials used to create or transmit threats or threatening communications including but not limited to: electronic printers, templates, cardstock, artwork, laminate stock, laminators, and reflective paint.

Computers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to: computers, scanners, color printers, digital cameras, copy machines, internet access devices, and graphic design software.

Any electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives, removable hard drives, removable storage devices (e.g. thumb or flash drives), compact discs or other optical storage devices, and other memory storage devices.

The word "communication" is defined as any means of transmitting and storing information, including, without limitation, electronic signals commonly referred to as e-mail, text messages, instant messages, tweet, voice-mail, voice-messaging, private messages, video calling history, "Friend" requests, status updates; Instagram messages, electronic recordings,

or other electronic means of transmitting information, including all associated metadata if stored and/or recorded in an electronic medium.

The word "document" is defined as any information, communication or historical event recorded in any form or medium (paper or electronic), including, without limitation: activity logs, photographs, status updates, comments, "Friend" lists, "Friend" requests, "News Feed information," IP logs, "Neoprint," photographs, "likes," chat histories, gifts, pokes, tags, memoranda, letters, transmittals, notes, compilations, summaries, charts, receipts, invoices, bills, deposit slips, checks (front and back), forms, ledger entries, journal entries, diary entries, calendar entries, database entries, drawings and/or diagrams, and any and all associated metadata associated with information stored and/or recorded in an electronic medium.

This Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and separately sealed, as though set forth fully herein.

Attachment C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set

out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in the Attachments; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, Section II, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

This warrant expressly incorporates the Affidavit submitted in support of the warrant, and separately sealed, as though set forth fully herein.

Attachment C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set

out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in the Attachments; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, Section II, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

This warrant expressly incorporates the Affidavit submitted in support of the warrant, and separately sealed, as though set forth fully herein.

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

9748 CANYON LANDING AVENUE
LAS VEGAS, NEVADA 89166

Case No. 2:19-mj- 845-BNW

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 _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

See Attachment "A".

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)*:

See Attachment "B".

YOU ARE COMMANDED to execute this warrant on or before _____ *(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.

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 HONORABLE BRENDA N. WEKSLER .
(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: 11/19 11:32 pm

Judge's signature

City and state: Las Vegas, Nevada

HONORABLE BRENDA N. WEKSLER
Printed name and title

000201

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

Return

Case No.: 2:19-mj-	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

000202

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

000203

ATTACHMENT A

PLACE TO BE SEARCHED

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

ATTACHMENT B

ITEMS TO BE SEIZED

I. **Statutes Violated**.

Potential violations of federal law include: Title 18, United States Code, Sections 875 (Transmission of Threat In Interstate Commerce), 876 (Mailing Threatening Communications), and 924(c) (Use of a Firearm in Relation to A Crime of Violence (also referred to as "Subject Offenses").

II. Description of Items To Be Seized

Cellular telephone devices, and any records associated with the use of those devices.

Any firearm or ammunition.

This list is intended to supplement the list of items to be seized as found in the Warrant authorized on October 29, 2019 for the search of the Place to Be Searched.

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

9748 CANYON LANDING AVENUE
LAS VEGAS, NEVADA 89166

Case No. 2:19-MJ-845-BNW

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):*
See Attachment "A".

located in the _____ District of Nevada, there is now concealed *(identify the person or describe the property to be seized):*
See Attachment "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*
18 U.S.C. §876 -	Mailing Threatening Communications
18 U.S.C. §924(c)	Use and Carry of a Firearm in Relation to a Crime of Violence

The application is based on these facts:
Please see attached.

- ☑ 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

JUSTIN STEELE - US Postal Inspector
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/1/19

Judge's signature

City and state: Las Vegas, Nevada

HONORABLE BRENDA N. WEKSLER
Printed name and title

000206

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

NICHOLAS A. TRUTANICH
United States Attorney
District of Nevada
Nevada Bar No. 13644
STEVEN W. MYHRE
Assistant United States Attorney
District of Nevada
Nevada Bar No. 9635
501 Las Vegas Blvd. South, Suite 1100
Las Vegas, Nevada 89101
Tel: 702.388.6336 / Fax: 702.388.6418
steven.myhre@usdoj.gov

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN THE MATTER OF THE SEARCH OF:	Case No.
9748 CANYON LANDING AVENUE	**UNDER SEAL**
LAS VEGAS, NEVADA 89166	

AFFIDAVIT OF JUSTIN STEELE IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Justin Steele, 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 premises located at 9748 Canyon Landing Avenue, Las Vegas, Nevada (hereinafter the "Place To Be Searched"), and to search for and seize the use, fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 875 (Transmitting a Threat in Interstate Commerce), 876 (Mailing Threatening Communications), and 924(c) (Use and Carry of Firearm in Relation to Crime of Violence) (hereinafter also referred to collectively as the "Subject Offenses").

2. I have been a United States Postal Inspector since 2015 and am currently assigned to the Phoenix Division of the United States Postal Inspection Service (hereinafter "USPIS"), External Crimes Team, located in Las Vegas, Nevada. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), authorized to conduct investigations into alleged violations of federal law. I hold a Bachelors' Degree in Chemistry and received federal law enforcement training from the USPIS. I have been trained to conduct, and have conducted, investigations into alleged federal crimes of mail fraud, mail theft, identity theft, credit card fraud, unlawful transportation of contraband, and the transmission of threatening communications. I have also received training and possess experience regarding the use of computers and other electronic devices to effect those crimes.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested Search Warrant and does not set forth all of my knowledge regarding the matters described herein.

4. On October 29, 2019, United States Magistrate Judge Daniel Albregts, duly authorized a Search Warrant for the Place to Be Searched, authorizing the search and seizure of the Items to Be Seized as delineated at Attachment B of the Warrant. The Search Warrant, Attachments, and supporting Affidavit are attached at Exhibit 1 and incorporated herein as though fully set forth herein. The Search Warrant has not been fully executed as of this date.

5. As set forth below, this is an Application to Supplement the Search Warrant to expand the list of Items to Be Seized to include any firearms and cellular telephone devices.

SUBJECT OFFENSES

6. The USPIS is conducting an investigation into the Subject Offenses, arising from a number of threatening communications believed to be mailed or transmitted by Latonia

Smith, the daughter of a former employee of the Planet Hollywood Hotel and Casino in Las Vegas, Nevada. As described more fully below, there is probable cause to believe that Ms. Smith became angered following the termination of her mother's employment at Planet Hollywood, causing her to send threatening communications to her mother's former supervisor in reprisal for the firing. Later, after related civil lawsuits were filed against Caesar's Entertainment – the parent company of Planet Hollywood – Ms. Smith is believed to have sent threatening communications to lawyers and employees representing Caesar's in those suits.

7. On October 31, 2019, Ms. Smith confronted one of the victims of the threatening communications with a firearm in Reno, Nevada. The victim was not hurt during the confrontation. Ms. Smith is believed to have returned to Las Vegas and is residing in the Place to Be Searched.

FACTS ESTABLISHING PROBABLE CAUSE

8. In addition to the facts set forth in the supporting affidavit of the original Search Warrant found at Exhibit 1 and incorporated herein, I submit the following.

9. In the evening of October 31, 2019, Attorney Wade Beavers, the recipient of the April 26, 2019, threatening communication, was in his apartment located at 750 Arrow Creek Parkway, Apartment 7103, Reno, Nevada. Sometime between 6 and 7 p.m., Mr. Beavers heard a knock at the door and, being Halloween, he answered the door believing the person to be a trick-or-treater. When he opened the door, he saw a person he knew to be Ms. Smith standing in the doorway, holding a firearm, which Mr. Beavers described as a matte black semi-automatic handgun.

10. Having seen Ms. Smith on previous occasions in connection with the civil employment litigation, he immediately recognized her. Ms. Smith entered the apartment and, while blocking the doorway, said to Mr. Beavers words to the effect of "we need to talk." Mr.

Beavers responded with words to effect of "don't do this!" and lunged for the handgun to wrest it away. During the ensuing struggle for the handgun, Ms. Smith moved away from the doorway, allowing an opportunity for Mr. Beavers to escape.

11. Mr. Beavers ran down the hallway of the apartment building knocking on doors until someone answered and let him, affording him the opportunity to call 911. By the time Reno police officers responded, Ms. Smith had left the property.

12. On November 1, 2019, Ms. Smith was located in Place to Be Searched, in Las Vegas, Nevada. She resides in that location with her mother.

13. I know from my training and experience that cell phones are used to navigate via GPS. I also know that cell phones register, or ping, on cellular towers when used to navigate, place calls, or even when in passive receive mode. Accordingly, any cell phone used to travel from Las Vegas to Reno, or Reno to Las Vegas, to commit the assault on Mr. Beavers is likely to contain evidence of location monitoring, navigation, or registration on cell phone towers and thus constitute evidence of the Subject Offenses.

PLACE TO BE SEARCHED

14. I further submit that there is probable cause to believe that evidence of the Subject Offenses is likely to be found at the Place To Be Searched as described below and in Attachment A to the Search Warrant, as follows:

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166:

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely

to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.

- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

15. The Place to Be Searched is the current residence of Latonia Smith as confirmed through independent sources, by driving by and visiting the residence, and by my interview of Ms. Smith. On the evening of November 1, 2019, Officers confirmed the presence of Ms. Smith at the residence.

ITEMS TO BE SEIZED

16. Based on the foregoing, I further submit there is probable cause to believe that located in the Place To Be Searched are the use, fruits, instrumentalities and evidence of violations of Title 18, United States Code, Sections 875, 876 and 924(c) ("Subject Offenses") as described below and in Attachment B to this Search Warrant.

Cellular telephone devices and any records associated with those devices.

Any firearms or ammunition.

SEALING

17. I further request that this Search Warrant, Supporting Application and Affidavit be sealed until further order of the Court. This is an ongoing investigation involving a crime of violence (communication threats of death or injury) and use of a firearm in relation to a crime of violence and the public disclosure of the information contained herein at this time may likely compromise the investigation to include: tipping off any perpetrators affording them time to destroy evidence or to abscond; identifying victims of the threats subjecting them to be re-victimization; and revealing the identity of person(s) suspected of committing criminal offenses and subjecting them to public scorn or humiliation before they have been formally charged and afforded due process of law.

CONCLUSION

18. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Items To Be Seized as forth in Attachment B, constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 875 and 876, and are likely to be found at the Place To Be Searched, as described at Attachment A.

Justin Steele
United States Postal Inspector

Subscribed and sworn to before me on this 15th day of November 2019.

BRENDA N. WEKSLER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PLACE TO BE SEARCHED

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

ATTACHMENT B

ITEMS TO BE SEIZED

I. **Statutes Violated.**

Potential violations of federal law include: Title 18, United States Code, Sections 875 (Transmission of Threat In Interstate Commerce), 876 (Mailing Threatening Communications), and 924(c) (Use of a Firearm in Relation to A Crime of Violence (also referred to as "Subject Offenses").

II. **Description of Items To Be Seized**

Cellular telephone devices, and any records associated with the use of those devices.

Any firearm or ammunition.

This list is intended to supplement the list of items to be seized as found in the Warrant authorized on October 29, 2019 for the search of the Place to Be Searched.

EXHIBIT "1"

EXHIBIT "1"

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

9748 CANYON LANDING AVENUE
LAS VEGAS, NEVADA 89166

Case No. 2:19-mj-818-DJA

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 _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

See Attachment "A".

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)*:

See Attachment "B".

YOU ARE COMMANDED to execute this warrant on or before 11/12/19 *(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.

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 HONORABLE DANIEL J. ALBREGTS
(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: 10/29/19 4:19 pm

DANIEL J. ALBREGTS
Judge's signature

City and state: Las Vegas, Nevada

HONORABLE DANIEL J. ALBREGTS
Printed name and title

000218

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

Return		
Case No.: 2:19-mj-	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

000219

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

ATTACHMENT A

PLACE TO BE SEARCHED

Residence located at 9748 Canyon Landing Ave., Las Vegas, NV, 89166

To include the physical structure and any storage areas, including all living areas, bedrooms, kitchen, bathroom areas, dedicated storage areas, any containers found therein that are likely to contain, hold or conceal any Items To Be Seized as described at Attachment B, and any building or structure appurtenant to the residence that are likely to contain, hold or conceal any Items To Be Seized.

The residence is further described as follows:

- 9748 Canyon Landing Ave. is a single family residence located in Whisper Peak gated community. It is located on the north side of Canyon Landing Ave. The house is labeled with 9748 in black letters on a white background. 9748 Canyon Landing Ave. is the third house to the east from Red Rock Crest.
- 9748 Canyon Landing Ave is a two-story light beige stucco building with light brown/tan colored tile roof. 9748 Canyon Landing Ave is south facing with a small gated courtyard before the front door. There are three windows on the front of the residence, one large double window above the two car attached garage, one small single window above and to the west of the front door, and a circular window with four metal bars across the window directly above the front door.

ATTACHMENT B

ITEMS TO BE SEIZED

I. **Statutes Violated.**

Potential violations of federal law include: Title 18, United States Code, Sections 875 (Transmission of Threat In Interstate Commerce) and 876 (Mailing Threatening Communications) (also referred to as "Subject Offenses").

II. **Description of Items To Be Seized.**

Evidence of indicia of occupancy for 9748 Canyon Landing Ave., Las Vegas, NV, 89166.

Evidence of violations of the Subject Offenses.

All documents relating to the creation or transmission of threats or threatening communications, including documents containing threatening communications.

Any materials used to create or transmit threats or threatening communications including but not limited to: electronic printers, templates, cardstock, artwork, laminate stock, laminators, and reflective paint.

Computers, peripherals, and all other electronic equipment used in connection with creating or transmitting threats or threatening communications, including but not limited to: computers, scanners, color printers, digital cameras, copy machines, internet access devices, and graphic design software.

Any electronic data storage devices used in connection with computers to create, store or transmit threats or threatening communications, including but not limited to: internal or external hard drives, removable hard drives, removable storage devices (e.g. thumb or flash drives), compact discs or other optical storage devices, and other memory storage devices.

The word "communication" is defined as any means of transmitting and storing information, including, without limitation, electronic signals commonly referred to as e-mail, text messages, instant messages, tweet, voice-mail, voice-messaging, private messages, video calling history, "Friend" requests, status updates; Instagram messages, electronic recordings,

or other electronic means of transmitting information, including all associated metadata if stored and/or recorded in an electronic medium.

The word "document" is defined as any information, communication or historical event recorded in any form or medium (paper or electronic), including, without limitation: activity logs, photographs, status updates, comments, "Friend" lists, "Friend" requests, "News Feed information," IP logs, "Neoprint," photographs, "likes," chat histories, gifts, pokes, tags, memoranda, letters, transmittals, notes, compilations, summaries, charts, receipts, invoices, bills, deposit slips, checks (front and back), forms, ledger entries, journal entries, diary entries, calendar entries, database entries, drawings and/or diagrams, and any and all associated metadata associated with information stored and/or recorded in an electronic medium.

This Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and separately sealed, as though set forth fully herein.

Attachment C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set

out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in the Attachments; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;

000227

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, Section II, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

This warrant expressly incorporates the Affidavit submitted in support of the warrant, and separately sealed, as though set forth fully herein.

Attachment C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set

out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in the Attachments; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

Entry @ 21:32 Exit @ 22:52

U.S. Postal Inspection Service

SEARCH WARRANT INVENTORY

Subject Name: Labrin Smith
Date (mm/dd/yyyy): 11/5/2019
Position/Box: ____/____
Subject Address: 1778 Canyon Landing Ave. Las Vegas, NV 8911
Floor/Room No.:
U.S. Postal Inspector(s): Sofia Slat, Daniel Carbonell, T. Isaac, Trevor Hudson, Jeff Ezell
Case No.: 2688317-DMI
Safe / Cabinet / Credenza / Desk / Drawer
Shelf / Table / Wall / Other

QUANTITY	DESCRIPTION OF ITEMS	
1	HP Office Pro 8710, S/N: CN31BH613C	DC
1	Apple Mac Mini, S/N: C07N2450DWYL	DC
1	Apple IPAD	TH
1	Portable Hard Disc, S/N: NL3QD946	TH
5	2 Sandisk Adapter, 3 Thumbdrives	DC
1	Mac Laptop, S/N: C02R54UGFWM	DC
1	Glock 17 Replica Air Gun	JE
1	Handwritten directions to Reno, NV	JE
1	Macbook Laptop, S/N: C02N18DPD63QQ	TH
1	Iphone belonging to Labrin Smith	RS
1	FedEx Receipts	JE
1	Iphone belonging to Anwar Peruzzi	RS
1	Samsung Cellphone found in Room B	DC
1	Iphone found in Room B	DC
1	Amazon Tablet found in Room B	DC

IS Form 8164, March 2009 Page ___ of ___ pages

000886

seen the pleadings, would have seen their names, gotten their identifying information from the pleadings to carry out the threats.

The wife of one of the attorneys, Jean Wirthlin, who you saw testify, was also connected to the defendant through her husband, who was directly involved in the litigation of the -- against the defendant. Because he sought the first temporary protective order.

Okay. So that's the receiver part of it. So moving to the crux of the case, we have to prove that it was the defendant who sent these communications. Because they were all sent anonymously. And we -- we have presented evidence that proves beyond a reasonable doubt that this defendant sent those communications and with the intent to instill fear and threaten injury.

So when considering the evidence of identity and intent here, you can consider everything I've just talked about. Talked -- the letters themselves, the language of the letters, the context of the communications, and the interactions between the defendant and these five victims.

But also look at her phone, the notes and e-mails on the phone, and the links between those notes and e-mails, and the threats themselves. And when we add this evidence into this, the connections, the weaving fabric of guilt become very clear and very strong.

You remember the testimony of -- of Mr. Gonzalez, who talked about the phone and how he extracted data from it. And one of the things he talked about was he looks for identifying data on the phone. As you recall, Agent -- or excuse me -- Inspector Steele testified this phone was recovered during a search, a court-authorized search, of the residence of the defendant. The phone was recovered, analyzed by the laboratory in Atlanta for the United States Postal Inspection Service. The phone had a password. The program that the forensic examiners use was able to break through that password after about a month working that process.

Mr. Gonzalez testified that when looking at the data on the phone, it identified the pass code that was recovered, which was 4991, which everyone has established is the birth year of the defendant in reverse; the user name of Toni Smith; the owner name of Latonia's iPhone; and Apple ID of lds11a@acu.edu. LDS being the initial of the defendants.

And it's her phone. So what's on her phone? In looking at Exhibit 93, this is the e-mail that was discovered on the phone from the defendant to Advanced Psychiatry.

Before I go into that, I just want to mention something as well. Over the course of the next couple of slides, and as you've heard and seen during the course of this trial, evidence came in and is in that is disturbing. It contains information that many people would consider of a private nature. We also