**Is the Particularity Requirement of the Fourth Amendment Particular Enough for Digital Evidence?**

*Major Paul M. Ervasti*[*]

*The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement [of the Fourth Amendment] that much more important.*[1]

## I. Introduction

Almost ninety years ago, Judge Learned Hand said that "[i]t is a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him."[2] Today, the typical computer or cell phone contains far more private information about a person than would have ever been found in a person's house.[3] A modern cell phone will contain internet browsing history, historical Global Positioning System (GPS) information about where a person is and was located, and a wealth of application "which together can form a revealing montage of the user's life."[4] Because of this, a search of a person's cell phone would likely be much more intrusive than even the most exhaustive search of a person's home.[5] Therefore, courts have struggled to strike a balance in applying the particularity requirement of the Fourth Amendment in such a way as to allow legitimate government searches of digital evidence, while still preventing the type of general ransacking of a person's effects that the framers of the Constitution sought to prevent.

In striking that balance, courts recognize the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[6] They have sought to keep the particularity requirement relevant in a digital context by imposing two different restrictions. First, some courts have required an affidavit supporting a search authorization to list the specific keywords or methods that will be used to search the numerous files and folders for evidence of a crime.[7] Second, other courts have focused on the subjective intent of the searchers. Those courts require law enforcement to obtain a new search authorization once they uncover evidence of an unrelated crime and subjectively change the focus of their search.[8]

This article first examines why digital searches are necessarily broad by their very nature. Files are easily mislabeled and hidden. Because evidence could be stored anywhere on a computer, a thorough search usually requires examining every file and folder. Next, the article analyzes the two ways courts have interpreted the particularity requirement—requiring keywords or search protocols and requiring a new warrant when the subjective intent of the searcher changes. Neither of these two methods works well in practice. Requiring law enforcement to specify keywords or search methodologies in order to prevent them from viewing files outside the scope of their search is unworkable. A searcher cannot know beforehand how files will be labeled and stored. Additionally, that level of specificity in how the search will be carried out is not mandated by the Constitution; neither should the subjective intent of the searcher matter. Since the original search usually requires examining every file on a piece of digital evidence, the scope of the search does not expand simply because an agent subjectively hopes to find evidence of an unrelated crime.

All of these inherent tensions in how the particularity requirement should be applied in a digital context were illustrated in the Navy-Marine Corps Court of Criminal Appeals in *United States v. Tienter*.[9] In *Tienter*, the court determined that the search of LCpl Tienter's cell phone was unreasonable under the Fourth Amendment because the scope of the search exceeded that which had been authorized

---

[*] Judge Advocate, United States Marine Corps. J.D., 2007, University of Minnesota; B.A., 2000, Saint Cloud State University. Previous assignments include Appellate Government Counsel, Navy-Marine Corps Appellate Review Activity, Washington Navy Yard, 2011-2014; Battalion Judge Advocate, 3d Battalion, 3d Marines, Helmand Province, Afghanistan, 2010; Deputy Staff Judge Advocate, 3d Marine Division, Okinawa, Japan, 2009-2010; Trial Counsel, Legal Services Support Section, Okinawa, Japan, 2007-2009; Platoon Commander, 2d Military Police Battalion, Camp Lejeune, North Carolina, 2003-3004; Operations and Services Officer, Provost Marshal's Office, Marine Corps Air Station, New River, North Carolina, 2001-2003. Member of the bars of Minnesota, the Court of Appeals for the Armed Forces, and the Supreme Court of the United States. This article was submitted in partial completion of the Master of Laws requirements of the 63rd Judge Advocate Officer Graduate Course.

[1] United States v. Burgess, 576 F.3d 1078, 1090-91 (10th Cir. 2009) (quoting United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)).

[2] Riley v. California, 134 S. Ct. 2473, 2490-91 (2014) (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

[3] Riley, 134 S. Ct. at 2490-91.

[4] *Id.*

[5] *Id.*

[6] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

[7] *See Id.*; United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); United States v. Osorio, 66 M.J. 632, 637 (A.F. Ct. Crim. App. 2008); *See also* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. & Tech. 75, 107 (1994) (advocating for an interpretation of the particularity requirement, which would require law enforcement to list keyword methods and search protocols when they apply for a warrant to search digital evidence).

[8] *See* Carey, 172 F.3d at 1275; United States v. Tienter, No. 201400205, 2014 CCA LEXIS 700 (N-M. Ct. Crim. App. Sep. 23, 2014).

[9] Tienter, 2014 CCA LEXIS 700.

in the search authorization.[10] The Criminal Investigative Division (CID) obtained authorization to seize LCpl Tienter's phone because there was probable cause to believe the phone contained text messages, which were evidence that another Marine had solicited LCpl Tienter to distribute a controlled substance.[11] The CID Special Agent said in the affidavit supporting the authorization that "search protocols directed exclusively to the identification and extraction of data within the scope of this warrant" would be used to analyze the data contained in the cell phone.[12]

LCpl Tienter was also the suspect in an unrelated sexual assault at the time CID seized his phone.[13] After the search, the government extracted the text messages on the phone into one 2,117 page Portable Document Format (PDF) file.[14] Later, the CID Special Agent (with the help of the Naval Criminal Investigative Service (NCIS) Special Agent working the sexual assault case) searched through that document using search terms associated with the sexual assault and unrelated to the drug offenses.[15]

Like in *Tienter*, most searches of computers or cell phones give law enforcement access to a vast amount of personal information unrelated to the original reason for the search. Courts have recognized that digital searches often require opening and examining many seemingly unrelated files. "The legitimate need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence, is one we've often recognized."[16] But these broad searches raise important questions about how the particularity requirement of the Fourth Amendment, which normally limits the scope of a search, should apply in a digital context. "Because computers typically contain so much information beyond the scope of the criminal investigation, computer-related searches can raise difficult Fourth Amendment issues different from those encountered when searching paper files."[17] "For example, officers searching a computer for a telephone number may use the opportunity to rummage through financial records, written correspondence, electronic mail, or other obviously personal and irrelevant records also contained on the computer."[18]

With that in mind, when the search is for digital evidence, should law enforcement be required to specify how the search will be conducted? The Fourth Amendment requires law enforcement to specify what they are looking for and what they intend to seize. In a digital context, should they also be required to specify what search protocols and what key words they will use when they are conducting their search? Does the subjective intent of the searcher matter? For example, in LCpl Tienter's case, should it matter whether law enforcement subjectively searches for evidence of a sexual assault or whether they merely continue a methodical search for drug evidence, knowing that they are likely to find evidence of a sexual assault?

In *Tienter*, searching through the extracted data to look for evidence of a sexual assault should not have raised any additional constitutional concerns because the agents were already authorized to look at every text message within the scope of the original search. Examining that same data to look for evidence of another crime did not expand the scope of the search or involve any additional invasion of privacy.

## II. Background

### A. The Particularity Requirement of the Fourth Amendment

This section briefly explains the origin of the particularity requirement and its intended purpose. The Fourth Amendment of the Constitution of the United States protects against unreasonable searches and seizures and provides that "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."[19] The drafters of the Bill of Rights intended this Amendment to prevent the issuance of writs of assistance or general search warrants.[20] The drafters, who lived under Colonial British rule, considered general search warrants to be particularly offensive to individual liberty because those types of warrants allowed the government to enter a citizen's home and go through all of the citizen's private papers and effects in search of anything that might incriminate him.[21] Thus, the requirement that a search warrant describe the place to be searched and the things to be seized with "particularity" prevents a search warrant from becoming a general warrant used to look for any incriminating evidence that might be found.[22]

---

[10] *Id.* at *3, 11.

[11] *Id.* at *2-3.

[12] *Id.* at *3.

[13] *Id.* at *4-5.

[14] *Id.* at *3, 11.

[15] *Id.* at *4-5.

[16] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (citing United States v. Hill, 459 F.3d 966 (9th Cir. 2006)).

[17] United States v. Hill, 459 F.3d 966, 968 (9th Cir. 2006).

[18] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. & Tech. 75, 86 (1994).

[19] U.S. CONST. amend. IV.

[20] Boyd v. United States, 116 U.S. 616, 625-26 (1886).

[21] Frank v. Maryland, 359 U.S. 360, 363-65 (1959); Boyd v. United States, 116 U.S. 616, 625-26 (1886).

[22] *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 7-9 (1977); Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

The particularity requirement works well to prevent overly broad searches when the search is of a physical space. Because the Fourth Amendment forces the government to describe with particularity what it is searching for and what it intends to seize, it therefore limits the scope of the search to places where there is probable cause to believe the evidence could be located.[23] The following quote from the Supreme Court illustrates how the particularity requirement limits the scope of a physical search:

> Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.[24]

Thus, in a physical search context "[t]he particularity requirement ensures that a '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.'"[25]

B. The Particularity Requirement Applied to Digital Searches

The particularity requirement, as normally interpreted, does not limit the scope of a digital search in the same manner as a physical search, because digital evidence could be anywhere on a computer. To meet the particularity requirement in a digital search, "warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material."[26] It is not enough for a warrant to authorize seizure of a computer without specifying that certain files on the computer are likely to contain evidence of a specific crime.[27] But doing so does not limit the scope of a search for digital evidence on a computer or cell phone in the same manner that it does during a physical search. Not only could files be stored anywhere on the computer, but they might also be intentionally hidden or mislabeled. For example, nothing prevents a savvy criminal from storing digital records of a stolen lawnmower in a folder labeled "upstairs bedroom." "Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality."[28] Because digital files are so easily mislabeled, hidden, or deleted, many courts have recognized that any thorough search for digital evidence requires "at least a cursory review of each file on the computer."[29]

But this need for at least a cursory review of each file risks turning every digital search into a general search in which law enforcement may examine every aspect of a person's life for evidence of any criminal activity.[30] Once it is established that a thorough search requires opening and looking at every file—even those that are seemingly unrelated to the object of the search—then any other unrelated incriminating evidence discovered would likely be lawfully obtained under the "plain view" doctrine.[31] An analysis of the plain view doctrine is beyond the scope of this article. However, the doctrine does create tension in a digital context that is greater than in a physical search context. If law enforcement may lawfully examine every file on a computer, then under the plain view doctrine there is no reason that they should have to turn a blind eye to evidence of other crimes that they happen to see. Courts either accept the fact that searches of digital evidence will necessarily be very broad or they find some other way to limit the scope of a search.

The way courts have struck the balance is through applying the particularity requirement differently in a digital context. They either (1) require a particular description of the types of files sought or the manner in which the search is to be conducted by requiring keywords or search protocols; or (2) decide whether the warrant sufficiently described the "things to be seized"[32] by analyzing the subjective intent of the officer. That is, they look at what the officer's subjective intent was as evidenced by the search terms and methods he used to search the computer rather than looking at whether the officer was searching in a place that the evidence was

---

[23] Maryland v. Garrison, 480 U.S. 79, 84-85 (1987).

[24] United States v. Ross, 456 U.S. 798, 824 (1982).

[25] Winick, s*upra* note 18, at 86 (quoting Maryland v. Garrison, 480 U.S. 79, 84 (U.S. 1987)).

[26] United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005).

[27] *Id.*

[28] United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010).

[29] *Id*.; *See also* United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("There is no way to know what is in a file without examining its contents . . . .").

[30] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) ("This pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.").

[31] *See, e.g.*, United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (applying plain view doctrine in digital context); United States v. Upham, 168 F.3d 532 (1st Cir. 1999) (also applying plain view doctrine in digital context); United States v. Fogg, 52 M.J. 144, 149 (C.A.A.F. 1999) (general discussion of plain view doctrine); Mil. R. Evid. 316(d)(4)(C). As will be discussed later, although some courts disagree on whether a search of digital evidence should allow the police to open and view every file or whether some limiting techniques should be used, it is undisputed that if the police do have a lawful purpose to examine a file and immediately recognize evidence of a different crime, the plain view doctrine would apply. *See infra* note 92 and accompanying text.

[32] U.S. CONST. amend. IV.

likely to be found. Both of these interpretations of the particularity requirement will now be analyzed in turn.

## III. Keywords or Other Search Protocols as a Method to Prevent General Searches

### A. The Case for Keywords—No Generalized Rummaging Allowed

#### *1. Introduction*

The Fourth Amendment "does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'"[33] "Although the particularity requirement compels government officials to specifically define the place to be searched and the anticipated fruits of the search, the requirement has never been applied to how the search will be carried out."[34]

But in a digital context, requiring greater specificity in how the digital evidence will be analyzed could be a way to prevent a wide-ranging generalized rummaging through a person's digital life. Requiring officers to specify how they intend to analyze the digital evidence recognizes that "over-seizing is an inherent part of the electronic search process" and that therefore searches of electronic records call 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."[35] "Reinterpreting the Fourth Amendment to require ex ante search protocols in the computer search context may provide the means to safeguard the huge amounts of information stored on individual hard drives."[36]

#### *2.* Comprehensive Drug Testing, Inc.

One example of this approach is in the Ninth Circuit's case of *United States v. Comprehensive Drug Testing, Inc.*[37] In that case, the United States had a warrant to seize the drug testing records of ten Major League Baseball players from a drug testing laboratory.[38] But when agents executed the warrant, they seized the records of hundreds of other players as well as many other individuals.[39] The warrant contained "significant restrictions on how the seized data were[sic] to be handled" which were generally designed to keep law enforcement agents from viewing records of other individuals that were unrelated to the ten players for which the warrant was issued.[40] One of the restrictions in how the search was to be carried out required computer personnel to conduct a preliminary screening of the records, to see which ones were relevant, and return the unrelated records to the laboratory before they were seen by the investigating case agents.[41] However, the investigating agents did not comply with those particularized requirements that specified how to conduct the search. Instead, the investigating agents reviewed many unrelated records of other players and uncovered evidence of drug use in those unrelated records.[42] When the government later tried to argue that the evidence of the other unrelated crimes was in plain view, the court rejected that argument and found that they had exceeded the limitations in the warrant which specified how the search was to be conducted.[43] The court held that the magistrate judge's restrictions on how the search was to be conducted struck a proper balance in protecting the privacy rights of other persons whose records were stored at the laboratory, for which the government did not have probable cause.[44]

Writing in concurrence, Chief Judge Kozinski wanted to more explicitly create a future rule for how searches of digital evidence are to be conducted.[45] He wanted to require, among other things, that digital searches require greater particularity in how the search is to be conducted. "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."[46]

Both the majority and the concurrence in *Comprehensive Drug Testing, Inc.* recognized the danger that a digital search can turn into an overly broad general search. Simply applying a normal search paradigm to this situation does not work. It is not enough to simply say that law enforcement has probable cause to search the digital records of the laboratory for records related to ten players, and that law enforcement may look anywhere that those records could be found because the digital records of those ten players could be located in any file or folder on the

---

[33] United States v. Grubbs, 547 U.S. 90, 97 (2006).

[34] Marc Palumbo, Note, *How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 Fordham Urb. L.J. 977, 984 (2009).

[35] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177.

[36] Palumbo, *supra* note 34.

[37] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1162.

[38] *Id.* at 1165.

[39] *Id.*

[40] *Id.* at 1168-69.

[41] *Id.*

[42] *Id.*

[43] *Id.* at 1176-77.

[44] *Id.*

[45] *Id.* at 1178-80 (Kozinski, C.J., concurring).

[46] *Id.* at 1180 (Kozinski, C.J., concurring).

laboratory's hard drives. So something more is required to "[strike] a proper balance" to protect the privacy rights of persons whose records were unrelated to the search.[47] The method that the Ninth Circuit used to strike that balance—requiring more particularity in how the search is conducted and not allowing the government to expand the scope of the search methodology—is a method particularly suited to digital searches but it is not a new approach.

*3. Comingled Records*

In many ways, the Ninth Circuit did not create new law in *Comprehensive Drug Testing, Inc.*. Rather, the court simply applied earlier case law dealing with comingled records to a new digital context. In finding that the officers exceeded the scope of the search, the court relied heavily on its own "venerable precedent" dealing with comingled paper records.[48]

In *Tamura*, the government had a warrant to seize employment records related to one individual but was forced to seize many other unrelated records involving other individuals due to the records being so intermingled that sorting through the records on site to determine which ones were relevant would not have been possible.[49] The court created a framework for situations where the government is forced to seize more records than are authorized in the warrant. In those cases, the government may seize unrelated documents under conditions that later examination of those documents will be completed in accordance with methods established by the magistrate.[50] The "essential safeguard" in these situations is the judgment of a neutral, detached magistrate who will monitor the seizure of the unrelated documents and the government's treatment of them.[51]

The Supreme Court also recognized in *Andresen v. Maryland* that the seizure of unrelated comingled documents does not necessarily turn an otherwise valid warrant into an impermissible general warrant.[52] That case dealt with the seizure of specific documents related to a fraudulent real estate transaction from a lawyer's office.[53] In dicta, the Court recognized the "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."[54] The Court went on to recommend a procedure similar to what the Ninth Circuit adopted in *Tamura*, where law enforcement officials conduct a cursory review of documents under a process that is supervised by a judicial officer and "conducted in a manner that minimizes unwarranted intrusions upon privacy."[55]

The challenge of digital searches is that based on the amount of private data on most computers and cell phones, every search now involves the same problems as comingled records searches. The framework for dealing with comingled records demonstrated in *Tamura* and *Comprehensive Drug Testing, Inc.* makes sense when the records are completely separate, involve different individuals, and only happen to be stored at the same location. For example, probable cause to search and seize packages belonging to a suspect that happen to be at a post office has never carried with it the authority to seize and open all the other packages of everyone else that happen to also be there. That basic assumption should not change simply because instead of packages, the relevant evidence is now digital files that happen to be stored on the same server or computer hard drive. So it seems relatively straight forward to say in *Comprehensive Drug Testing, Inc.* that when the government has probable cause to seize drug testing records from ten specific individuals, it should not open and examine the records of hundreds of other unrelated individuals simply because those records happen to be stored in the same place.

It would be a far different matter when all the evidence or records belong to the same person. For example, if law enforcement has probable cause to search a person's bedroom for a certain piece of evidence, they could search anywhere in the bedroom where the evidence could be located. No court would dictate that the searchers develop search methods and protocols that would only allow them to see the type of evidence they were looking for but nothing else. In essence, it is a far different thing to suggest that law enforcement should have to wear blinders that only allow them to see exactly what they are looking for. But Chief Judge Kozinski's concurrence in *Comprehensive Drug Testing, Inc.* would require just that: "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."[56] As discussed in the next section, at least some courts have agreed.

---

[47] *Id.*

[48] *Id.* at 1167 (citing United States v. Tamura, 694 F.2d 591 (9th Cir. 1982)).

[49] United States v. Tamura, 694 F.2d 591, 594-96 (9th Cir. 1982).

[50] *Id.*

[51] *Id.* at 596.

[52] *See* Andresen v. Maryland, 427 U.S. 463 (1976).

[53] *Id.* at 479-83.

[54] *Id.* at 482 n.11.

[55] *Id.*

[56] United States vs. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, C.J., concurring).

*4. Requiring Greater Particularity Outside of a Comingled Records Context*

At least one district court has held that because of the privacy concerns involved in searching through a vast amount of private information on a person's computer that "prior to allowing any search of the contents of the computers, the court would require the government to provide a protocol outlining the methods it would use to ensure that its search was reasonably designed to focus on documents related to the alleged criminal activity."[57] The court required such a search protocol to prevent the search from becoming a generalized rummaging through all other private matters contained on the computer and to ensure that law enforcement instead searched for only the type of documents specified in the warrant.[58] The court reasoned that such restrictions on the manner in which the search was conducted were necessary to apply the particularity requirement to a digital context.[59]

Likewise, the Tenth Circuit also reasoned that the "storage capacity of computers requires a special approach" to the particularity requirement of the Fourth Amendment.[60] In *United States v. Carey*, the court stated that in most digital searches any "investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other."[61] Probable cause to search financial records contained in spreadsheets would not, under the court's view, grant any authority to view other types of files, telephone lists or word documents "absent a showing of some reason to believe that these files contain the financial records sought."[62] The court also stated that magistrates "should review the search methods proposed by the investigating officers" to prevent digital searches from becoming impermissible general searches.[63]

The court based its "special approach" to the particularity requirement in large part on a law review article by Raphael Winick.[64] Perhaps the strongest rationale for this approach comes from Winick himself:

> Once computer data is removed from the suspect's control, there is no exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant. After law enforcement personnel obtain exclusive control over computer data, requiring them to specify exactly what type of files will be inspected does not present any undue burden. A neutral magistrate should determine the conditions and limitations for inspecting large quantities of computer data. A second warrant should be obtained when massive quantities of information are seized, in order to prevent a general rummaging and ensure that the search will extend to only relevant documents.[65]

At least one military court appears to have adopted this approach.[66] Whether requiring greater particularity in a warrant by requiring law enforcement personnel to specify in advance what type of files they are looking for and how the digital search will be conducted really does not present "any undue burden" is something that numerous other courts have disagreed with.

B. The Case Against Keywords—Open Every File

*1. Suspects Easily Hide or Mislabel Computer Files*

Most courts have differed from *Carey's* "special approach" to the particularity requirement in two different ways. First, they reject the idea that probable cause to search a computer could be limited to certain types of files. Second, they do not require any sort of pre-approved search protocol dictating how the search will be conducted.

---

[57] In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004).

[58] *Id.* at 954-56.

[59] *Id.* at 954 ("The degree of particularity that is required for search warrants under the Fourth Amendment in any given situation may not be determined by resorting to some simple formulaic approach, but instead varies depending on the circumstances of the case and the types of items involved. The search and seizure of a computer requires careful scrutiny of the particularity requirement."). However, at least one other district court in the same jurisdiction has since questioned whether the particularity requirement in fact demands such a description of how a digital search is to be carried out. *See* United States v. Gocha, 2007 U.S. Dist. LEXIS 58962, at *18-20 (N.D. Iowa, Aug. 10, 2007) (rejecting the reasoning in *West End* and finding that the particularity requirement does not require a description of how the electronic search will be conducted because when officers apply for authorization to search, it is often impossible for them to not know "the particular electronic format in which the evidence may be maintained by the suspect" and they therefore cannot reasonably know what search methods they will use).

[60] United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).

[61] *Id.* at 1275 n.8.

[62] *Id.*

[63] *Id.*

[64] *Id.* at 1275-76 (citing Winick, *supra* note 18, at 86).

[65] Winick, *supra* note 18, at 107.

[66] United States v. Osorio, 66 M.J. 632, 637 (A.F.C.C.A. 2008) (citing *Carey* approvingly and holding that "when dealing with search warrants for computers, there must be specificity in the scope of the warrant which, in turn, mandates specificity in the process of conducting the search. Practitioners must generate specific warrants and search processes necessary to comply with that specificity and then, if they come across evidence of a different crime, stop their search and seek a new authorization.").

The court in *Carey* claimed that any reasonable investigator could differentiate between spreadsheets, word documents, and video files, and that therefore probable cause to search for financial records stored in an excel format would not constitute probable cause to open other types of files such as word documents.[67] The Ninth Circuit issued *Carey* in 1999. No doubt, the judges felt themselves computer savvy and were probably quite proud of being able to distinguish a file with a Microsoft Excel file format (.xls) extension from one with a document file format (.doc) extension. But in spite of what many judges believe, they "are not skilled computer forensic experts" and "[l]ike most lawyers, they tend to have only a vague sense of the technical details of how computers work."[68] The *Carey* court probably did not understand how easy it is to change a file to make it appear like something else.

That is why other courts have not adopted the reasoning of the court in *Carey* and imposed similar restrictions. Because digital files are so easily mislabeled, hidden, or deleted, many courts have recognized that any thorough search for digital evidence requires "at least a cursory review of each file on the computer."[69] So *Carey's* "special approach" to particularity—where probable cause to search for financial information in a spreadsheet would not allow the police to open a word document—would be similar to saying that when the police have probable cause to seize cocaine, they may not seize a "plastic bag containing a powdery white substance" simply because the suspect wrote "flour" or "talcum powder" on the bag.[70]

*2. Searching is an Art, Not a Science*

Most courts have likewise not required search warrants to contain search protocols or other particularized descriptions of how the search is to be carried out. A "search warrant itself need not contain a particularized computer search strategy."[71] That is because "[w]arrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible."[72] Although police know that they are looking for evidence of a crime on a computer, they often do not know what operating system the suspect uses, what, if any encryption is used, how the files are titled, where they are stored, or hundreds of other details that impact how they analyze the computer for evidence. This makes it nearly impossible for investigators to know the particular search process they will use when they apply for a warrant.[73]

Even if law enforcement officers could describe the particular search process they planned on using in advance, "[l]imitations on search methodologies have the potential to seriously impair the government's ability to uncover electronic evidence."[74] The use of code words, aliases, short-hand jargon, abbreviations, or even simple misspellings might prevent the police from finding relevant evidence if they are limited to searching for pre-approved keywords.[75] "Every Westlaw or LEXIS user is familiar with the difficulty of crafting search terms that find the correct case on the first try; requiring a forensic investigator to find crucial evidence with a keyword search specified prior to forensic analysis is just as impractical."[76] For that reason, the Department of Justice (DOJ) Manual recommends not placing any restrictions on the manner in which the search will be conducted in the warrant itself.[77]

Additionally, placing detailed descriptions of computer search methodologies in warrant applications forces magistrates to become computer forensics experts, a job they are poorly qualified for.[78] Rather than have magistrates dictate to the government ex parte[79] the exact search process

[67] United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).

[68] Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 575 (2005).

[69] United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010); *See also* United States v. Stabile, 633 F.3d 219, 237 (3rd Cir. 2011) ("[I]t is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required."); United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) (relevant files are often hidden, mislabeled, and manipulated to conceal their contents); United States v. Burgess, 576 F.3d 1078, 1092-94 (10th Cir. 2009) (examination of most files and folders is usually required in a digital search, and this does not make the search overly broad); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("There is no way to know what is in a file without examining its contents . . . ."); United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006) (evidence of financial crimes could be located anywhere on a hard drive, because files are easily concealed or mislabeled).

[70] United States v. Hill, 459 F.3d 966, 977-78 (9th Cir. 2006).

[71] United States v. Stabile, 633 F.3d 219, 238 (3rd Cir. 2011) (quoting United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005)).

[72] United States v. Adjani, 452 F.3d 1140, 1147-48 (9th Cir. 2006) (quoting United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)).

[73] Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 575 (2005) ("Nor will investigators necessarily know what forensic tool the analyst may use when performing his search. Different forensic tools have different features; tasks that may be easy using one program may be hard using another. It is difficult to know what the particular search requires and what tools are best suited to find the evidence without first taking a look at the files on the hard drive. In a sense, the forensics process is a bit like surgery: the doctor may not know how best to proceed until he opens up the patient and takes a look. The ability to target information described in a warrant is highly contingent on a number of factors that are difficult or even impossible to predict ex ante.").

[74] U.S. DEP'T OF JUSTICE , CRIMINAL DIV., COMPUTER CRIME & INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, 3rd Ed., 79 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual 2009.pdf [hereinafter DOJ MANUAL].

[75] *Id.* at 79-80.

[76] *Id.* at 79.

[77] *Id.* at 79-82.

[78] Kerr, *supra* note 68, at 575-76.

[79] *Id.* (noting that the warrant application process is ex parte by nature).

it should use, it is better to have judges simply decide later after hearing from the defense as well whether the government's search methods were reasonable.[80]

## IV. Subjective Intent—Does it Matter What the Searcher is Searching For?

### A. Normally it Does Not

"[A]n investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant."[81] "Thus, 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 it may be found."[82] The fact that an officer expects and intends to find a piece of evidence outside the scope of the warrant does not invalidate the seizure so long as the officer has not expanded the search and is searching in an area where the original evidence was likely to be found.[83]

Under this view, if the police had a warrant to search a computer for files related to drug evidence, it would not matter if police suspected that child pornography was on the computer or even if police specifically opened certain files believing that they contained child pornography. So long as they were looking in files where the drug evidence might reasonably be located (which, as discussed earlier, might be anywhere on the computer), clicking on files indicative of child pornography with the specific intent to find child pornography would not be an unreasonable expansion of the search.[84]

### B. Should Subjective Intent Matter in a Digital Context?

Recognizing the potential that this doctrine will morph every digital search into a general search, some courts and commentators have recommended overturning *Horton*[85] and reinstating the inadvertence requirement for digital searches.[86] The rationale for this approach is that it protects individual rights by ensuring that the police do not circumvent the particularity requirement of the Fourth Amendment by intentionally searching for items not particularly described in a warrant.[87]

Requiring that unrelated evidence be discovered inadvertently is one way to ensure that the search is "directed in good faith toward the objects specified in the warrant."[88] This seems to be the concern of the Navy-Marine Corps Court of Criminal Appeals in *Tienter*. The court found it fundamentally different to inadvertently stumble across incriminating evidence of the sexual assault while searching through over 2,000 pages of documents related to the drug offenses, than to use specific search words tailored to find evidence of the sexual assault in those same documents.[89]

But whether the incriminating evidence was stumbled upon should not have mattered nor would it in a typical physical search. For example, if a police officer has authorization to open 100 boxes in a person's house to search for drugs, it would not matter if the officer only sought out and opened the one box that the officer subjectively believed contained child pornography. So long as the officer was looking in a place that the warrant allowed him to look, he would not be impermissibly expanding the scope of the search. But the court in *Tienter* rightly recognized that this analogy falls apart in a digital context. For example, if instead of 100 boxes, the room contained billions of boxes and the police never intended on opening and viewing all of them without the aid of some narrowing search criteria, then the search criteria they use should have to be related to the object of the search. If the police in *Tienter* had obtained authorization to search the computer for evidence of drug crimes, but then immediately started searching the hard drive for files related to the sexual assault, then this does seem to circumvent the whole purpose of the particularity requirement. And this is true even though the police might have otherwise had authority to open every file and briefly examine it for drug evidence.

Critics of focusing on the officer's subjective intent usually point out how difficult it is to determine someone's subjective state of mind.[90] And officers may simply be trained to conduct more thorough searches.[91] For example, presumably nothing would have stopped the officer in

---

[80] DOJ MANUAL *supra* note 74, at 80.

[81] United States v. Stabile, 633 F.3d 219, 238 (3rd Cir. 2011) (citing Maryland v. Garrison, 480 U.S. 79, 84 (1987)); Horton v. California, 496 U.S. 128, 138 (1990) (reasonableness of search does not depend on the subjective state of mind of the officer).

[82] Maryland v. Garrison, 480 U.S. 79, 84 (1987) (quotations omitted).

[83] *See, e.g.*, United States v. Williams, 592 F.3d 511, 522-24 (4th Cir. 2010) (rejecting the requirement that evidence outside the scope of the warrant must be found inadvertently).

[84] *Id.* at 523; Horton, 496 U.S. at 138.

[85] Horton v. California, 496 U.S. 128, 138 (1990) (holding that the reasonableness of search does not depend on the subjective state of mind of the officer).

[86] *See* Nicholas Hood, *No Requirement Left Behind: The Inadvertent Discovery Requirement—Protecting Citizens One File at a Time*, 45 Val. U.L. Rev. 1529 (2011) (advocating that in a digital context, files outside the scope of the warrant should have to be discovered inadvertently).

[87] *Id.* at 1580.

[88] United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (quotations omitted).

[89] United States v. Tienter, No. 201400205, 2014 CCA LEXIS 700, *7 (N-M. Ct. Crim. App. Sep. 23, 2014).

[90] Kerr, *supra* note 68, at 578.

[91] *Id.*

*Tienter* from reading all 2,000 pages of text messages and then just happening to see the texts related to the sexual assault.[92]

## V. Conclusion

Courts have struggled to strike a balance between the legitimate government need to conduct a thorough search of digital evidence with the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[93] Courts have tried to strike that balance by restricting the broad nature of a search of digital evidence in two different ways. First, some courts have required an affidavit supporting a search authorization to list the specific keywords or methods that they will use to search the numerous files and folders for evidence of a crime. Second, other courts have focused on the subjective intent of the searchers and have required law enforcement to obtain a new search authorization when they uncover evidence of another crime and change the focus of their search.

In the end, neither of these two methods works particularly well. Requiring greater specificity in the warrant regarding how the search will be carried out is often impossible and does not work in practice. "Court-mandated forensic protocols are also unnecessary because investigators already operate under significant constitutional restrictions. In any search, 'the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.'"[94]

Because courts may assess whether the government's actions in conducting a search were unreasonable, there is no need to modify any of the particularity requirements of the Fourth Amendment for a digital context. The general requirement that any search be reasonable will already adequately uphold the Constitution and protect individual rights, without harming the legitimate law enforcement need for thorough digital searches.

---

[92] *See* DOJ MANUAL, supra note 74, at 91. ("Arguably, [the agent] could have continued his systematic search of defendant's computer files pursuant to the first search warrant, and, as long as he was searching for the items listed in the warrant, any child pornography discovered in the course of that search could have been seized under the 'plain view' doctrine.").

[93] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

[94] DOJ MANUAL, supra note 74, at 80 (quoting Dalia v. United States, 441 U.S. 238, 258 (1979)).