IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,	)	FINAL BRIEF ON BEHALF OF
	)	APPELLANT
Appellee	)	
v.	)	
	)	
Specialist (E-4)	)	Crim. App. Dkt. No. 20150386
LUIS G. NIETO,	)	
United States Army,	)	USCA Dkt. No. 16-0301/AR
Appellant	)	

JOSHUA G. GRUBAUGH
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703)693-0682
USCAAF Bar No. 36576

HEATHER L. TREGLE
Captain, Judge Advocate
Branch Chief,
Defense Appellate Division
USCAAF Bar No. 36329

CHARLES D. LOZANO
Lieutenant Colonel, Judge Advocate
Deputy Chief,
Defense Appellate Division
USCAAF Bar No. 36344

INDEX

Table of Cases, Statutes, and Other Authorities

Supreme Court

Court of Appeals for the Armed Forces

Federal Circuit Courts of Appeals

Federal District Court Cases

Uniform Code of Military Justice

Other Statutes, Materials, and Regulations

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,	)	FINAL BRIEF ON BEHALF OF
	)	APPELLANT
Appellee	)	
v.	)	
	)	
Specialist (E-4)	)	Crim. App. Dkt. No. 20150386
LUIS G. NIETO,	)	
United States Army,	)	USCA Dkt. No. 16-0301/AR
Appellant	)	

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES:

Issue Presented

WHETHER THE MILITARY JUDGE ERRED IN DENYING APPELLANT'S MOTION TO SUPPRESS THE EVIDENCE SEIZED FROM APPELLANT'S LAPTOP COMPUTER.

Statement of Statutory Jurisdiction

The Army Court of Criminal Appeals (Army Court) had jurisdiction over this matter pursuant to Article 66, Uniform Code of Military Justice, 10 U.S.C. § 866 (2012) [hereinafter UCMJ]. This Honorable Court has jurisdiction over this matter under Article 67(a)(3), UCMJ, 10 U.S.C. § 867(a)(3) (2012).

Statement of the Case

On April 23, May 21, and June 3, 2015, Specialist (SPC) Luis G. Nieto, was tried at Fort Bliss, Texas, before a military judge sitting as a general court-martial. Pursuant to his plea, SPC Nieto was convicted of abusive sexual contact (four

specifications), absence without leave, violating a general order, false official statement, and indecent visual recording, in violation of Articles 120, 86, 92, 107, and 120c, UCMJ, 10 U.S.C. §§ 920, 886, 892, 907, and 920c (2012). The military judge sentenced SPC Nieto to reduction to E-1, total forfeitures of pay and allowances, confinement for five years, and a bad-conduct discharge. The convening authority approved only so much of the sentence as provided for reduction to E-1, total forfeitures, confinement for four years, and a bad-conduct discharge, and approved 142 days of confinement credit against the sentence to confinement.

On December 31, 2015, the Army Court affirmed the findings and sentence, however they modified the promulgating order to reflect the military judge's finding of an unreasonable multiplication of charges, and renumbered the specifications of Charge I. (JA 1). Specialist Nieto was notified of the Army's Court decision and petitioned this court for review on January 28, 2016. On March 21, 2016, this Honorable Court granted SPC Nieto's petition for review.

Statement of Facts

On May 18, 2013, Special Agent (SA) John Foshee of the 48th Military Police Detachment, Criminal Investigation Command (CID), interviewed Corporal (CPL) Robert Ochiltree. Corporal Ochiltree informed SA Foshee that at Forward Operating Base (FOB) Azi Zullah, Afghanistan, SPC Nieto pointed a cellphone

over the latrine stall door while other Soldiers were using the latrine. (JA 123-134). On May 20, 2013, SA Scott Sandefur signed an affidavit requesting seizure authorization from a military magistrate for SPC Nieto's cellphone and laptop computer. (JA 119-120.).

Special Agent Sandefur testified he could not remember how CID learned SPC Nieto owned a laptop. (JA 24-25). Nothing within the affidavit mentioned SPC Nieto used his laptop in the commission of the offenses, or that he had transferred evidence from his cellphone to his laptop. (JA 119-120). Special Agent Sandefur testified he spoke to the magistrate about a generic Soldier profile—that Soldiers typically download digital files from their cellphones to their laptops, and this formed the nexus between SPC Nieto's cellphone and his laptop. (JA 29). However, SA Sandefur could not recall a case he investigated before May 20, 2013, where he had seen the transfer of digital evidence from a cellphone to a laptop. (JA 26-27). Special Agent Sandefur's profile was based on his personal experiences. (JA 17 and 30). The military magistrate granted SA Sandefur's request to seize SPC Nieto's phone and laptop. (JA 122).

The digital forensic examiner informed SA Bryce Dunn he could not analyze SPC Nieto's cellphone without a search authorization. (JA 33). On June 17, 2013, SA Dunn requested authorization to search SPC Nieto's phone and laptop. (JA 127-128). The affidavit SA Dunn presented to the military magistrate was the

same as SA Sandefur's, except for two additions. Special Agent Dunn averred that SPC Nieto confessed to using his phone to view and record Soldiers in the latrine. He also noted those who record sex acts typically transfer digital data from a portable device to one with a larger storage capacity, such as a computer. (JA 127-128).

Special Agent Dunn's experience as a CID agent informed his belief that data is typically transferred from a portable device to one with a larger storage capacity. (JA 127-128). However, SA Dunn could not remember a case he worked before July 17, 2013, where he had seen such a data transfer. (JA 44-45). There was no equipment found in SPC Nieto's room that provided for the transfer of data from a cellphone to a laptop. (JA 43-44). Further, no evidence was presented to the magistrate that SPC Nieto was recording sex acts, meaning SPC Nieto did not fit the profile SA Dunn presented. (JA 119-125).

The only evidence presented to the magistrate concerning the number of Soldiers recorded by SPC Nieto was SA Dunn's affidavit and CPL Ochiltree's statement. (JA 38-41). Special Agent Dunn did not testify to any oral statements made to the magistrate, and the magistrate did not consider additional evidence before granting the authorization to search SPC Nieto's laptop. (JA 31-47). The magistrate did not have any additional information beyond CPL Ochiltree's statement and the July 17, 2013 affidavit with which to make his probable cause

determination. The July 17th affidavit and CPL Ochiltree's statement only specify that SPC Nieto recorded two Soldiers in the latrine.[1] (JA 127-131).

Specialist Nieto objected to the search and seizure of his laptop computer, claiming the military magistrates did not have a substantial basis to find probable cause. (JA 110-117). On May 21, 2015, the military judge ruled the military magistrates had a substantial basis to determine "the existence of probable cause as to images being found on [SPC Nieto's] laptop computer." (JA 162-165). The military judge's findings of fact relied upon SA Sandefur's affidavit and oral statements, SA Dunn's affidavit, and CPL Ochiltree's sworn statement when approving of the magistrates' authorizations to search and seize SPC Nieto's laptop. (JA 162-165). The military judge ruled evidence derived from SPC Nieto's laptop was admissible. Specialist Nieto entered into a conditional guilty plea with the government, preserving his right to challenge the military judge's ruling regarding the exclusion of evidence collected from SPC Nieto's laptop computer. (JA 166-168).

Summary of Argument

The military judge erred when he concluded there was a substantial basis to find probable cause to search and seize SPC Nieto's laptop computer. While there was

[1] While the record of trial (ROT) suggests SPC Nieto recorded many more Soldiers, nothing in the ROT indicates this evidence was presented to the military magistrates.

probable cause for SPC Nieto's cellphone, the government failed to adequately connect SPC Nieto's cellphone to his laptop computer. *United States v. Clayton*, 68 M.J. 419 (C.A.A.F. 2010), articulates the limits of when law enforcement can reasonably infer evidence of a crime was transferred from one location to another location. Here, the investigators' inferential leap bridged too large a chasm, going well beyond *Clayton*.

The hypothetical nexus connecting SPC Nieto's cellphone to his laptop was especially weak. Investigators could not state how they learned SPC Nieto owned a laptop. (JA 24-25). They also provided the magistrates with a generic profile of data transfer applicable to all Soldiers. This profile evidence was the only nexus connecting SPC Nieto's cellphone to his laptop. To uphold the military judge's ruling would permit the government to search multiple electronic devices anytime someone used a cellphone in the commission of a crime. The investigators' actions and the military judge's ruling deprived SPC Nieto of his protections under the Fourth Amendment and the Military Rules of Evidence (Mil. R. Evid.) 311-317.

Argument

WHETHER THE MILITARY JUDGE ERRED IN DENYING APPELLANT'S MOTION TO SUPPRESS THE EVIDENCE SEIZED FROM APPELLANT'S LAPTOP COMPUTER.

Standard of Review

This Court reviews a military judge's denial of a motion to suppress for an abuse of discretion, viewing the evidence in the light most favorable to the party prevailing below. *United States v. Keefauver*, 74 M.J. 230, 233 (C.A.A.F. 2015). An abuse of discretion occurs when the military judge's findings of fact are clearly erroneous or he misapprehended the law. *United States v. Leedy*, 65 M.J. 208, 213 (C.A.A.F. 2007). The military judge misapprehends the law if there was not a substantial basis for the magistrate to find probable cause. *United States v. Huntzinger*, 69 M.J. 1, 5 (C.A.A.F. 2010) (citing *Leedy*, 65 M.J. at 212). Whether there was a sufficient basis to find probable cause is a legal question reviewed de novo, using a totality of the circumstances test. *Huntzinger*, 69 M.J. at 5 (citing *Leedy*, 65 M.J. at 212).

Law and Argument

By finding a substantial basis to determine the existence of probable cause, the military judge discarded any requirement of an actual nexus between the evidence sought and the location to be searched. While he cited *Clayton*, the military judge's ruling goes far beyond this Court's decision in that case.

There was no evidence connecting SPC Nieto's crimes to his laptop computer. The investigators inferred SPC Nieto was likely to have transferred data from his cellphone based on "the history of what Soldiers do with their cellphones." (JA

17). With this logic, use of a cellphone in the commission of a crime equates to probable cause to seize all electronic devices found in a dwelling. Further, CID did not establish any relevant facts that would trigger this inference. The investigators did not communicate to the magistrates whether SPC Nieto had large amounts of digital data on his cellphone, the storage capacity of SPC Nieto's cellphone, nor did they uncover whether SPC Nieto possessed equipment which would make data transfer possible.

1. There was no probable cause to seize SPC Nieto's laptop computer on May 20, 2013.

The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. Absent probable cause, the government's seizure of SPC Nieto's laptop computer was unlawful. Mil. R. Evid. 315(f) and 316. Probable cause relies on a "common-sense decision whether, given all the circumstances . . . there is a fair probability that contraband" will be found. *Leedy*, 65 M.J. at 213 (quote marks omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 236).

> The threshold for probable cause is subject to evolving case-law adjustments, but at its core it requires factual demonstration or reason to believe that a crime has or will be committed. As the term implies, probable cause deals with probabilities. It is not a "technical" standard, but rather is based on "factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Probable cause requires more than bare suspicion, but something less than a preponderance

> of the evidence. . . . The duty of the reviewing court is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.

Leedy, 65 M.J. at 213 (final ellipsis in original) (citations omitted).

The authorization to seize SPC Nieto's laptop lacked probable cause and relied on bare suspicion. There was no connection from the latrine where SPC Nieto used his cellphone to his laptop computer. *See United States v. Hicks*, 2012 U.S. Dist. LEXIS 137189 (W.D. Ky. Sept. 24, 2012) (holding no probable cause to conclude suspect transferred digital data from his phone to computer).

"Probable cause to search exists when there is a reasonable belief that the . . . evidence sought is located in the place . . . to be searched." Mil. R. Evid. 315(f)(2). It has been recognized that "[i]f there is probable cause to believe that someone committed a crime, then the likelihood that that person's residence contains evidence of the crime increases." *United States v. Jones*, 994 F.2d 1051, 1055-56 (3d Cir. 1993). However, "[t]he critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). While direct observation can establish probable cause, it can also be established through an inference of a nexus. *United States v. Potts*, 586 F.3d

823, 831 (10th Cir. 2009) ("[D]irect evidence that contraband is in the place to be searched is not required."); *see also United States v. Alexander*, 835 F.2d 1406, 1409 (11th Cir. 1988) (inferring that tools of a robbery were located in an automobile), *noted in United States v. Lopez*, 35 M.J. 35, 39 (C.M.A. 1992) (inferring the location of stolen items).

While probable cause can be established through inference, the definition of probable cause nonetheless "contemplates *some* nexus between the contraband or evidence sought and the place the government wants to search." *Clayton* 68 M.J. at 426 (Ryan, J., dissenting) (emphasis added). The only nexus between SPC Nieto's cellphone and laptop that the magistrate knew of on May 20, 2013, was a generic profile that Soldiers typically transfer digital media from their cellphones.

Special Agent Sandefur testified he orally communicated to the magistrate the likelihood Soldiers would save digital media from their cellphone to their laptop computer. (JA 17). Special Agent Sandefur testified Soldiers' send deployment photographs back to home or family, or post them to the Internet, after transferring the files from their cellphone to computer. (JA 17). This profile was based on SA Sandefur's personal experience in sharing deployment photos with his loved ones at home. (JA 30). However, this profile was not on the face of the May 20, 2013, affidavit. *See Leedy*, 65 M.J. at 214 (stating this Court's analysis focuses on "the evidence as set out in the four corners of the requesting affidavit . . . illuminated by

factors such as the veracity, reliability, and basis of knowledge of the individual presenting the evidence") (citations and quotation marks omitted).

There are many problems with applying SA Sandefur's generic Soldier profile to SPC Nieto. First, SA Sandefur could not name any case he worked on before May 20, 2013, where he saw the transfer of digital files containing evidence of a crime from a cellphone to a laptop. (JA 26-27). The generic Soldier profile SA Sandefur used was based entirely on his personal experiences, and not those of an experienced investigator. This Court has given deference to law enforcement experiences when establishing a nexus through profile evidence, but has yet to expand this to personal experiences. *See United States v. Gallo,* 55 M.J. 418, 422 (C.A.A.F. 2001) ("As to the nexus requirement, the affidavit by the agent, who had *26 years' experience in law enforcement*, set forth his opinion as to how pornographic material is obtained and stored. … A judicial officer may give considerable weight to the conclusion of *experienced law enforcement officers* regarding where evidence of a crime is likely to be found.") (citing *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987) (internal citations omitted) (emphasis added).

Second, no evidence demonstrated SPC Nieto had the same motivations SA Sandefur cited in his generic profile. It makes little sense that SPC Nieto would share evidence of a crime in the same way most Soldiers share deployment photos

with their friends and family. Crimes are ordinarily secreted away, and to treat SPC Nieto the same as a young Soldier proud of his deployment experiences is to ignore common sense. Probable cause determinations may be based on reasonable inferences. *See Gates*, 462 U.S. at 240. There is no authority permitting probable cause determinations to be based on *all* possible inferences.

Third, SA Sandefur's profile of how Soldiers use their cellphones is based on an outdated premise that cellphones are incapable of emailing photographs or posting digital media to the Internet directly. Specialist Nieto owned a smartphone, thus the inference that he likely used a laptop to store or share the media is faulty. (JA 123-124 and 138).

Other than the nexus created by SA Sandefur's generic Soldier profile, the government presented no evidence of a connection between SPC Nieto's cellphone and his laptop computer. Special Agent Sandefur informed the military magistrate that SPC Nieto pointed his cellphone at two Soldiers while they used the latrine. The May 20, 2013, affidavit contained only four paragraphs, as well as CPL Ochiltree's sworn statement. Nothing in those two documents mentioned SPC Nieto's laptop, nor do they add anything beyond identifying the two Soldiers who observed SPC Nieto pointing his cellphone while they used the latrine.

By finding a substantial basis in probable cause, the military judge interpreted *Clayton* to mean that because digital evidence is transferrable, the government can

search devices in SPC Nieto's room for evidence of a crime, even though there was no connection between SPC Nieto's cellphone and his room. The military judge stated, "It is a normal inference to be drawn—as was done in *US v. Clayton*—that data is transferred from one digital device to another." (JA 164). This ruling over-simplified *Clayton*, and ignored what distinguished *Clayton* from SPC Nieto's case.

Investigators knew Lieutenant Colonel (LTC) Clayton belonged to a group posting child pornography on the Internet. *Clayton,* 68 M.J. at 422. Two other group members had been arrested and confessed to possessing child pornography. *Id.* Lieutenant Colonel Clayton requested subscription privileges from the group, and the group sent him up to twenty-five postings a day. *Id.* The email LTC Clayton registered with the group was traced to an Internet protocol address in Kuwait, where investigators found LTC Clayton accessed his email from his government laptop. *Id.* Lieutenant Colonel Clayton also had internet access in his room. *Id.* at 423.

The inferential nexus in *Clayton* was from a membership in a child pornography group sending messages on the Internet to a laptop computer kept in LTC Clayton's bunk. *Id.* at 424. That someone would access their email address, and hence the illicit communications, from a laptop computer was a reasonable conclusion. *Clayton* also found the portability of laptops and the ease with which

computer media is replicated on other devices supported the inference that LTC Clayton had child pornography on his personal laptop. *Id.* at 424-425.

Specialist Nieto's case does not have the same factual predicates. There was no evidence SPC Nieto used the laptop in the latrine. Special Agent Dunn was not even sure how he knew SPC Nieto owned a laptop, and the investigators failed to uncover devices that may transfer data from a cellphone to a laptop. Unlike LTC Clayton, SPC Nieto did not have evidence of a crime on the Internet he could have used multiple devices to access. Further, the magistrate only knew SPC Nieto likely used his cellphone to record images of two Soldiers, which is a small amount of data not requiring transfer to another device.

The only evidence supporting the authorization to seize SPC Nieto's laptop were the inferences that: 1) data is transferred to devices which can store more data; and 2) Soldiers typically transfer data from cellphones to laptops. Neither one of these theories is sufficient to justify the search or seizure of electronic devices from the dwelling of a U.S. citizen, unless this Court would explicitly hold Fourth Amendment protections for digital media are de minims.

Many jurists have commented on the apparent weakening of the Fourth Amendment in the digital age, especially in the context of child pornography cases. *See United States v. Gourde*, 440 F.3d 1065, 1074 (9th Cir. 2006) (Reinhardy, J., dissenting, "[I]t is important that courts not grow lax in their duty to protect our

right to privacy and that they remain vigilant against efforts to weaken our Fourth Amendment protections."); *United States v. Coreas*, 419 F.3d 151, 158 (2d Cir. 2005) ("Such a rule … not only violates the First Amendment protection against guilt by association but also makes a mockery of the Fourth Amendment's focus on particularity and on protection of the privacy of the individual to be searched."); and *Clayton* (Ryan, J., dissenting, "I cannot agree with the continued dilution of the requirement that there be an actual, as opposed to an intuitive or a hypothetical, nexus between the evidence sought and the location to be searched."). This court cannot allow the concept of probable cause to be further diluted by affirming the military judge here.

To allow the military judge's reasoning to stand means anytime law enforcement suspects a digital device has been used in a crime, every device capable of storing digital evidence could be seized from a home. This would cause unreasonable intrusions into the home the Fourth Amendment was designed to protect. *Payton v. New York*, 445 U.S. 573, 585 (1980) ("The physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.") (internal quotations omitted); *Lauro v. Charles*, 219 F.3d 202, 211 (2d

Cir. 2000) (describing "particular gravity the Fourth Amendment accords to government intrusions" on privacy of the home).[2]

The military judge's finding of a substantial basis in probable cause interpreted *Clayton* to mean digital evidence is transferrable, so the government can search SPC Nieto's bunk for any device capable of storing that digital evidence. There is no limiting principle to the logic of the trial court's ruling. Specialist Nieto only had a laptop computer, but what if he had more? The growing list of devices capable of storing digital data includes: an external hard drive, a USB flash drive, DVDs, computer disks, video game consoles, e-book readers, computers, other cellphones, etc. Extrapolating on the military judge's ruling equates to all data storage devices could be seized and searched under the theory, "digital data is fungible."

By analogy, this Court would not allow a similar dilution of the Fourth Amendment to authorize the seizure of drugs in a dwelling for a suspect selling drugs on the street when: 1) investigators could not say how they knew the suspect

---

[2] While SPC Nieto may not have had the same privacy interests while deployed as a citizen does in their own home, he did have a reasonable expectation of privacy on the computer located on his bunk. Military Rules of Evidence 311-317 apply in a deployed environment. *See United States v. Huntzinger,* 69 M.J. 1 (C.A.A.F. 2010). The military judge ruled there was a substantial basis to find probable cause in searching SPC Nieto's laptop. His reasoning did not identify lesser protections to SPC Nieto's laptop computer due to the deployment, meaning the fungible aspect to data drove the ruling, not SPC Nieto's deployment.

owned a house, 2) they never saw him use his house for any purpose, 3) investigators only know "people tend to put stuff in their houses," and 4) the basis for that inference is from personal experience seeing other people put stuff in their houses. *See Keefauver*, 74 M.J. 230 (holding package addressed to home containing marijuana did not create basis to search entire home for evidence of drugs). Thus, there was no basis to determine probable cause existed to seize SPC Nieto's laptop computer, and the evidence derived from the laptop should have been suppressed. Mil. R. Evid. 311.

2. Inevitable discovery and the search authorization of July 17, 2013, do not save the government's illegality on May 20, 2013.

"The doctrine of inevitable discovery creates an exception to the exclusionary rule allowing admission of evidence that, although obtained improperly, would have been obtained by another lawful means." *United States v. Wallace*, 66 M.J. 5, 10 (C.A.A.F. 2008) (citing *Nix v. Williams*, 467 U.S. 431, 444 (1984). Here, the doctrine of inevitable discovery does not apply because there is no other lawful means through which the government could have obtained the evidence from SPC Nieto's laptop computer.

There was no probable cause to seize SPC Nieto's computer on May 20, 2013. Yet the government held onto SPC Nieto's laptop for two months while it attempted to bolster the basis in probable cause to search the laptop with its affidavit from July 17, 2013. However, "[f]reezing the scene to procure a

command authorization requires probable cause or exigent circumstances." *United States v. Hoffmann*, 75 M.J. 120, 125 (C.A.A.F. 2016) (citing *Segura v. United States*, 468 U.S. 796, 810 (1984) (plurality opinion)). By seizing the laptop for two months before searching it, the government essentially froze the scene. But there was no probable cause to seize SPC Nieto's laptop on May 20, 2013, and the record does not contain any exigent circumstances, thus violating *Hoffmann's* rule on when the government may freeze the scene. *Id.*

In *Hoffmann,* the government attempted to cleanse their illegal seizure through a neutral and detached magistrate's issuance of a search authorization several months after the seizure. *Id.* This Court found that the search affidavit must have been, "supported by probable cause known to the investigators *at the time of the seizure* and otherwise valid." *Id.* (emphasis added). But since there was no probable cause at the time of the seizure nor any exigent circumstances, the inevitable discovery doctrine failed to cleanse the illegal seizure. *Id.* at 127.

The circumstances in SPC Nieto's case are exactly the same as *Hoffmann.* The government illegally seized SPC Nieto's laptop computer, even though there was no probable cause or exigent circumstances justifying the seizure. Several months after the illegal seizure, the government procured a search authorization. When evaluating the legality of that later search, this Court must do so through what was known to the investigators at the time of the seizure. At the time of the seizure on

May 20, 2013, there was only a bare bones affidavit and SA Dunn's generic Soldier profile. Therefore, the inevitable discovery doctrine fails to save the government from their illegality.

3. The military good-faith exception does not save the defective authorizations because the magistrates did not have a substantial basis for determining the existence of probable cause.

The Supreme Court held that the exclusionary rule barring illegally obtained evidence from the courtroom does not apply to evidence seized "in objectively reasonable reliance on" a warrant issued by a detached and neutral magistrate judge, even where the warrant is subsequently deemed invalid. *United States v. Leon,* 468 U.S. 897, 922 (1984). This has become known as the good-faith exception to the exclusionary rule.

The President promulgated the following military good-faith exception rule:

> Evidence that was obtained as a result of an unlawful search or seizure may be used if:
>
> (A) The search or seizure resulted from an authorization to search, seize or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by competent civilian authority;
>
> (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
>
> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the

> issuance of the authorization or warrant. Good faith shall be determined on an objective standard.

Mil. R. Evid. 311(c)(3).

As the Court recently found in *Hoffmann*, 75 M.J. at 127-128, if the magistrate did not have a substantial basis for determining the existence of probable cause, then the military good-faith exception rule will not apply. Because the magistrate did not have any basis for finding probable cause, the good-faith exception cannot save the defective authorization.

Conclusion

Wherefore, SPC Nieto requests this Honorable Court set aside the findings of guilty and sentence.

JOSHUA G. GRUBAUGH
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703)693-0682
USCAAF Bar No. 36576

HEATHER L. TREGLE
Captain, Judge Advocate
Branch Chief,
Defense Appellate Division
USCAAF Bar No. 36329

CHARLES D. LOZANO
Lieutenant Colonel, Judge Advocate
Deputy Chief,
Defense Appellate Division
USCAAF Bar No. 36344

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing in the case of *United States v. Nieto,* Army Dkt. No. 20150386, USCA Dkt. No. 16-0301/AR, was electronically filed with the Court and Government Appellate Division on April 19, 2016.

MICHELLE L. WASHINGTON
Paralegal Specialist
Defense Appellate Division
(703) 693-0737