In the Matter of the UNITED STATES OF AMERICA'S APPLICATION FOR A SEARCH WARRANT TO SEIZE AND SEARCH ELECTRONIC DEVICES FROM EDWARD CUNNIUS.

Feb. 11, 2011.
United States District Court,
W.D. Washington,at Seattle.
No. 2:11-mj-00055-JPD-JLR.

MEMORANDUM ORDER DENYING THE GOVERNMENT'S APPLICATION FOR A WARRANT TO SEIZE AND SEARCH ELECTRONIC DEVICES

JAMES P. DONOHUE, United States Magistrate Judge.

I. INTRODUCTION AND SUMMARY CONCLUSION

***1** This matter comes before the Court on the government's application for a warrant to search the residence of Edward Cunnius, to seize any computers or digital devices (collectively "digital devices") [FN1] that may be located at the premises, and to search all electronically stored information ("ESI") contained in any digital devices seized from Mr. Cunnius' residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods. Specifically, in addition to the search of the residence and the seizure of digital devices, the application requests the authority for investigative officers to: (1) search all ESI contained in Mr. Cunnius' digital devices and related to the use of the devices; (2) conduct the search without segregation by a filter team; (3) conduct the search without foreswearing the plain view doctrine; and (4) permit investigative agents to obtain a second warrant if, during the search of the ESI, the investigating and searching agents find evidence of crime outside the scope of the instant warrant. On February 7, 2011, the Court advised the Assistant United States Attorney ("AUSA") that the warrant, as presented, would not be granted. The United States has refused to accede to the Court's view that a filter team and forswearing reliance on the plain view doctrine are appropriate, and indeed, required in this specific case. Accordingly, the AUSA requested the Court to file a memorandum opinion, so that the government can appeal. A copy of the requested warrant and affidavit in support is attached as Exhibit 1. That request has led to this opinion.

Because the government, in this application, refuses to conduct its search of the digital devices utilizing a filter team and foreswearing reliance on the plain view doctrine, the Court DENIES the application as seeking an overbroad or general warrant in violation of the Fourth Amendment and the law of this Circuit.[FN2]

II. DISCUSSION

A. *The Warrant Application to Seize and Search ESI devices*

The affidavit in support of the government's warrant application indicates that agents received information from Microsoft Corporation ("Microsoft") in October 2010 regarding an individual, Mr. Cunnius, whom they believed was advertising counterfeit

Microsoft software via the internet classified advertising service Craigslist. Specifically, a Microsoft anti-piracy investigator informed agents that a shipment of counterfeit Microsoft software from China, addressed to "Edward Russell Cunnius" at 2305 Rucker Avenue # 5, Everett, Washington, had been seized by Customs and Border Protection ("CBP") on October 18, 2010. In response to the CBP seizure, Microsoft sent a warning letter advising Mr. Cunnius that it had received information that he or someone with his company may have distributed illegal and/or unlicensed Microsoft software. The letter informed Mr. Cunnius of the consequences of illegal distribution.

The Microsoft investigator also informed the agents that Mr. Cunnius was responsible for numerous Craigslist advertisements over the past few months that offered to sell brand new, in-the-box, Microsoft software at prices well below typical retail prices for the same software. After contacting Mr. Cunnius at the phone number listed on the Craigslist advertisements, Microsoft conducted an undercover test purchase of several products from Mr. Cunnius at his home in Everett, Washington. These products were purchased at prices substantially below retail value, and upon further examination, were found to be counterfeit.

2 Following Microsoft's test purchase, undercover law enforcement agents conducted two test purchases from Mr. Cunnius at his apartment. On each occasion, agents contacted Mr. Cunnius via the telephone number listed in his Craigslist advertisements, and met with Mr. Cunnius at his apartment. The agents purchased several boxes of purportedly genuine, new, in-the-box, Microsoft software from Mr. Cunnius on December 13, 2010, and December 21, 2010, respectively. During each purchase, Mr. Cunnius retrieved the boxes containing the software from a closet in the bedroom of his apartment. According to the affidavit, he was evasive in response to questions regarding the authenticity of the products, and stated that if customers complained to him, he would instruct them to go buy the products for much higher prices at retail establishments. The agents submitted the products purchased from Mr. Cunnius to Microsoft for analysis by their product identification specialists, who determined that the products were counterfeit.

In response to questions regarding Mr. Cunnius' supplier, Mr. Cunnius told the undercover agents that it took him years to make his contact with his supplier and that he receives his product through the mail. He also told the agents that he communicates with his source via electronic mail, and pays him through electronic transfer from his bank.

The government then applied to this Court for a warrant authorizing agents to search Mr. Cunnius' apartment and seize evidence, fruits and instrumentalities of the crimes of (1) copyright infringement and/or (2) trafficking in counterfeit goods. Specifically, the government believes that evidence related to how Mr. Cunnius obtained counterfeit software, paid for it, and how he distributed the counterfeit software is likely to be discovered on digital devices located at his apartment. This evidence may include e-mail correspondence with Mr. Cunnius' source, evidence of internet banking transactions, and evidence of his online advertisements and marketing of counterfeit software. In addition, the government wishes to search for evidence of dominion and control of any digital device located in the apartment in order to determine who else may be responsible for

obtaining and trafficking in the counterfeit software purchased from Mr. Cunnius, and who may have been using the computers at the relevant time.

There is no suggestion that the target is using the digital devices to "burn" counterfeit discs, or to transmit counterfeit copies electronically. Instead, the target of the investigation allegedly sells in-the-box counterfeit copies that have been imported.

The Court finds that the warrant affidavit establishes probable cause to search the digital devices located at Mr. Cunnius' residence for evidence of criminal copyright infringement and/or trafficking in counterfeit goods. Probable cause exists if "it would be reasonable to seek the evidence in the place indicated in the affidavit." *United States v. Wong,* 334 F.3d 831, 836 (9th Cir.2003) (quoting *United States v. Peacock,* 761 F.2d 1313, 1315 (9th Cir.1985)). The two crimes contemplated by the warrant in this case involve the "distribution" or "trafficking" of certain goods. Specifically, criminal copyright infringement includes "willfully infring[ing] a copyright" if that infringement was committed "for purposes of commercial advantage or private financial gain ... by the reproduction or distribution, including by electronic means ... of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000." 17 U.S.C. § 506(a), (b). Similarly, trafficking in counterfeit goods involves "intentionally traffic[king] or attempt[ing] to traffic in goods or services and knowingly us[ing] a counterfeit mark on or in connection with such goods or services ... the use of which is likely to cause confusion, to cause mistake, or to deceive...." 18 U.S.C. § 2320(a), (b). In light of the sworn affidavit that Mr. Cunnius advertises the counterfeit goods by posting advertisements containing digital photographs of the products on the website Craigslist, communicates with his source by e-mail, and pays his source using electronic transfers from his bank, the Court can reasonably assume that digital devices contain evidence relating to the crimes alleged.

3 However, despite the existence of probable cause to search the digital devices, the Court finds the warrant requested by the government overbroad. The affidavit contains no reference to use of a filter team, and no promise to foreswear reliance on the plain view doctrine. With respect to the procedures to be employed by law enforcement personnel to execute the search of digital devices, once they have been seized, the affidavit provides:

> In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data falls within the list of items to be seized pursuant to the warrant.

> The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate, and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.
>
> If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offense referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offense referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.
>
> Unless the government seeks an additional order of authorization from any Magistrate Judge in the District, the government will return any digital device that has been forensically copied, that is not an instrumentality of the crime, and that may be lawfully possessed by the person/entity from whom it was seized, to the person/entity from whom it was seized within 90 days of seizure.
>
> If, in the course of their efforts to search the subject digital devices, law enforcement agents or analysts discover items outside of the scope of the warrant that are evidence of other crimes, that data/evidence will not be used in any way unless it is first presented to a Magistrate Judge of this District and a new warrant is obtained to seize that data, and/or to search for other evidence related to it. In the event a new warrant is authorized, the government may make use of the data then seized in any lawful manner.

4 Larson Aff. ¶ 46(c)-(g).

As discussed below, permitting the government to conduct a search along these lines would violate the Fourth Amendment and the law of this Circuit.

B. *The Fourth Amendment Prohibits General Searches*

The instant warrant application cannot be squared with the Fourth Amendment's prohibition on general searches. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one "particularly describing the place to be

searched and the persons or things to be seized." *Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987) (citing U.S. Const. amend. IV). As the Supreme Court noted:

[t]he manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Id. This understanding of the Fourth Amendment's particularity requirement broke no new ground. Indeed, sixty years before *Maryland v. Garrison* was decided, the Supreme Court recognized general searches were long deemed to violate the Constitution. *Marron v. U.S.,* 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 (1927).

The Fourth Amendment's particularity provision was enacted to respond to the evils of general warrants and writs of assistance which English judges had employed against the colonists. *Virginia v. Moore,* 553 U.S. 164, 169, 128 S.Ct. 1598, 170 L.Ed.2d 559 (2008). As the Supreme Court stated:

> The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;" since they placed "the liberty of every man in the hands of every petty officer."

Boyd v. United States, 116 U.S. 616, 625, 6 S.Ct. 524, 29 L.Ed. 746 (1886) (internal footnotes omitted). The requirement was thus designed to ensure only a specific place is searched and that probable cause to search that place actually exists. *See Steele v. United States,* 267 U.S. 498, 501-02, 45 S.Ct. 414, 69 L.Ed. 757 (1925).[FN3]

Here, the government seeks permission to search every bit of data contained in each digital device seized from Mr. Cunnius' residence. Contrary to the Fourth Amendment's particularity requirement limiting searches to only the specific areas and things for which there is probable cause to search, the government seeks to scour everything contained in the digital devices and information outside of the digital devices. This practice is akin to the revenue officers in colonial days who scoured "suspected places" pursuant to a general warrant.

***5** The Court has considered the fact that the search warrant application seeks permission to search and seize evidence of the specified crimes, and a second warrant would be needed to seize evidence of other crimes for which there is no probable cause shown. However, the ability to seek a second warrant after finding evidence as to which there was no probable cause to search only magnifies the danger of the warrant constituting a general warrant. The requirement that a second warrant be obtained provides no

meaningful limitation on the scope of the search conducted under the first warrant and no meaningful protection against the government obtaining evidence for which it lacks probable cause. For the first warrant would be nothing more than a "vehicle to gain access to data for which the government has no probable cause to collect." *Comprehensive Drug Testing v. United States,* 621 F.3d 1162, 1177 (9th Cir.2010) (en banc) (" *CDT III* ").[FN4] Indeed, the warrant the government now seeks would permit it to seize evidence found outside the scope of the first warrant whether that evidence was initially in plain view, or not.

C. *What is Involved in a Digital Search?*

As noted above, there is no suggestion in the affidavit that the digital devices at issue are being used to burn counterfeit discs or otherwise create or electronically transmit illegal copies of the software at issue. Instead, the affidavit makes it clear that the allegedly counterfeit software at issue is being imported. The search of the digital devices would undoubtedly be helpful to reveal the source(s) of supply, the quantity, customer names of the counterfeit merchandise, financial gains from the activity, and knowledge of the counterfeit nature of the goods. Against these legitimate needs, the Court weighs the vast amount and nature of data that can be stored on or accessed by personal computers, an analysis which illustrates the continued importance of the Fourth Amendment's particularity requirement.

1. *A Digital Search Captures Vast Quantities of Data*

A government search of even a single, non-networked computer involves searching vast quantities of ESI. As pointed out in the warrant affidavit, a single gigabyte of storage space is the equivalent of 500,000 double-spaced pages of text. Larson Aff. ¶ 45(b). Computer hard drives are now being sold for personal computers capable of storing up to two terabytes, or 2,048 gigabytes of data. *Id.* If a computer is networked, this exponentially increases the volume of data being searched. Thus, the sheer volume of ESI involved distinguishes a digital search from the search of, for example, a file cabinet.

2. *A Digital Search Captures Innocent and Personal Information With No Relevance to the Asserted Crimes*

Because it is common practice for people to store innocent and deeply personal information on their personal computers, a digital search of ESI will also frequently involve searching personal information relating to the subject of the search as well as third parties. As Judge Kleinfeld noted:

> ***6** The importance of this case is considerable because, for most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests-including perfect strangers-are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation.
>
> There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality

> in allowing search warrants. Emails and history links may show that someone is ordering medication for a disease being kept secret even from family members. Or they may show that someone's child is being counseled by parents for a serious problem that is none of anyone else's business. Or a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures. Just as a conscientious public official may be hounded out of office because a party guest found a homosexual magazine when she went to the bathroom at his house, people's lives may be ruined because of legal but embarrassing materials found on their computers. And, in all but the largest metropolitan areas, it really does not matter whether any formal charges ensue-if the police or other visitors find the material, it will be all over town and hinted at in the newspaper within a few days.
>
> Nor are secrets the only problem. Warrants ordinarily direct seizure, not just search, and computers are often shared by family members. Seizure of a shared family computer may, though unrelated to the law enforcement purpose, effectively confiscate a professor's book, a student's almost completed Ph.D. thesis, or a business's accounts payable and receivable.

U.S. v. Gourde, 440 F.3d 1065, 1077 (9th Cir.2006) (Kleinfeld, J., dissenting).

3. *Digital Devices Function as a Portal in the Age of Cloud Computing* [FN5]

The language in the instant warrant raises another significant constitutional concern related to the interactive nature of modern digital devices. These digital devices are not just repositories of data, but access points, or portals, to other digital devices and data, typically obtained through the internet or stored on a network. All data on the internet is both separate and one. The requested warrant is, in essence, boundless. This is made evident by the fact that the government seeks authorization, among other things, to obtain "all passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data." Larson Aff. ¶ 47(g).

This poses a multitude of problems, and it highlights the concerns raised by Judge Kleinfeld. First, once the government has all passwords, it is able to access a defendant's most sensitive information. To the extent the defendant may have medical records on-line, that information is now available to the government. If the defendant's wife, who is not alleged to be involved in any criminal activity, is sending embarrassing, private e-mail messages, that information is now available for use by the government. If the government wants to see what books the defendant is reading, or what movies his wife is viewing, all of this would be fair game under the warrant presented by the government. Moreover, if the defendant has been looking at legal but "dirty" pictures the government will know this as well, even if the defendant had intended to "throw them away." The government candidly acknowledges that its protocols "are exacting scientific procedures designed to protect the integrity of evidence and recover even hidden, erased, compressed, password-protected, or encrypted files." Larson Aff. ¶ 45.

4. *A Digital Search Captures ESI of Which the User Is Unaware*

***7** In addition to granting the government access to ESI that was consciously downloaded by computer users, this boundless search would reveal ESI that computer users have no way of knowing is stored on their device. [FN6] A search of a file cabinet, in contrast, would include only items put in the file cabinet by a person. A conscious, even if unknowing, act is required. This act perhaps would be analogous to intentionally downloading a file. However, in contrast to the conscious act of downloading a file or storing something in a file cabinet, cache files are a set of files automatically stored on a user's hard drive by a web browser to speed up future visits to the same websites, without the affirmative action of downloading. *See U.S. v. Romm,* 455 F.3d 990, 993 n. 1 (9th Cir.2006). *See also U.S. v. Parish,* 308 F.3d 1025, 1030-31 (9th Cir.2002). "Most web browsers keep copies of all the web pages that you view up to a certain limit, so that the images can be redisplayed quickly when you go back to them." *Romm,* 455 F.3d at 993 n. 1. Thus, a person's entire online viewing history can be retrieved from the cache, without any affirmative act other than visiting a web page.

5. *A Digital Search Captures "Destroyed" Data*

Unlike information in a file cabinet that can simply be taken out and destroyed, ESI is present after attempts to destroy it. In addition to data stored in cache files, ESI can be recovered from "unallocated space" on a hard drive, which "contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software." *United States v. Flyer,* No. 08-10580, slip op. at 2429 (9th Cir. Feb. 8, 2011). The government knows that once ESI is created, it is very difficult to destroy, and indeed, the government highlights this function. In the affidavit, the government states

> Once created, electronically stored information ("ESI") can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the user. The browser often maintains a fixed amount of hard drive space devoted to these files, and files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.... Even when such action [the affirmative attempts to delete] has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

Larson Aff. ¶ 44(a).

Although the probative evidence stored in any digital device seized in this case would seem to be limited to the supplier(s), possible customers, warnings, and the underlying financial data, the government has indicated that it may "search for and attempt to recover deleted, hidden, or encrypted data 'to determine whether the data fall within the list of items to be seized.' " Larson Aff. ¶ 46(c). Such a request sweeps into the search of a single ESI device all sites, all data, and all persons that device accessed via the internet.

6. *General Principles of the Fourth Amendment*

***8** In opposing the requirement of a filter team and forswearing reliance on the plain view doctrine, the government has taken the position that the characteristics set forth above relating to digital searches do not require heightened Fourth Amendment protection, citing the U.S. Supreme Court's assertion in *Katz v. United States* that "the Fourth Amendment protects people, not places." 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). It contends that a digital search is no more intrusive than a properly authorized search that requires officers to sift through all of an individual's papers, and every possible place where such papers might be found within the home. The government also cites the Ninth Circuit's statement in *United States v. Giberson* that "[w]hile it is true that computers can store a large amount of material, there is no reason why officers should be permitted to search a room full of filing cabinets or even a person's library for documents listed in a warrant but should not be able to search a computer." 527 F.3d 882, 888 (9th Cir.2008).

Following *Giberson,* however, the Ninth Circuit began to refine its analysis. In *U.S. v. Payton,* the court explained that " *Giberson* held that computers were not entitled to a special categorical protection of the Fourth Amendment. Instead, they remained subject to the Fourth Amendment's overall requirement that searches be constitutionally 'reasonable.' " 573 F.3d 859, 863-64 (9th Cir.2009). Under *Giberson,* "[i]f it is reasonable to believe that a computer contains items enumerated in the warrant, officers may search it." *Id.* at 864 (citing *Giberson,* 527 F.3d at 888). With respect to the actual search conducted by the agents, however, the *Payton* court observed that "the nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests ... *We believe that it is important to preserve the option of imposing such conditions when they are deemed warranted by judicial officers authorizing the search of computers.*" *Id.* at 864 (emphasis added). The *Payton* court concluded that "the special considerations of reasonableness involved in the search of computers are reflected by the practice, exemplified in *Giberson,* of searching officers to stop and seek an explicit warrant when they encounter a computer that they have reason to believe should be searched." *Id.* As discussed further below, this refinement continued in the *CDT* line of cases.

D. *Comprehensive Drug Testing Inc. v. United States*

The unconstitutionality of the instant warrant application, as well as the application presented in *CDT III,* is revealed by tracing the odyssey of the *CDT* litigation. Here, the government seeks to search all data contained in digital devices seized from Mr. Cunnius' residence, as well as information outside the devices. The government intends to perform this search without a filter team to separate from the investigative agents information that is outside the scope of the warrant. Additionally, the warrant does not foreswear reliance on the plain view doctrine, and further seeks authorization to obtain and use information found outside the scope of the initial warrant whether or not that information was found in plain view.

***9** With this background, the Court turns to the Ninth Circuit opinion in *CDT III.* In that case, the government obtained a warrant to search CDT's facilities limited to the records of ten baseball players for whom there was probable cause to suspect of drug use. Included in the warrant was a provision to allow seizure of computer records from CDT facilities for off-site examination and segregation of the evidence. To justify this provision, which the government acknowledged included information beyond that relevant to the investigation, the supporting affidavit contained information about the difficulty and hazards of retrieving only ESI for which the government had probable cause.

Based on these representations, a magistrate judge granted the government permission to engage in a broad seizure. However, the warrant the magistrate judge authorized also contained important restrictions on the handling of seized data, including review and segregation by noninvestigating law enforcement personnel rather than the case agents. The purpose of the segregation requirement was to prevent case agents from accessing information outside the scope of the warrant.

Utilizing this warrant, agents found at CDT's facilities the "Tracey Directory," which included, among hundreds of other documents, a spreadsheet containing the names of all the major league baseball players who had tested positive for steroids.[FN7] The government had probable cause to search and seize records of ten baseball players. After deciding it was impractical to sort through the information on-site, the agents removed the data for off-site review. Although the warrant required segregation and screening, the case agent ignored this requirement and took control of the data.

Based on its search of the Tracey Directory, the government obtained additional warrants to search the facilities of CDT and Quest for information regarding more baseball players who they discovered had tested positive for steroids, and issued subpoenas demanding production of the same records it had just seized. The government claimed it was justified in obtaining this additional incriminating information, based on the plain view doctrine of evidence found outside the scope of the warrant. In response, CDT and the baseball players' association moved for return of the seized property.

The litigation in *CDT III* involved multiple district courts. Two district courts ordered the government to return the property.[FN8] The judges expressed grave dissatisfaction with the government's conduct; some accused the government of manipulation and misrepresentations. As one district judge stated in rejecting the government's arguments, "whatever happened to the Fourth Amendment? Was it ... repealed somehow?" *CDT III,* 621 F.3d at 1177 (citing *CDT I,* 513 F.3d at 1117).

The government appealed to the Ninth Circuit. In a reissued decision, the panel reversed two of the district courts' orders to return the property, and held the government was bound by the third court's order containing factual determinations including the government's failure to comply with the warrant and that it had displayed a callous disregard for the rights of third parties. *CDT I,* 513 F.3d 1085. Despite these

determinations, the Ninth Circuit initially upheld the seizures. The dissent strenuously argued the decision was unfounded, ignored factual findings of the lower courts, and would have dire ramifications. As Judge Thomas stated, "Today's decision marks the return of the prohibited general warrant through an endorsement of a disguised impermissible general search warrant-a tactic we rejected in *United States v. Rettig,* 589 F.2d 418 (9th Cir.1978)." *Id.* at 1143 (Thomas, J., concurring in part, dissenting in part).

10 The case was then taken *en banc. CDT II,* 579 F.3d 989. The *en banc* panel reversed and ordered the return of all testing results, save the ten athletes named in the first warrant. The majority explored the government's improper conduct and further reflected on the balance between law enforcement's perhaps legitimate need to over-seize in conducting searches of ESI devices, with the Fourth Amendment's prohibition on general or overbroad searches. To strike this balance, the court directed magistrate judges to adhere to the following five guidelines:

> 1. Magistrate[ ] [Judges] should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006.

On September 13, 2010, the Ninth Circuit issued a revised *en banc* opinion. *CDT III,* 621 F.3d 1162. The new opinion did not change the outcome of the first *en banc* decision, but the five guidelines that were previously part of the majority decision became part of a concurring opinion authored by Chief Judge Kozinski. In his concurrence, joined by four other judges, Chief Judge Kosinski notes the guidelines are "hardly revolutionary," are "essentially *Tamura's* solution to the problem of necessary over-seizing of evidence," and also offer "the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects." *Id.* at 1178, 1180 (Kozinski, C.J ., concurring).

In the Court's view, the Ninth Circuit's final *en banc* opinion does not permit the issuance of the warrant the government seeks in this case for four reasons. First, although the five guidelines are no longer mandatory, the majority did not hold magistrate judges are prohibited from employing them or that they are improper or inappropriate. Rather the Court, exercising its independent judgment, as it must, has arrived at the conclusion that some of the guidelines should be applied based on the specifics of the present case.[FN9] *See id.* at 1178 (Kozinski, C.J., concurring). It is also important to note that the Court does not and will not robotically apply the five guidelines. For example, the Court is satisfied, in this particular case, that the fifth guideline's concern is met by the government's representations that it will return the devices unless they are found to be instrumentalities of the criminal offenses named in the warrant.

***11** Second, the warrant application in *CDT III* was drafted in a manner designed to ensure that it would be lawful and comport with the requirements of the Fourth Amendment. The warrant contained a panoply of safeguards absent here. As the Ninth Circuit stated "the magistrate judge ... wisely made such broad seizure subject to certain procedural safeguards." *CDT III,* 621 F.3d at 1168. Germane to the present case, these safeguards included: (1) that investigative agents not review and segregate the data; (2) that specialized forensic computer search personnel review and segregate the data and not give it to the investigative agents; and (3) seized evidence outside the scope of the warrant be returned within 60 days.

The *CDT III* court endorsed these safeguards noting that the government's argument the investigative agents could access all data seized is nothing but "sophistry." *Id.* at 1172. As the Court stated, "it would make no sense to represent that computer personnel would be used to segregate data if investigative personnel were also going to access all the data seized. What would be the point?" *Id.* The court found the government's failure to follow this procedural protection to reach information not covered by the warrant was a "callous disregard of the Fourth Amendment," not only because of the binding findings of the district court, but also as matter of "simple common sense." *Id.*

Hence, there is nothing in *CDT III* indicating it is unwise for a magistrate judge to require the warrant application contain such safeguards where requests for broad computer searches are made, that such safeguards are inappropriate, or that once such safeguards are ordered, it is permissible for the government to ignore them. These safeguards are particularly appropriate in this case. According to the affidavit, the target of the search is a disabled man who conducts business out of his home. There is no evidence he is using the computer to create illegal copies, but the computer is likely to store information regarding his supplier, customers and financial transactions. There is no suggestion that utilizing a filter team in this investigation would compromise the government's ability to prosecute this case. There is no suggestion that requiring waiver of the plain view doctrine as a *quid pro quo* for the evident over-seizing will compromise the government's ability to prosecute this case.

In contrast to the warrants issued in *CDT III,* the government, here, applies for the broadest warrant possible-the authority to search every single thing-but minus any of the

procedural safeguards the Ninth Circuit in *CDT III* deemed to be wise. Perhaps the government believes that its promise to use "only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized" is a sufficient safeguard. Larson Aff. ¶ 46(d). However, such protection is illusory and does not justify the government's request to conduct a search without a filter team and to rely on the plain view doctrine. Once the Court authorizes the government to search all data, the government can, and will.

12 Third, the *CDT III* opinion rejected the government's arguments that under *United States v. Tamura,* 694 F.2d 591 (9th Cir.1982), it did not have to return any data it found about baseball players outside the scope of the first warrant because that evidence was in "plain view" when agents examined the Tracey Directory. Calling this argument "too clever by half" the Ninth Circuit found the "point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search ... into a general search...." *CDT III,* 621 F.3d at 1170. The government's claim that everything is in "plain view" when it is given permission to search broadly would "make a mockery of *Tamura* and render the carefully crafted safeguards in the Central District warrant a nullity." *Id.* at 1171. Hence, while the *CDT III* majority opinion does not state the government in all cases "must foreswear reliance on the plain view doctrine," the opinion essentially requires as much.[FN10]

The instant warrant application goes a step beyond the position it took in *CDT III.* In this case, not only does the government fail to foreswear reliance on the plain view doctrine, it requests that it be allowed to seek a warrant that permits it to obtain a second warrant to seize additional evidence whether it was found in the initial search in plain view or not.

And fourth, the Ninth Circuit's "concluding thoughts" in *CDT III* put to rest any notion the warrant sought here is appropriate. Broad searches of ESI devices create "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1176. The Ninth Circuit further provided:

> Once a file is examined ... the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search some computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media.
>
> ...
>
> ... It is not surprising, then, that all three of the district judges below were severely troubled by the government's conduct in this case. Judge Thomas, too, in his panel dissent, expressed frustration with the government's conduct and position, calling it a "breathtaking expansion of the 'plain view' doctrine, which clearly has no application to intermingled private electronic data.

...

> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

***13** *Id.* at 1176-77.

In this case, the Court finds that the requested warrant application impermissibly grants the government a general or overbroad search warrant in violation of the Constitution and the law of the Circuit. The Court also reaches this conclusion while recognizing that quite often, broad searches of digital devices and "over-seizing is an inherent part of the electronic search process." [FN11] However, a balance must be struck between the government's investigatory interests and the right of individuals to be free from unreasonable searches and seizures. Few computers are dedicated to a single purpose; rather, computers can perform many functions, such as " 'postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.' " *United States v. Andrus,* 483 F.3d 711, 718 (10th Cir.2007) (citing Orin S. Kerr, Searches and Seizures in the Digital World, 119 Harv. L.Rev. 531, 569 (2005)). Almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. To maintain the balance between the government's investigatory interests and the Fourth Amendment, the Court is ready to grant the government's instant application on the conditions set forth in this opinion. But the government, much like it did in the *CDT* line of cases, does not seek to perform the search with constitutional safeguards, i.e., a filter team or foreswearing reliance on the plain view doctrine. The government's warrant application therefore does not pass Constitutional muster, and cannot be squared with the Ninth Circuit's opinion in *CDT III.*

E. *The Fourth Amendment and Use of "Hash Values"*

The instant warrant search protocol also purports to authorize the government to use hash values to perform the search. The government's proposed use of hash values does not necessarily narrow the scope of the search requested. Specifically, although "hash values" can be used to exclude files that do not interest the government such as a digital device's operating system, they can also be used to search and find evidence outside the scope of the warrant automatically and systematically. This is because most law-enforcement forensic software can automatically search for evidence of other crimes, such as child pornography, based on known hash values. *See United States v. Mann,* 592 F.3d 779, 783-84 (7th Cir.2010) (detective ignored warrant limitations and conducted

general search using Forensic Tool Kit (FTK) and its accompanying "KFF alert system" to locate child pornography).

The instant warrant application proposes to use "hash values," but contained no restrictions on that use, allowing the government to search for evidence of crime for which is lacks probable cause, such as child pornography. Moreover, the warrant affidavit does not demonstrate "hash values" exist that can be used to ferret out the evidence for which the government has probable cause in this case. The Court concludes that the following language must be added to the instant warrant application in order to address the problems with using hash values:

14 However, these methodologies, techniques and protocols will not include the use of "hash value" libraries to search the electronically stored information for items that are not set forth in the items authorized to be seized in Attachment B of this warrant.

As this new language is necessary to address both the scope and reasonableness of the search the conduct seeks to conduct, it must be included in the government's ESI application.

III. CONCLUSION

This Court is required under the U.S. Constitution and the law of the Circuit to deny the instant warrant application. Counterfeiting products is a serious crime and costs American intellectual property owners billions of dollars annually, results in lost jobs, and creates substantial threats to consumers of these products. Probable cause exists to search Mr. Cunnius' digital devices for evidence relating to counterfeit products. But the government asks the Court to do what the law does not permit. The government would have the Court give it the authority to scour all data contained in the seized digital devices, and more, without any of the procedural protections *CDT III* deemed both wise and necessary, and the authority to obtain a second warrant to seize any other data found outside the scope of the first warrant whether it was found in plain view or not. This request is exactly what *CDT III* prohibited: "the process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1177. Moreover, if the Court sanctions this action, its decision effectively becomes non-reviewable. *See United States v. Leon,* 468 U.S. 897 (1984).

CDT III provided strong guidance to this Court regarding ESI searches. While the guidelines are not mandatory, most are appropriately required in this case. The government may disagree with the decision enunciated in *CDT III.* The government's options, however, are to seek review of *CDT III* with the U.S. Supreme Court or to comply. Neither the government nor this Court has the option to pretend that *CDT III* does not exist. Because the Court finds the government's warrant application, without the protections set forth in this Order, fails to comply with the Fourth Amendment and the law of this Circuit, the Court DENIES the government's application for a search warrant.

As this matter involves an on-going criminal investigation, the Clerk of Court is directed to file this Order under seal. This Order will be unsealed at the earlier of when any warrant relating to this matter is executed, or when a decision is made not to proceed with the prosecution of the matter, or otherwise by written order. A copy of this Order shall also be provided to the United States and the assigned United States District Judge.

FN1. "Digital devices" is defined in the warrant affidavit to include any electronic device capable of processing or storing data in digital form. Larson Aff. ¶ 37 n. 1; Larson Warrant App., Att. B, ¶ 2.

FN2. The Court is prepared to authorize the search of the residence. This opinion focuses on the search of digital devices contained in the residence. There are other changes to the warrant regarding hash values that would be required, as discussed in Part II Section E of this opinion. The Court does not understand the government to have objections to these changes, but if this is not the case, the government should address the issue in its appeal.

FN3. The Fourth Amendment's prohibition on the issuance of general warrants goes hand in hand with the requirement that each search must be carefully tailored to its justifications. Hence, even if a warrant is not an impermissible general warrant, it still cannot be granted unless it is carefully tailored to its justification.

FN4. The Ninth Circuit's initial panel decision is found at *Comprehensive Drug Testing v. United States,* 473 F.3d 913 (9th Cir.2006). This panel decision was withdrawn and superseded by *Comprehensive Drug Testing v. United States,* 513 F.3d 1085 (9th Cir.2008) (" *CDT I* "). The Ninth Circuit then granted rehearing *en banc, Comprehensive Drug Testing v. United States,* 545 F.3d 1160 (9th Cir.2008), and issued its first *en banc* decision at *Comprehensive Drug Testing v. United States,* 579 F.3d 989 (9th Cir.2009) (" *CDT II* "). The initial *en banc* decision was then revised and superseded by *CDT III,* 621 F.3d 1162.

FN5. "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet. A cloud platform can either be external or internal. An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google. This software-as-a-service allows individuals and businesses to collaborate on documents, spreadsheets, and more, even when the collaborators are in remote locations. By contrast, an internal or private cloud is a cluster of servers that is networked behind an individual or company's own firewall." David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing,* 93 MINN. L. REV. 2205, 2216 (2009) (internal citations omitted).

FN6. The Ninth Circuit has defined "downloading" as "the act of manually storing a copy of an image on the hard drive for later retrieval." *U.S. v. Romm,* 455 F.3d 990, 994 n. 3 (9th Cir.2006). *See also U.S. v. Mohrbacher,* 182 F.3d 1041, 1045-46 (9th Cir.1999) (describing downloading).

FN7. Some of these baseball players were included in the warrant, some were not.

FN8. One judge allowed the government to retain the materials regarding the ten players identified in the initial warrant. The subpoenas at issue were also quashed.

FN9. Parenthetically, the Court notes the distinction between searching a "third party" computer, as was the case in *CDT III,* and searching a suspect's computer, would be a distinction without a difference. First, the Ninth Circuit stated *CDT III* was "more generally ... about the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information," not about searches of a third party computer. *CDT III,* 621 F.3d at 1165-66. Second, in rejecting the government's argument that it could seize items in "plain view," the Court gave several examples including: "Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been." *Id.* at 1171. In giving this example, the Court cited to *United States v. Hill,* 322 F.Supp.2d 1081 (C.D.Cal.2004), a case involving the search of an individual's computer and residence. *Id.* And third, in *CDT III's* "concluding thoughts" section, the Ninth Circuit stated that a broad computer search "calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the ***right of individuals*** to be free from unreasonable searches and seizures." *Id.* at 1177 (emphasis added).

FN10. The Court notes a generalized seizure of ESI would be justified where there is probable cause to conclude that the entirety of the contents of the ESI device is evidence of crime. *Cf. United States v. Kow,* 58 F.3d 423, 427 (9th Cir.1995) ("A generalized seizure of business documents may be justified if the government establishes probable cause to believe the entire business is merely a scheme to defraud or that all of the business's records are likely to evidence criminal activity."). Here, the government has not presented any evidence that in this case, Mr. Krause's ESI devices contain only evidence of criminal activity.

FN11. *CDT III,* 621 F.3d at 1177.