IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee v. James Richards, IV Lieutenant Colonel (O-5), United States Air Force, Appellant	)))))))))	REPLY ON BEHALF OF APPELLANT Crim. App. Dkt. No. 38346 USCAAF Dkt. No. 16-0727/AF

BRIEF ON BEHALF OF APPELLANT

INDEX OF BRIEF

TABLE OF CASES, STATUTES, AND OTHER AUTHORITIES

Supreme Court of the United States

Court of Appeals for the Armed Forces

Other Courts

Other Authorities

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee	)	
v.	)	REPLY ON BEHALF OF APPELLANT
James Richards, IV Lieutenant Colonel (O-5), United States Air Force, Appellant	)	Crim. App. Dkt. No. 38346 USCAAF Dkt. No. 16-0727/AF

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

Pursuant to Rule 19 of this Court's Rules of Practice and Procedure, Appellant hereby Replies to the United States' Answer, filed on 16 February 2017.

Argument

At the outset, Appellant acknowledges that he was mistaken in stating that the image found in the unallocated space that prompted SA Nishioka to stop searching to seek an additional search warrant was among the files later found the Toshiba and Gateway hard drives. But, as discussed in more detail below, the analysis is not changed because pictures will often contain internal data (including the date the picture was taken), that law enforcement certainly had the capability of determining whether the file had catalogue information or metadata associated with it, and if the file had metadata associated with it indicating that the file fell outside of the date range, it should not have been opened.

A. The 9 November 2011 search authorization was overbroad.

The government argues that the 9 November search authorization was not overbroad because "for all practical purposes, it already contained an implicit date limitation." Answer at 15. The government argues that the agents were "restricted to looking for online communications that showed Appellant violating Florida law," and that the agents were "restricted to searching for communications that took place between mid-2010 and 9 November 2011." Answer at 16. As discussed more fully below, if what the government says is true and the search authorization imposed a temporal limitation, then the agents exceeded the scope of the authorization by failing to limit the scope of their search to the terms of the search authorization. The government also argues that the reference to the Florida statute in the 9 November search authorization "fulfilled the same function as a date limitation would have done," and would have only permitted AFOSI to search for evidence of crimes with a nexus to Florida, "which naturally limited the time frame of events occurring after Appellant moved there in mid-2010." Again, if this is true, then the agents exceeded the scope.

But there is another problem with the government's argument. Although the search authorization itself lists the Florida statute Appellant was suspected of having violated, and discusses the development of the relationship between Appellant and AP, it says nothing about Appellant "mov[ing to Florida] in mid-

2010." This information can only be found by looking outside the terms of the search authorization and its accompanying affidavit. While that may seem like a minor detail, it does not appear to be information that the magistrate had at the time he issued the search authorization. JA at 270-272. Nor is it information that was available to DCFL when they were requested to conduct the forensic examination of the electronic media. JA at 367-373. If the failure to incorporate an affidavit into a search authorization invalidates the search authorization[1], then information *not contained* within an incorporated affidavit cannot save an otherwise invalid search authorization. By arguing the existence of facts that are not found within the search authorization itself, not found within the accompanying affidavit, and not found within the request for DCFL examination of the media, the government perpetuates the issue in this case, which is that the Fourth Amendment's particularity requirement cannot be satisfied by references to information outside of the search authorization and incorporated affidavit.

The government argues that the search authorization in this case limited the search of evidence of specific crimes or specific types of material by restricting the agents to search for online communications that violated Florida law, and that SA Nishioka "understood the limited nature of the search authorization" because "upon finding child pornography, he suspended his original search and obtained

[1] *See Groh v. Ramirez*, 540 U.S. 551 (2004).

another search authorization." Answer at 16-17. While it may be that SA Nishioka understood that the search authorization did not cover child pornography, it is clear that SA Nishioka did not understand (or perhaps did not care) that his search was limited by date range, as the government now argues that it was. Indeed, if SA Nishioka understood that the search authorization was limited by date range, he would have only looked at files falling within that date range. Similarly, if the forensic analysts at DCFL understood that the search was limited by date range, they would have provided to SA Nishioka only those files falling within that date range.

The government next argues that the granted issue "raises the question of whether a search authorization should restrict law enforcement agents to using a certain search methodology to ensure they only view evidence within a certain date range for which there is probable cause." Answer at 18. The government cites *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009) for the proposition that it is "folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives." But while the Tenth Circuit declined to require law enforcement to employ any particular search methodology, it went on, "that is not to say methodology is irrelevant," and noted that "the search method must be tailored to meet allowed ends." *Burgess*, 576 F.3d at 1094.

Appellant has not suggested that this Court require any search authorization to restrict law enforcement to any specific search methodology other than a method that meets the particularity requirement. Nor has Appellant suggested that law enforcement be limited to "search only certain files/documents on a computer with a certain name or term, or located in a certain area of the computer hard drive." Answer at 19 (*quoting United States v. Graziano*, 558 F.Supp.2d 304, 315 (E.D.N.Y. 2008)). Appellant has not suggested that the search should be restricted "by directory, filename or extension" or "to an email program or specific search terms." Answer at 20, (*quoting Burgess*, at 1093 and *United States v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006)). But it is clear from the record in this case, particularly Mr. Kleeh's testimony, that the DCFL has the ability to determine when a file was created (R. at 547); cached (R. at 520); backed-up (R. at 538); saved (R. at 547); viewed (R. at 537); moved (R. at 519); accessed (R. at 520); deleted (R. at 519); or otherwise manipulated (R. at 583). It is therefore not unreasonable to limit law enforcement to searching for computer files falling within a date range, because they clearly have the capability to do it.

Quoting *United States v. Richards*, 659 F.3d 527, 540 (6th Cir. 2011), the government argues, "so long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in

order to determine whether they contain such evidence." Respectfully, this does not really answer the question. If an examination of the metadata reveals that the file does not fall within the date range, there is simply no reason for the executing officer to open the file. The government also cites a footnote in *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) for the proposition that "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." In making that statement, however, the Supreme Court "recognize[d] that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable," and "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen*, 427 U.S. at 482 n. 11.

The government cites *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) for the proposition that "[a]lthough there were presumably communications on the computers that did not relate to the offenses, a search does not become invalid merely because some items not covered by the warrant are seized." But the issue in *Guest v. Leis* was whether the *seizures* of the *computers themselves* was lawful. The Sixth Circuit concluded,

> In the instant cases, when the seizures occurred, defendants were unable to separate relevant files from unrelated files, so they took the computers to be able to sort out the documents off-site. Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files.

Thus, *Guest v. Leis* does not stand for the broad proposition that all files on a computer can be opened if law enforcement obtains a warrant for the computer.

The government again cites *Burgess*, at 1094, for the proposition, "in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files." Answer at 21. But the Court in *Burgess* went on to say that it had "not abandoned the concerns expressed in *Carey*," in which it had previously held that "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant." *Burgess*, at 1094, citing *United States v. Carey*, 172 F.3d 1268, 1775 (10th Cir. 1999). Just as in *Carey*, law enforcement officers in this case should have taken the "intermediate step" of sorting the documents by date and only searching the ones for which there was probable cause as described in the search authorization.

In a footnote, the government cites *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010), stating, "The Fourth Circuit has gone so far as to assert that

due to the likelihood of mislableled or concealed files, 'a computer search must, by implication, authorize at least a cursory review of each file on the computer.'" Answer at 21, n.9. First of all, application of the "plain view" doctrine in the context of computer searches done pursuant to a warrant, as was done in *United States v. Williams*, effectively converts an otherwise valid search pursuant to a warrant[2] into a general search in violation of the Fourth Amendment. In *Williams* the Fourth Circuit concluded, "Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied." *Williams*, 523 F.3d at 522. The Fourth Circuit in *Williams* began with a faulty premise – a computer search *does not* authorize a cursory review of every file on the computer. Taken to its logical conclusion, *Williams* means that once there is probable cause to believe that there is evidence of a crime on a computer, the entire contents of the computer are in plain view so long as law enforcement obtains a warrant. Appellant's research reveals no military case, and no Federal Circuit Court of Appeals case, that reads the Fourth Amendment so broadly as to permit such an intrusion into a person's privacy.

Law enforcement in this case had the ability to segregate the files and only open the files that fell within the date range for which there was probable cause. It

[2] Appellant does not concede that the search in this case was valid.

could have done that without requiring any specific "search methodology" to be spelled out in the warrant. It did not segregate the files by date because the search authorization did not require the government to search only for files related to criminal activity within the date range. In this regard, the search authorization was overbroad.

The government next argues that search authorizations should not be required to include date limitations, and cites two Federal District Court cases for that proposition. In the first, *United States v. Loera*, 59 F.Supp.3d 1089, 1153 (D. N.M. 20 October 2014), it was relevant to the trial court that the case "concerned electronic mail hijacking and computer fraud – crimes that inherently involve using technology to deceive others[.]" That concern is not present in this case. The District Court also noted that the Tenth Circuit had not directly addressed the issue (*Id.*), although Appellant's research reveals that it had. In *United States v. Leary*, 846 F.2d 592, 604-605 (10th Cir. 1988), the Court found error due to a failure to include a "specific period of time coincident to the suspect transaction" among the information "available to the government to make the description of the items to be seized much more particular." The second case cited by the government, *United States v. Will*, 2015 U.S. Dist. LEXIS 79887 at *21 (N.D. W.VA. 19 July 2015), relies on *Williams*, discussed *supra*, for its holding that "the three requirements for the plain view exception are met." Appellant respectfully submits that this Court

should not be persuaded by the decisions of trial-level courts decided on different sets of facts and which, in the case of *Leora*, may not adhere to the conclusions of its own superior Court of Appeals; and in the case of *Will*, does adhere to its superior Court's decision—a decision which violates the Fourth Amendment.

The government also argues that specifying a date range would be inappropriate because it may not reveal incriminating evidence located in unallocated space. Mr. Kleeh testified that when a file is deleted it stays on the computer in unallocated space until another file is written to that location. JA at 660. The file remains on the computer indefinitely until the file system writes another file over it. JA at 662. The files do not necessarily get written over in the order they are deleted, and it could be written over years after the file is put in unallocated space. *Id.* There may be data remaining about the file "if the catalogue record of it, if that still exists, it would have dates and times with it," and "[y]ou could have internal data associated with it." JA at 663. "Internal data" is often referred to as metadata," and some computer applications "will record dates and times internal to that document such as when it was created, when it was last edited, the author of the document." *Id.* Also, "[p]ictures will often contain what they call access data which will record the make and model of a camera, the date they were taken," and that information will be included on a file that is in unallocated space. *Id.*

Mr. Kleeh testified that none of the information is immediately lost when a file is put into unallocated space, "but if that catalogue gets overwritten, a new file comes and the system writes over that catalogue, the data to the file could still be in unallocated space, but there wouldn't be any record of it anywhere so you would lose the dates and times from the file system." JA at 663. The "internal metadata, that would still remain until that section of the data got overwritten." JA at 664. Mr. Kleeh testified that the catalogue and the file are in two different locations, and internal data is stored within the file itself. JA at 664. A catalogue is overwritten in the same way file data is; a new catalogue record gets created over an old one. *Id.*

Mr. Kleeh clarified the difference between an "unallocated file," and a "lost file." A "strictly unallocated file is just data that was located beyond the user's access." JA at 698. There is "no catalogue of it, nothing that records where that data is located," and there is therefore "no way even from a forensic standpoint" to determine whether the file was created at a particular time by a particular user. JA at 698. A "lost file," on the other hand" is a "recovered deleted file" which the user deleted and could no longer access, but the catalogue was recoverable through the use of forensic software. *Id.* According to Mr. Kleeh, it was not entirely correct to say that files located in unallocated space contain no metadata or information with respect to when they were deleted or viewed, or where they were

downloaded from. JA at 699. "That is where like the deleted, recovered, the lost files come in, and the metadata internal to the file . . . such as time stamps for like cameras." *Id.* Mr. Kleeh testified that with respect to lost files, the file is not overwritten and the catalogue saying where that file is located is not overwritten. JA at 700. These "may include metadata such as file location, date last accessed, and date deleted." *Id.*

Mr. Kleeh testified that when doing the imaging process, DCFL does not filter for specific dates. JA at 702. If they were to screen for certain dates, it could do so only by looking for metadata, and it would take place at the end of the imaging process. JA at 703. Mr. Kleeh testified, "Once the FDE gets it, they could then filter based upon the metadata." JA at 703.

There are a number of points to be made from Mr. Kleeh's testimony. Picture files, even those that have been deleted, often contain data which will record the date the pictures were taken. DCFL has the capability of determining, from examining the file itself or the catalogue if it is available, whether there is enough information to determine whether a file falls within a particular date range. And DCFL has the capability of segregating those files. While the government claims that "[t]here does not appear to be any information in the record as to whether the image of child pornography SA Nishioka initially found in unallocated space on the first FDE had any dates or times associated with it" (Answer at 7,

n.5), it is entirely possible that it did. And if it did[3], and if the date reveals that the file falls outside the range of the search authorization, it should never have been opened.

Based on the foregoing, Appellant respectfully submits that the search authorization was overbroad.

B. The good faith exception does not apply.

The government has not met its burden to show by a preponderance of the evidence that the "good faith" exception to the exclusionary rule should apply. See Mil.R.Evid. 311(d)(5)(A). For the good faith exception to apply, the government must establish that law enforcement's reliance on a defective search authorization is objectively reasonable. *United States v. Hoffmann*, 75 M.J. 120, 127 (C.A.A.F. 2016). The good faith doctrine applies where the seizure resulted from an authorization issued by a military magistrate; the magistrate had a substantial basis for determining probable cause existed; and law enforcement reasonably and in good faith relied on the authorization. *United States v. Nieto*, No. 16-0301/AR (C.A.A.F. 21 Feb. 2017). When reviewing a military magistrate's probable cause determination, this Court examines whether the military magistrate "had a

[3] Appellant does not concede that it is appropriate for law enforcement to open files found in unallocated space that *do not* contain metadata or for which there is no catalogue available. He merely states that where the range of dates of the offense is known to law enforcement, agents must at the very least first determine whether the file falls within the range of dates, and if it does not, and the agents know that it does not, it cannot be opened.

substantial basis for concluding that probable cause existed. *United States v. Nieto*, Slip. Op. at 6. A "substantial basis exists when, based on the totality of the circumstances, a common-sense judgement would lead to the conclusion that there is a fair probability that evidence of a crime will be found at the identified location." *Id.* If a military magistrate does did not have a substantial basis to find probable cause, the exclusionary rule ordinarily applies. *Hoffmann*, 75 M.J. at 124. An exception to the exclusionary rule applies if the government establishes that law enforcement's reliance on a defective authorization is objectively reasonable. *Id*. at 127.

As discussed previously, the military magistrate did not have a substantial basis for concluding that evidence of a crime would be found in any files pre-dating mid-2010. The government appears to concede this point, both as it relates to SA Nishioka's search for evidence relating to the "little brothers" (Answer at 30), and its claim that "the inclusion of the Florida statute in the warrant already limited the agents to searching only for evidence for which there was probable cause." Answer at 16.

The government claims that Appellant "appears to be conflating the affidavit and the search authorization" by arguing that the search authorization fails the third prong of *United States v. Leon*, 468 U.S. 897 (1984) because there was no probable cause in the affidavit to support a conclusion that Appellant had committed any

offense prior to April 2010. Answer at 27. Respectfully, Appellant has not "conflated" anything. The third prong of *Leon* addresses the sufficiency of the affidavit, and the fourth prong of *Leon* addresses the warrant itself. There is nothing in the affidavit to support a conclusion that Appellant had committed an offense prior to April of 2010, and it was therefore inappropriate under the third prong of *Leon* to seek a search authorization that was unlimited in its temporal scope. Although SA Winchester outlined the relevant dates when she described the offense, she did not request that the military magistrate issue a search authorization for files limited by those dates. Instead, she requested authority "to search for and collect: a) *All* electronic media and power cords for devices capable of transmitting or storing online communications located within SUBJECT's personal possession." JA at 328 (emphasis added). And the search authorization is facially deficient under the fourth prong of *Leon* in that it fails to particularize the things to be seized inasmuch as it permits the seizure of *all* communications, irrespective of the dates.

The government argues that even if the search authorization was overbroad in failing to contain a temporal limitation, it "was not so facially deficient that the AFOSI agents could not have reasonably presumed it to be valid[,]" and "a reasonably trained officer would not have known that the search was illegal despite the magistrate's authorization." Answer at 28. This is so because there is no

requirement requiring all search authorizations to contain date limitations, and "a reasonably trained officer would not have known that the search was illegal despite the magistrate's authorization." *Id.* This, again, is where the government's concession that the search authorization actually contains a temporal limitation is troubling. The government claims on the one hand that the search authorization actually contained a temporal limitation, but then claims on the other hand that if it was overbroad in failing to contain a temporal limitation, it was not facially deficient. The search authorization either contained a temporal limitation or it did not. If it did, the agents exceeded the scope. If it did not, it was overbroad. But in any event, even absent binding precedent, the affidavit accompanying the search authorization defined the crime under investigation as limited in duration. A reasonably trained law enforcement officer would know that where the affidavit describes a crime in limited terms, a search is unlawful where search authorization issued pursuant to the affidavit is unlimited and the agent fails to confine the search to the limitation described in the affidavit. *See generally Massachusetts v. Sheppard*, 486 U.S. 981, 989 (1984) (holding that where the offense described on the face of the warrant was different from the offense described in the affidavit, a reasonable police officer would have concluded that the warrant authorized a search for materials outlined in the affidavit). In this regard, the warrant itself was so facially deficient in failing to particularize the things to be seized that the

officers could not presume it to be valid. *See Leon*, 468 U.S. at 923. It appears that all of the law enforcement officers involved in this case looked to the terms of the search authorization (which was unlimited in scope) rather than the affidavit (which was limited in its description of the offense by the relevant date range, but unlimited in its request of files to be seized). Although she clearly knew the relevant date range, SA Winchester never requested that the military magistrate limit the search authorization by the relevant date range; she never requested DCFL to segregate or otherwise limit the data by date; DCFL made no attempt segregate the date, although it could have; and SA Nishioka appeared to look at every file he was given without regard to date until he came across an image that appeared to be child pornography, even though the affidavit described a limited period of misconduct.

The government argues that because SA Nishioka was searching in a location in which it was objectively reasonable to search, his subjective intent was not relevant. Answer at 30. As the Supreme Court stated in *Maryland v. Garrison*, 40 U.S. 79, 84 (1987), "the scope of a lawful search is defined by *the object of the search* and the places in which there is probable cause to believe that it may be found." (emphasis added). Thus, while SA Nishioka may have been searching in a place in which it was reasonable to look for evidence of a crime, his claim that he was actively searching for something other than the object of the search is certainly

relevant to whether he was conducting the search in an objectively reasonable manner – that is, whether he was acting in good faith. The government also quotes *Horton v. California*, 496 U.S. 128, 138 (1990), which holds, "The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure *if the search is confined in an area and duration by the terms of the warrant or a valid exception to the warrant requirement.*" (emphasis added). Appellant takes no issue with this as a general proposition, but again notes that SA Nishioka's failure to confine the search to the terms of the authorization is relevant to whether his conducting of the search was objectively reasonable. The search was not "confined in an area and duration by the terms of the warrant" because SA Nishioka did not limit his search, and his admission that he was specifically looking for items of evidence outside the scope of the search warrant undercuts any claim that he was acting in good-faith reliance on the search authorization.

The government also argues that SA Nishioka's stopping of the search when he came across an image of child pornography demonstrated good faith. According to the government, "This demonstrates that SA Nishioka knew he was not allowed to exceed the scope of the search authorization and was determined not to do so." Answer at 31. Respectfully, the most this demonstrates is that SA Nishioka knew that the search authorization did not cover child pornography. It

says nothing about what SA Nishioka knew or reasonably should have known about the date restriction. The government also argues SA Nishioka "consulted the legal office," and cites *United States v. Riccardi*, 405 F.3d 852, 864 (10th Cir. 2005) for the proposition that "by consulting the prosecutor about the scope of the warrant, the officers showed their good faith in compliance with constitutional requirements." Answer at 31. Unlike *Riccardi*, where the agents obtained assurances from the district attorney that they were acting within the scope of the warrant, whatever discussions SA Nishioka and SA Winchester may have had with legal[4] apparently had to do with whether there was probable cause with respect to child pornography that would support a new search authorization request, not with respect to the scope of the search authorization that had already been issued. It does not appear from the record that at the time SA Nishioka searched the unallocated space and found the first image of child pornography that anyone was thinking about the scope of the search authorization as it related to the date range.

The government argues that the deterrent effect of applying the exclusionary rule in this case would not outweigh the substantial costs to the justice system of suppressing the evidence. Answer at 32. In making this argument the government claims that the agents "confined their search to the terms of the search

[4] There is nothing in the record to suggest that SA Nishioka did anything other than "notif[y] the legal office." JA at 762. SA Winchester "coordinated with" the SJA "and requested a probable cause determination," and the SJA "agreed probable cause existed to conduct a search of the electronic media." JA at 292.

authorization as written." As discussed, if the search authorization was limited in its temporal scope, as the government now claims, then the agents *did not* confine their search. SA Nishioka testified that he methodically looked through all of the files in the allocated space, then began to look through all of the files in the unallocated space. JA at 773. If the search authorization as written was unlimited in temporal scope, it was overbroad because it failed to state with particularity the things to be seized, and as discussed, the "good faith exception" cannot save it.

But in any event, the exclusionary rule "applies only where it results in appreciable deterrence for future Fourth Amendment violations and where the benefits of deterrence must outweigh the costs." *United States v. Wicks*, 73 M.J. 93, 104 (C.A.A.F. 2014). This Court, in *Nieto*, at 9, discussed the Supreme Court's holding in *Riley v. California*, 134 S.Ct. 2473, 2489 (2014) that cellular phones "are in fact minicomputers that have immense storage capacity allowing them to store thousands of pictures, or hundreds of videos." In that case, the Supreme Court noted that a cellular phone "collects in one place many distinct types of information . . . that reveal much more in combination than any isolated record," and the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." *Id*. at 2490. The Court recognized that "a cell phone search would typically expose to

the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id*. at 2490-91.

The government argues that the Agent's conduct was reasonable in this case; Appellant obviously disagrees. In fact, it appears that although SA Winchester accurately defined the temporal scope of the offense at issue in in the affidavit, she did not specifically ask for a warrant that was limited by that scope. The military magistrate did not issue a warrant that was limited by that scope. SA Winchester did not ask DCFL to segregate any of the data by those date, and DCFL did not segregate the data by those dates. And SA Nishioka opened all of the files in the allocated space before he moved on to the unallocated space, all apparently without regard to the date. In other words, although everyone involved in this case knew or should have known that the date range was relevant, no one apparently cared. That is the very definition of recklessness, and the exclusionary rule should apply to deter similar law enforcement conduct in the future.

C. The pre-April 2010 evidence would not have been inevitably discovered.

Finally, the government argues that the exclusionary rule should not apply because the evidence would have been inevitably discovered. The government must establish by a preponderance of the evidence that "*when the illegality*

occurred, the government agents possessed or were actively pursuing evidence or leads that would have inevitably led to the discovery of the evidence and that the evidence would inevitably be discovered in a lawful manner had the illegality not occurred." *Hoffmann*, at 124-25 (emphasis in original). The government relies on *United States v. Crespo-Rios*, 645 F.3d 37 (1st Cir. 2011) for the proposition that child pornography found on the defendant's computer would have been inevitably discovered irrespective of whether there was probable cause to search for child pornography because the agents had probable cause to search for chats and other evidence of enticement. Answer at 34. According to the government, "The search for such evidence had to account for mislabeled or concealed files, and thus 'forensic experts would have thoroughly combed through files and would have inevitably discovered the child pornography that *Crespo* now seeks to suppress[,]'" and the agents in this case still had probable cause to search for online communications between Appellant and AP. Answer at 34-35.

The government claims that, "Assuming the agents were confined to searching for files within a certain date range, it would have still been reasonable and lawful for SA Nishioka to search in a folder of pictures labeled 'unallocated' since those files likely no longer had dates associated with them." Answer at 35. Nothing in the record supports a conclusion that those files "likely no longer had dates associated with them." As discussed previously, Mr. Kleeh testified that

such files "often" still had internal data associated with them, and the catalogue data is not immediately overwritten and may, in fact, remain for quite some time. In fact, a great deal of the evidence admitted against Appellant came from unallocated space and had internal data associated with it. In this regard, the government also overstates the evidence when it states on page 23 of the Answer that "there was a significant chance that a specific date and time would no longer be associated with such files." Mr. Kleeh never said there was a "significant chance." Instead, he said, "*if* that catalogue gets overwritten . . . there wouldn't be any record of it anywhere" (JA at 663) and says that a "strictly unallocated file is . . . just floating around residual from other activities, essentially, and there is no catalogue," whereas with a "lost file . . . we are able to recover that information, that catalogue." Indeed, a great deal of evidence admitted against Appellant came from unallocated space yet DCFL was able to make determinations about the dates.

The government was limited to searching for evidence within a certain date range, and it should have determined that these files fell within that range before opening them. The government has therefore failed to meet its burden to show by a preponderance of the evidence that the evidence in this case would have been inevitably discovered.

D. The error was not harmless beyond a reasonable doubt.

The government acknowledges that Appellant would be prejudiced in the event this Court determines that admission of the evidence was erroneous. Answer at 35. Appellant respectfully submits that the evidence was erroneously admitted, the admission was not harmless beyond a reasonable doubt, and respectfully requests the findings of guilty under Charge I and the sentence be set aside.

WHEREFORE Appellant so prays.

Respectfully submitted,

FOR: William E. Cassara
Counsel for Appellant
PO Box 2688
Evans, GA 30809
CAAF Bar No. 26503
706-860-5769
bill@williamcassara.com

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(d) because it contains 5,961 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because it has been prepared in a proportional typeface using Microsoft Word Version 2016 with Times New Roman 14-point typeface.

FOR: William E. Cassara
Counsel for Appellant
PO Box 2688
Evans, GA 30809
CAAF Bar No. 26503
706-860-5769
bill@williamcassara.com

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing was electronically mailed to the Court and to the Director, Air Force Government Trial and Appellate Counsel Division, on February 27, 2017.

PATRICK A. CLARY, Capt, USAF
Detailed Military Appellate Counsel
USCAAF Bar No. 35634
United States Air Force
1500 W. Perimeter Rd, Ste 1100
Joint Base Andrews NAF, MD 20762
(240) 612-4770
patrick.a.clary.mil@mail.mil