Why the Plain View Doctrine Should not Apply to Digital Evidence

RayMing Chang
Suffolk University Law School

Follow this and additional works at: https://dc.suffolk.edu/jtaa-suffolk

Part of the Litigation Commons

Recommended Citation
WHY THE PLAIN VIEW DOCTRINE SHOULD NOT APPLY TO DIGITAL EVIDENCE

RayMing Chang*

TABLE OF CONTENTS
I. INTRODUCTION .................................................................................. 32
II. THE PECULIAR NATURE OF DIGITAL PROPERTY ............................. 35
III. OBTAINING A WARRANT FOR DIGITAL PROPERTY ......................... 37
   A. Probable Cause ............................................................................ 37
   B. Particularity Particularly ............................................................. 38
IV. THE DOCTRINE’S EFFECT ON EXECUTION OF DIGITAL WARRANTS ... 43
   A. Generally .................................................................................... 43
   B. The Tenth Circuit’s Avoidance of the Plain View Doctrine .......... 46
   C. Illusory Limits to the Plain View Doctrine ................................. 50
      1. File Labeling and File Types ..................................................... 51
      2. Deleted Files ............................................................................. 53
      3. On-site Search, Mirroring, or Seizure ........................................ 54
      4. Time Limits .............................................................................. 56
   D. Limited Protection Against the Plain View Doctrine ...................... 58
      1. Professional Privilege ................................................................. 58
      2. Privacy Protection Act ............................................................... 58
V. THE FUTURE OF THE PLAIN VIEW DOCTRINE FOR DIGITAL EVIDENCE . 59
   A. Maintaining the Status Quo ........................................................... 60
   B. Partially Eliminating the Doctrine for Digital Evidence .............. 61
   C. Completely Eliminating the Doctrine for Digital Evidence ......... 65
VI. CONCLUSION ..................................................................................... 66

* RayMing Chang is currently a Presidential Management Fellow working for the U.S. Air Force as a program manager assigned to the Protected Satellite Communications Group, MILSATCOM Systems Wing. This article reflects the author's then present opinions, which should not be attributed to the U.S. Air Force. RayMing’s other legal research is available at http://ssrn.com/author=612935. RayMing thanks his family and friends for their support. In particular, RayMing thanks Nicole Marti; Kat Schmitt; Stephanie Chang; the soon-to-be Angela Doray; and Maj. John Wong, USAF for their support. He is grateful to Professor Fran Gilligan for his guidance with the initial drafts of this article.
I. INTRODUCTION

Courts should not apply the plain view doctrine to digital evidence because the application of the plain view doctrine to digital evidence threatens to nullify Fourth Amendment protection for digital property.\(^1\) What constitutes plain view for digital property is still a question of first impression for most courts. However, several courts have addressed this issue. These courts have begun to apply the plain view doctrine, or theories that bear a striking resemblance to the plain view doctrine, in such a manner that transforms searches executed pursuant to a warrant for digital property into general searches of the digital property. In other words, digital property warrants are transforming into a species of *de facto* general warrants. General warrants are bad. The Fourth Amendment was designed to protect against general warrants.\(^2\)

The Fourth Amendment is intended to protect Americans by prohibiting unreasonable searches and seizures.\(^3\) Fourth Amendment protection naturally extends to digital property stored on computers and other electronic storage devices. But, of course, digital property is different from physical property. The Tenth Circuit, in *United States v. Walser*,\(^4\) aptly stated the dilemma:

> The advent of the electronic age and . . . the development of desktop computers that are able to hold the equivalent of a library’s worth of information, go beyond the estab-

\(^1\) This article uses the term “digital property” to encompass digital data contained on computers and other electronic storage devices. The term “digital evidence” is used to distinguish regular digital property from digital property being used or offered as evidence.


\(^3\) The Fourth Amendment to the United States Constitution was created, in part, as a prophylactic against the evil of general searches. The Fourth Amendment specifically provides:

> 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 person or things to be seized.

U.S. CONST. amend. IV. Practitioners apply the Fourth Amendment by examining “if evidence is the product of an illegal, government search or seizure of a protected person, place, or thing” and if it is such a product, then “the evidence is inadmissible against a party with standing.” 1 *Edward J. Imwinkelried et al.*, *Courtroom Criminal Evidence* § 1801 (3d ed. 1998).

\(^4\) 275 F.3d 981 (10th Cir. 2001).
lished categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.5

The plain view doctrine is precisely such an area of Fourth Amendment jurisprudence that requires us to acknowledge those key differences and proceed accordingly.

The plain view doctrine is an exception to the Fourth Amendment that allows police to use evidence found during the execution of a warrant that is technically outside the scope of the warrant. "To satisfy the plain view doctrine: (1) the officer must be lawfully in the place where the seized item was in plain view; (2) the item’s incriminating nature was ‘immediately apparent;’ and (3) the officer had ‘a lawful right of access to the object itself.’"6

Courts have begun grappling with how the plain view doctrine applies to digital evidence and have attempted to define the scope of digital property search warrants. Police have also begun to grapple with this issue and various government bodies have issued non-binding search and seizure guidance for computers.7 Unfortunately, case law to date reveals that searches executed pursuant to warrants covering digital property can easily transform into general searches of a suspect’s digital property.

A key difference between non-digital and digital property is that police must search all of a suspect’s digital property in order to effectively execute a warrant because of the amorphous nature of digital data. The combination of the need for comprehensive searches of digital property and the fact that evidence outside the technical scope of a warrant can be admitted into evidence via the plain view doctrine causes a digital property

5 Id. at 986.
warrant to transform into a sort of de facto general warrant. Even the Tenth Circuit's attempt to avoid allowing general searches of digital property by requiring the police to obtain additional warrants when they find evidence of crimes outside the scope of the original warrant still results in de facto general searches because the incriminating evidence has already been uncovered. The implications are startling.

American lives have come to revolve around digital property, as evidenced by the explosion in computer usage in the United States and the growing prevalence of the Internet in everyday life. Inevitably, digital property will become more valuable. Digital property will become more pervasive. Because of the plain view doctrine, digital property will also become more incriminating.

This article analyzes how courts apply the plain view doctrine to warrants for digital evidence. It focuses on digital property contained in individually owned computers and storage devices. Part II briefly examines the special nature of digital property. Part III examines the logistics of getting a warrant for digital evidence, focusing especially upon particularity. Part IV analyzes how the plain view doctrine affects the execution of a digital evidence warrant. Part V discusses three alternative future paths and compares the benefits that accrue to courts, police, and citizens from: (1) maintaining the status quo, (2) partially eliminating the application of the plain view doctrine to digital evidence, or (3) completely eliminating the application of the plain view doctrine to digital evidence. Ultimately, this article argues that courts should no longer apply the plain view doctrine to warrants for digital evidence.

---

8 This article addresses only digital property owned and controlled by a specific owner. In the case of personal computers or discrete storage devices, the owner usually controls the whole device. Digital evidence in other contexts implicates myriad legal issues that fall outside the scope of this article's focus on digital property controlled by individuals. For example, a search of servers owned by Internet Service Providers ("ISPs") and other online services for personal information is subject to a Fourth Amendment analysis that must take into account that a third party is involved. See, e.g., Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (holding, inter alia, that users of an electronic bulletin board system ("BBS") did not have standing to challenge the seizure of BBS computers and that BBS users had a diminished expectation of privacy in material posted on the BBS). Other situations that require special treatment include the distribution of data over public computer networks (e.g. the Internet) and the use of computers at a workplace. Also, non-content information can be gleaned without examination of the contents of a computer hard drive. A computer connected to a network has an Internet Protocol ("IP") Address that can reveal its general location; the IP Address can also reveal the exact location of a computer, much like a street address for a house, in the case of many permanently connected computers or other computers with static IP Addresses.

9 Professor Orin Kerr has opined: "If everything comes into plain view, the plain view exception threatens to swallow the rule. Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants." Kerr, supra note 2, at 566. Yet
II. THE PECULIAR NATURE OF DIGITAL PROPERTY

Undisputedly, digital property is different from the "papers" and "effects" that the Founding Fathers contemplated when adopting the Fourth Amendment.\(^\text{10}\) The manifest difference between digital and physical property merits special consideration. Digital storage devices can hold an enormous quantity of data.\(^\text{11}\) The School of Information Management and Systems at the University of California, Berkeley estimates that about five exabytes of new information, which is equivalent to 37,000 times the amount of information in the Library of Congress book collections, was created in 2002 alone.\(^\text{12}\) Of the five exabytes of new information created in 2002, 92% were created and stored on magnetic media, primarily computer hard disks.\(^\text{13}\) The computers that created much of that digital data are now ubiquitous. The U.S. Census Bureau found that in August 2000 over half of the households in the United States, fifty-four million households, had one or more computers.\(^\text{14}\)

People now use computers and other digital devices for almost everything imaginable. Rather than storing images, movies, documents, correspondence, personal records, and a plethora of other personal data in physical form, people are storing this data in digital media. The physical world is converging with the digital world. Consequently, it is inevitable that the amount of digital property created will continue to grow. As digital property becomes embedded in our everyday lives, people envisage the digital property in a "virtual world" using labels from non-digital physical property counterparts such as "files," "cabinets," and "desktops."

At first blush, the analogy between physical files and virtual files

---
\(^\text{10}\) See, e.g., Kerr, supra note 2, at 536-47 (discussing the special nature of digital property and identifying four major differences between searches involving computers and traditional searches: the environment, the copying process, the storage mechanism, and the retrieval mechanism). The treatment of digital property in criminal law can be contrasted with copyright law, which is based on perception. Cf. 17 U.S.C. § 101 (2006).
\(^\text{13}\) Id.
seems workable, and courts have attempted to use this analogy. However, analogizing virtual objects in a digital storage device with physical papers and effects is a tenuous proposition. Digital data stored on computers require interfaces and translation in order for a person to perceive the data. Data is represented numerically and stored on elements that can be read to interpret zeros and ones. The sheer diversity of information that can exist in a digital storage device is mind boggling. An object in the physical world is discrete and is easily separable from the object’s physical location, whereas digital data must be interpreted through machines because one bit looks much like another bit until a machine organizes it into something useful.

Police cannot see digital property directly. When police look at a hard drive, they cannot interpret the magnetic charges on the surface of the disks with their bare eyes. Neither can a police officer see the Fowler-Nordheim tunneling that links gates within a flash drive’s EEPROM chip. Police cannot see whether digital property is evidence of a crime without electro-mechanical assistance. One bit “looks” much like another bit until a machine reads a digital property storage device and a program, which is also a set of bits, translates the digital property into a perceivable form that may or may not represent the true nature of the digital property.

Plain view considerations make digital property’s special characteristics even more apparent. Is it really plain view if police must “open” every “file” on a digital storage device in order to see what data is really contained within that file? Is it really plain view if one has to reconstruct the bit structure of a file? Are “hidden files” really in plain view? What if file tables contain incorrect information? When forensic specialists reconstruct files and recover data that a person might assume is permanently deleted, is that plain view? What about file size? After all, the size of a file does not accurately predict its contents; a one kilobyte (1K) file containing child pornography is just as illegal as a one hundred megabyte (100MB) file containing child pornography. Furthermore, the virtual or physical labels that purport to describe digital property are not dispositive. Are encrypted files in plain view? If a police officer is looking for a phone number among a person’s digital property, should the officer only look at text files, or look to see if there is an image of the phone number or even a

---

15 E.g., United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (analogizing computer files with physical files).
movie of the phone number? These considerations and other factors make it almost impossible for police to logically restrict a digital property search because police have to practically search all the digital property within an electronic storage device in order to effectively execute a search. Courts have begun to struggle with this reality.

III. OBTAINING A WARRANT FOR DIGITAL PROPERTY

The warrant sets the stage for police to be in a lawful position where they can take advantage of the plain view doctrine. Therefore, it is very important to consider how a warrant for digital evidence is issued. The basic requirements that must be met before a warrant can be issued are: (1) a neutral magistrate, (2) an oath or affirmation (3) based upon probable cause, and (4) a description that particularly describes the object of the search. The requirements that a warrant be supported by an oath or affirmation and issued by a neutral magistrate do not implicate any special considerations in the digital property context. However, probable cause and particularity are affected by the distinctive nature of digital property.

A. Probable Cause

Generally, a court finds probable cause to search when it determines that "the affiant had reasonable grounds at the time of his affidavit and the issuance of the warrant for the belief that the law was being violated on the premises being searched." Probable cause is important in justifying broad language that would satisfy the Fourth Amendment particularity requirement. Whether there is probable cause depends on the facts of the case in question.

In United States v. Hay, the Ninth Circuit considered a case in-
volving a personally owned computer where probable cause supported a warrant containing boilerplate language. The affidavit attached to the warrant stated “that individuals involved in possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit material and that deleted computer files can likely be retrieved by computer experts”; that language was boilerplate language and not fact-specific to the case. The court held boilerplate language to be sufficient to support probable cause.24

Probable cause for searches of personally owned computers has also been challenged on the basis of staleness. For example, the court in United States v. Horn25 confronted the question of whether there was probable cause for searching a computer based on letters written three months before the magistrate issued the warrant.26 The Horn court held that the warrant was not stale because the defendant exhibited a deep and continuing interest in child pornography; therefore, there was a reasonable likelihood that he kept some records of correspondence related to child pornography and that child pornography would probably still be in his possession.27

Digital property requires some special considerations when ascertaining whether there is probable cause, but these considerations raise no significant hurdles. The particularity requirement, on the other hand, is more challenging.

B. Particularity Particularly

Particularity is especially important for warrants for digital property because particularity delineates the scope of a search. The difficulty that courts have with particularity for digital evidence presages the difficulty that courts have with adjudicating questions regarding the execution of digital evidence warrants and the application of the plain view doctrine.

Particularity mandates that the warrant must “particularly describ[e] the place to be searched and the person or things to be seized.”28 In cases involving searches of digital evidence contained in computers and other storage devices, when evaluating whether a warrant particularly described the place to be searched and the things to be seized, most courts have found that broad language allowing the search of all computer equipment in relation to a particular type of crime is particular enough to

24 Id. at 635-36.
25 187 F.3d 781 (8th Cir. 1999).
26 Id.
27 Id. at 786-87.
28 U.S. CONST. amend. IV.
satisfy Fourth Amendment requirements. Courts have come to realize that sophisticated criminals will attempt to hide evidence in myriad ways.

The First Circuit, in United States v. Upham, held that a warrant authorizing a search of “[a]ny and all computer software and hardware, ... computer disks, disk drives ... [a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]” was valid because:

As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.

Rather than relying on the justification of searching for a needle in a computer haystack, the Seventh Circuit, in United States v. Hall, held that a warrant listing “[h]ardware, computer disks, disk drives, internal modems, tape drives, disk application programs, data disks, system disk operating systems” was sufficiently particular because the “items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography” such as “‘child pornography,’ ‘minors engaged in sexually explicit conduct,’ and ‘sexual conduct between adults . . . and minors.’”

The Ninth Circuit has several reported opinions regarding particularity of warrants for computer equipment; these opinions reflect reasoning similar to that of the Seventh Circuit. In 2004, the Ninth Circuit considered United States v. Meek. The Meek court held that a warrant which authorized, inter alia, a search of “computer equipment, computer generated printouts, data storage devices, and documentation of computer hardware” was not overbroad because it “specifically referred to items related to the sexual exploitation of children, describing those items with as much preci-

---

29 Interestingly, the DOJ Guidelines distinguishes between computers that are instrumentalities of a crime and when a computer is “merely a storage device for evidence of crime.” DOJ Guidelines, supra note 7. This distinction does not seem to have much substantive effect on particularity.

30 168 F.3d 532 (1st Cir. 1999).
31 Id. at 535.
32 142 F.3d 988 (7th Cir. 1998).
33 Id. at 995-97.
34 366 F.3d 705 (9th Cir. 2004).
In United States v. Wong, the court reasoned "that the officers were provided with objective standards alerting them to the items which could be seized . . . search warrant contained a comprehensive list of twelve items the police expected to find . . . directly related to . . . murder." The defendant in United States v. Lacy argued that a warrant authorizing the seizure of his entire computer system was overbroad. The Lacy court found that the warrant "contained objective limits to help officers determine which items they could seize—allowing seizure only of documents linked to [child pornography], for example." The Ninth Circuit's opinions reveal a focus on creating an objective standard that considers within a temporal context, i.e. when the warrant is drafted, the government's ability to describe the items to be searched as precisely as possible.

The Tenth Circuit followed the same reasoning as the Seventh and Ninth Circuits. In Davis v. Gracey, the Tenth Circuit held that a warrant authorizing "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws" was sufficiently particular because it included only items that were connected to the criminal activity and not items that did not harbor pornography.

Several federal district and state courts have also found warrants containing broad language to be particular enough. The First Circuit seems to be the only court to explicitly reason that the difficulty of searching a computer justifies broad language in a warrant and that practical concerns dictate that language authorizing the search of all of a computer's

35 Id. at 716.
36 334 F.3d 831 (9th Cir. 2003).
37 Id. at 837-38. The warrant list included "[a]ny writings or documents . . . [a]ny maps, receipts [sic], or writings, depicting Churchill County, Nevada; and [a]ny and all identification and documents belonging to [murder victim]." Id. at 837. "While Item Nine, which requested to search the computer and its components to 'obtain data as it relates to this case,' did not specify the information police expected to find on the computers or the exact location of the evidence, the content of Item Nine referred to the specific items included in the warrant list. The specificity of the items listed in the warrant combined with the language in Item Nine directing officers to 'obtain data as it relates to this case' from the computers is sufficiently specific to focus the officer's search." Id.
38 119 F.3d 742 (9th Cir. 1997).
39 Id. at 746.
40 Id.
41 111 F.3d 1472 (10th Cir. 1997).
42 Id. at 1479.
43 E.g., United States v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (holding that warrant authorizing search of a "computer and all of its related disks, software and storage devices was sufficiently particular and narrow"); People v. Ulloa, 124 Cal. Rptr. 2d 799, 802-03 (Cal. Ct. App. 2002) (holding that warrant authorizing search of "computers [etc.] containing any of the items noted above," which included photographs, videotapes, or movies of simulated or actual sexual acts, was not overbroad).
contents is the narrowest language possible. Most courts that have held that broad warrant language meets the particularity requirement seem to reason that a connection to a crime is the key factor in finding whether a warrant is sufficiently particular.

Conversely, several courts, primarily federal courts, have found certain warrant language to be overbroad and insufficiently particular. The Ninth Circuit, in *United States v. Kow*, 44 found that a warrant contained only "vague references to 'fraudulent' transactions and possible disparities between actual and reported income [and] the warrant failed to give any indication of the alleged crime to which the seized documents pertained." 45 Additionally, the *Kow* court found that the government knew where it could find relevant documents, but omitted from the warrant any detail as to what was known about the sought-after evidence. Thus, the court held that the warrant was invalid because it authorized a search of "virtually every document and computer file." 46 This holding, though reaching a contrary result, is consistent with the Ninth Circuit's holdings in *Meek, Wong, and Lacy* because of the focus on whether there is a sufficient description of a specific crime that is correlated with the broad warrant language.

Several federal district courts have also found certain language to be insufficiently particular. In *Arkansas Chronicle v. Easley*, 47 the court held that a search warrant authorizing a search of, *inter alia*, "any and all computer equipment" that contains letters, correspondence, memoranda, and journals was overbroad when the search was for a video and three still photographs, even though a crime was specified. 48 This holding is at odds with the majority of federal appellate and district court opinions because a crime was asserted. The court was likely influenced by the number of items that the police seized, which included items that could not contain photographs or videos because the court noted that the "fruits of the search confirm the excessive breadth of the warrant, as does the seizure of one computer belonging to [defendant's] minor child." 49

The court in *United States v. Clough* 50 held that a warrant was overbroad because it contained "no restrictions on the search, no refer-

---

44 58 F.3d 423 (9th Cir. 1995).
45 Id. at 427.
46 Id.
48 Id. at 793.
49 The police seized: "Eight (8) desktop computers; Two (2) laptop computers; Four hundred and fifty-four (454) 3.5-inch diskettes; One hundred and seventy (170) CD-Roms; Eight (8) mini-CD-Roms; Four (4) zip-disks; One (1) hard-drive; Fourteen (14) VHS tapes; Four (4) notebook binders containing [notes]; One (1) manilla folder with documents inside." Id. at 784-85.
ences to statutes, and no references to crimes or illegality.”

This seems in line with the requirement of the majority of courts that there be some reference to a specific crime in a warrant. In United States v. Hunter, the court held that a description of computer disks was sufficiently particularized, but the language “[a]ll computers ... [a]ll computer storage devices ... [and a]ll computer software systems” was a catch-all paragraph that lacked sufficient limitation. A warrant with the phrases “including but not limited to” and “all” was found to transform a warrant into a general warrant because it authorized the search of all items on the premises without regard to the subject matter in Matter of Search Warrant for K-Sports Imports, Inc. The Hunter and K-Sports courts express disapproval of catch-all phrases because catch-alls essentially make any described limits superfluous. The disapproval of catch-all phrases is consistent with the reasoning of the majority of courts that a warrant be at least nominally limited.

Generally, courts will find particularity if a crime is associated, however loosely, with the evidence described in a warrant. In accord, several district courts have held that warrants that do not connect the sought-after evidence to a specific crime are insufficiently particular. However, two district courts disapprove of the use of catch-all phrases for digital evidence, which appears to be inconsistent with the holdings of the majority of courts. Thus far only one court, the Arkansas Chronicle court, disfavors broad warrant language as a general rule, but the specific facts of the case give it limited applicability. Therefore, particularity proves to be a low hurdle. Police may search all of a suspect’s digital property so long as police remember to assert that a crime is associated with that property.

51 Id. at 87-88 (the language in question was “a. text documents of any variety, including e-mail, websites, records of chat sessions, correspondence or shipping records; and b. digital images of any variety, including still images and videos”).
53 Id. at 584.
55 In practice, some courts interpret even arguably narrow warrant language in ways that give police remarkable leeway to conduct digital property searches. In United States v. Gleich, the court held that a search of three computers did not exceed the scope of a warrant because the warrant authorized a search and seizure of items that could contain “[p]hotographs, pictures, visual representations, or videos in any form that include sexual conduct by a minor, as defined by [state statute].” 293 F. Supp. 2d 1082, 1089 (D.N.D. 2003). In United States v. Musson, the court held that narcotics agents did not exceed the scope of the warrant in seizing computer disks not described in the warrant because “in the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take.” 650 F. Supp. 525, 532 (D. Colo. 1986) (quoting United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986)). The court in People v. Gall held that laptop computers “were reasonably likely to serve as ‘containers’ for writings, or the functional equivalent of ‘written or printed material’ and therefore fell within the scope of a warrant that authorized the search of written or printed material.” 30 P.3d 145, 153-54 (Colo. 2001). The Gall court
There are many exceptions to the Fourth Amendment such as consent, exigent circumstances, a search incident to arrest, and the plain view doctrine. Among these exceptions, the plain view doctrine has critical significance for digital property. Under the plain view doctrine "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant." The key question that arises in the digital property context is: What if police are always in a lawful position after obtaining a warrant and can view everything?

A. Generally

"To satisfy the plain view doctrine: (1) the officer must be lawfully in the place where the seized item was in plain view; (2) the item's incriminating nature was 'immediately apparent;' and (3) the officer had 'a lawful right of access to the object itself.' During a search of a suspect's digital property executed pursuant to a broadly worded warrant, a police officer is arguably "lawfully in a place" where all of a suspect's digital property is in plain view. If all of a person's digital property is in plain view, then the application of the plain view doctrine to digital property searches logically transforms digital property searches into general searches. Courts are beginning to explicitly apply the plain view doctrine to digital property and the unfortunate transformation of digital property

also asserted that it was good policy to allow seizure and removal of computers, characterized as sealed containers, for off-site searches because it is less intrusive than on-site searches. Id.


58 Id. at 838 (citing Horton v. California, 496 U.S. 128, 136-37 (1990)).

59 An interesting argument that a defendant may assert is that though a computer may be validly seized under a warrant, a second warrant is necessary to search the actual contents of the computer. In United States v. Simpson, the defendant argued that police lacked the authority to search the seized computer disks and hard drive because the warrant just authorized the search of the seized computers and not the component parts. 152 F.3d 1241 (10th Cir. 1998). The Tenth Circuit rejected that argument and held that computer disks and hard drives are not closed containers that are "somehow separate from the computers themselves." Id. at 1248.
searches into general searches is already taking place.

Many courts, including the Supreme Court, have not yet considered the question of how the plain view doctrine should apply to digital property searches. Of the federal circuit courts, only the Ninth Circuit has directly addressed this issue. In *United States v. Wong*, the Ninth Circuit considered the admissibility of evidence related to child pornography that was found during a search for evidence connected to the disappearance and murder of the appellant’s girlfriend. The *Wong* court held that the child pornography that was discovered was properly admitted under the plain view doctrine. The court explained: “the police were lawfully searching for evidence of murder in the graphics files, that they had legitimately accessed and where the incriminating child pornography was located.”

Several federal district courts have applied the plain view doctrine to admit evidence found outside the technical scope of a warrant. In *United States v. Gray*, the Eastern District of Virginia held that a Federal Bureau of Investigation agent “was entitled to examine all of defendant’s files to determine whether they contained items that fell within the scope of the warrant.” That language is very significant. The court explicitly allowed the examination of all of the defendant’s files after the digital property warrant was issued. The *Gray* court found that that material outside the scope of the warrant, which was inadvertently discovered, was admissible under the plain view exception. In *United States v. Nichols*, an unreported opinion, the Northern District of Indiana considered a case where a detective came across evidence of child pornography while searching for evidence of pirated videos. The *Nichols* court seemed to apply the plain view doctrine, but it also discussed the Tenth Circuit’s second warrant requirement; the Tenth Circuit’s warrant requirement is discussed in the next section of this article. The *Nichols* court expressed approval that the detective sought a second warrant after discovering the child pornogra-

---

60 334 F.3d 831 (9th Cir. 2003).
61 Id. at 833.
62 Id. at 838.
63 Id. The Ninth Circuit’s reasoning in *Wong* is similar to the Tenth Circuit’s reasoning in *Carey* and *Walser*, which are discussed in the following section, but the Tenth Circuit did not explicitly recognize the applicability of the plain view doctrine to digital property searches. See infra Part IV.B. Also, unlike the Tenth Circuit, the Ninth Circuit did not require the police to get a second warrant. See infra Part IV.B.
65 Id. at 528-31.
67 Id. at *1-*2.
68 Id. at *6-*9 (discussing the plain view doctrine and how the pornographic files were in plain view).
The child pornography in Nichols was held to be admissible as evidence.\(^69\)

Another federal court applied the plain view doctrine in the guise of inevitable discovery. The Southern District of New York, in United States v. Harding,\(^70\) denied a motion to suppress evidence of child pornography found on a computer disk because, the court reasoned, the agents would have inevitably discovered the child pornography in executing the part of the warrant authorizing a search of the disk for evidence of fraud.\(^71\) The Southern District in that case was incorrect in its application of inevitable discovery because the only reason the investigators found the material was because they were searching pursuant to a warrant for fraud. It is not inevitable that police will search a person pursuant to a warrant and there was no other independent method of discovery mentioned by the Harding court. The Harding court was likely pondering the plain view doctrine and thus should have hung its argument on the plain view hook.

The application of the plain view doctrine to digital evidence is also occurring in state courts. The Indiana Court of Appeals, in Frasier v. State,\(^72\) held that images of child pornography found on the defendant’s computer were inadvertently discovered in plain view because, though the warrant only authorized officers to search a computer for evidence relating to marijuana, the officer was allowed to open ambiguously labeled and possibly mislabeled files.\(^73\) The People v. Ulloa\(^74\) court, in dicta, reasoned that photographs found on the defendant’s computer during the execution of a warrant authorizing search of “computers [etc.] containing any of the items noted above,” which included photographs, videotapes, or movies of simulated or actual sexual acts, would have been admissible under the plain view doctrine.\(^75\) The New York Supreme Court, in People v. Emerson,\(^76\) heard a case where police came across image files clearly labeled as having child pornography that indeed did contain child pornography.\(^77\) The Emerson court held that those file names were in plain view.\(^78\) Recently, the Court of Appeals of Virginia decided that deleted files were also in

\(^{69}\) Id.
\(^{70}\) Id. at *9.
\(^{72}\) Id. at 420 (the specific words of the court were: “because the agents inevitably would have discovered their contents in the proper execution of the other portion of the warrant”).
\(^{74}\) Id. at 465-66.
\(^{75}\) 124 Cal. Rptr. 2d 799 (Cal. Ct. App. 2002).
\(^{76}\) Id. at 803-04.
\(^{77}\) 1 Misc. 3d 638 (N.Y. Sup. Ct. 2003).
\(^{78}\) Id.
\(^{79}\) Id. at 641-45.
A trend is clearly emerging where courts are admitting evidence found outside the scope of a digital property warrant under the plain view doctrine. These courts, by admitting evidence outside the scope of a digital property warrant, have transformed digital property warrants into *de facto* general warrants that allow general searches of a particular suspect’s digital property. This transformation of digital property warrants increases the danger of pretextual searches. For example, one possible pretextual search scenario is for police to target a person by issuing a warrant for “illegal possession and distribution of copyrighted materials.”

There is almost certainly probable cause to search nearly every computer in the United States for copyright infringement because of the very nature of computers and how computers are used today. Once the warrant is issued, everything on the computer or on other storage devices may be searched and used against the targeted person. The danger from these *de facto* general warrants for digital property will increase as time passes and more of our lives is recorded and stored in digital property. Several courts have tried to mitigate this risk by limiting digital property warrants.

**B. The Tenth Circuit’s Avoidance of the Plain View Doctrine**

The Tenth Circuit has heard two digital property cases that have drawn the attention of many courts and commentators. The two cases, *United States v. Carey* and *United States v. Walser*, implicated the plain view doctrine, but the court avoided the application of the plain view doctrine in both cases. The Tenth Circuit’s failure to address the plain view doctrine, despite its obvious applicability, makes its reasoning in these cases problematic. Additionally, the Tenth Circuit’s approach is problematic because it focused on the subjective intent of police, which is contrary to United States Supreme Court precedent. Moreover, the requirement for a second warrant that emerged in the *Carey-Walser* cases still results in

---

80 Rosa v. Commonwealth, 628 S.E.2d 92, 93 (Va. Ct. App. 2006) ("We hold that the officer acted reasonably in opening the picture files and that the deleted files were in plain view.").


82 A person operating a computer can easily infringe a copyright, even unintentionally. See http://www.respectcopyrights.org/ (last visited Oct. 21, 2006).


84 172 F.3d 1268 (10th Cir. 1999).

85 275 F.3d 981 (10th Cir. 2001).

the transformation of digital property warrants into *de facto* general warrants.\(^{87}\)

The Tenth Circuit in *Carey* held that police exceeded the scope of the search warrant by extending a search for evidence of drug trafficking into a search for child pornography. The search warrant authorized a search of the defendant’s computer for evidence of drug trafficking.\(^{88}\) The officer who searched the defendant’s computer opened an image file containing child pornography; after opening that file, the officer then spent five hours searching for more child pornography and “temporarily abandoned” his search for evidence relating to drug trafficking.\(^{89}\) The court held that the officer exceeded the scope of the search warrant because the officer knew, or at least suspected, that he would find evidence not related to drug trafficking in the JPG image files, *i.e.*, child pornography.\(^{90}\) The court did not opine as to what exactly constituted plain view in the context of computer files, but noted that the images were in “closed files” and therefore the plain view doctrine did not apply.\(^{91}\) The court stated:

> Although the question of what constitutes “plain view” in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here. Judging this case only by its own facts, we conclude the items seized were not authorized by the warrant. Further, they were in closed files and thus not in plain view.\(^{92}\)

The court limited its holding to the files that the officer opened after discovering the first pornographic image.\(^{93}\) The officer’s critical mistake, in the Tenth Circuit’s view, was in not obtaining a second warrant once he discovered the child pornography.

The Tenth Circuit further elaborated on *Carey* in *Walser*. The *Walser* court held that an officer did not exceed the scope of a warrant, which authorized a search for evidence of drug trafficking, by opening and viewing a video file containing child pornography.\(^{94}\) The officer used a

\(^{87}\) We cannot rely on police officers to respect a suspect’s privacy by refraining from requesting a second warrant. A diligent police officer would just have to make sure that she gets a second warrant when she finds out-of-scope evidence.

\(^{88}\) *Carey*, 172 F.3d at 1272-73 (specifically, the warrant was for “names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.”).

\(^{89}\) *Id.* at 1273.

\(^{90}\) *Id.* at 1274-75.

\(^{91}\) *Id.* at 1273.

\(^{92}\) *Id.*

\(^{93}\) *Id.* at 1273 n.4.

\(^{94}\) *United States v. Walser*, 275 F.3d 981, 987 (10th Cir. 2001).
"clear search methodology" by "search[ing] for relevant records in places where such records might logically be found." The officer came across a file with a ".avi" extension and opened it. After opening the video file and confirming his belief that it contained child pornography, the officer suspended his search and went to a magistrate judge to obtain a new warrant. The Tenth Circuit focused on the fact that the officer inadvertently discovered the file. The court did not explicitly refer to the plain view doctrine, but its "inadvertent discovery" reasoning seems strikingly similar to the plain view doctrine. The court noted approvingly that the officer "showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography."

The officer in Walser did not make the same "mistake" as the officer in Carey.

There are several defects in the Carey and Walser opinions. These defects arise from the Tenth Circuit's reluctance to directly address the application of the plain view doctrine to digital evidence. Instead, the Tenth Circuit inappropriately adjudicated Carey and Walser by ignoring the technical realities of computer forensics, departing from precedent, and adding a superfluous easy-to-circumvent procedure.

First, the Tenth Circuit mistakenly avoided the application of the plain view doctrine in Carey and Walser. The plain view doctrine clearly applied in both cases because in each case all elements of the doctrine were satisfied. In both Carey and Walser (1) the officer was lawfully viewing the contents of a suspect's digital property where the file was in plain view; (2) the file's incriminating nature was immediately apparent because the officer had to view the file; and (3) the officer had a lawful right of access to the file because of a warrant. However, the Tenth Circuit expressed distaste about applying the plain view doctrine and applied a "closed file" construct. The court's distaste may have stemmed from the investigator's obvious deviation from the literal scope (sans exceptions) of the warrant and the fact that applying the plain view doctrine to digital property warrants logically results in general searches. However, the abandonment theory and the "closed file" construct articulated by the Tenth Circuit do not recognize the reality that police must comprehensively search a suspect's digital property in order to properly execute a warrant. Data can be hidden in myriad ways, such as mislabeling, encryption, and

95 Id. at 986. The officer first searched the "My Documents" folder and then the "Recycle Bin." Id. The officer then searched the "Microsoft Works" subfolder in the "Program Files" folder because of the belief that Microsoft Works is a spreadsheet program and that drug trafficking records would be kept in that folder. Id.
96 Id. at 987.
97 Id.
98 Id.
99 Walser, 275 F.3d at 987.
deletion. The only search methodology that is thorough is a complete search of digital property. There is no perfect search tool that can restrict its search just to the evidence related to a particular crime. The Tenth Circuit does not recognize the reality that police must search every file. If police must search all of a suspect’s digital property, then there can be no inadvertence or abandonment in discovering evidence.

Second, the Tenth Circuit improperly focused on the subjective intent of the police searching the defendant’s digital property in developing the abandonment theory. The Tenth Circuit overlooked the clear instruction from the United States Supreme Court in Horton v. California:

[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a

100 See supra Part II; infra Part IV.C.
101 See infra Part V.B.
102 The Tenth Circuit, upon petition for rehearing of Carey, stated:
Because the government contends we failed to properly follow Horton v. California, 496 U.S. 128, 130 (1990), we recognize inadvertance [sic] is not a Fourth Amendment requirement. We note, however, “inadvertence is a characteristic of most legitimate ‘plain-view’ seizures.” Id. As such, the fact that Detective Lewis did not inadvertently come across the pornographic files is certainly relevant to our inquiry. Our holding is based, however, on the fact that Detective Lewis impermissibly expanded the scope of his search when he abandoned the search for drug-related evidence to search for evidence of child pornography. The petition for rehearing is denied.

Carey, 172 F.3d at 1277-78. The U.S. Supreme Court stated:
The suggestion that the inadvertance [sic] requirement is necessary to prevent the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements that no warrant issue unless it “particularly describ[es] the place to be searched and the persons or things to be seized,” and that a warrantless search be circumscribed by the exigencies which justify its initiation.

Horton, 496 U.S. at 139-40 (citations omitted). The syllabus that prefaces Horton summarizes succinctly, “even though inadvertence is a characteristic of most legitimate ‘plain-view’ seizures, it is not a necessary condition.” Id. at 130 (syllabus to the case). Yet, the Tenth Circuit managed to incorporate inadvertence into its abandonment theory.

103 Other commentators have also noted this deficiency. See Ziff, supra note 83 at 853-57 (criticizing the reasoning in Carey because of a restrictive warrant interpretation and focus on subjective intent).
valid exception to the warrant requirement.\textsuperscript{104}

From an objective viewpoint, police must search all of the contents of a suspect’s digital property described in a warrant in order to ascertain the true nature of the contents. Paraphrasing the United States Supreme Court and applying the fact pattern from \textit{Carey}, the fact that the investigator in \textit{Carey} fully expected to find child pornography during the course of a search should not invalidate its seizure if the search was within the terms of a warrant or a valid exception, \textit{e.g.}, the plain view doctrine.

Third, the Tenth Circuit’s avoidance of the plain view doctrine in \textit{Carey} and \textit{Walser} is unsuccessful because the resulting jurisprudence merely adds an easy-to-meet procedural requirement that is functionally equivalent to the plain view doctrine. The additional procedural step of getting another warrant for evidence unrelated to the crime covered by the first warrant provides little protection. Law enforcement has quickly adapted to the \textit{Carey} and \textit{Walser} jurisprudence. An example of this adaptation can be found in the DOJ Guidelines, which states that “agents should obtain a second warrant to search a computer seized pursuant to a valid warrant if the property targeted by the proposed search is different from that underlying the first warrant.”\textsuperscript{105} The second warrant requirement provides little protection because the police would have \textit{already found the out-of-scope evidence}, and getting the second warrant would just be standard operating procedure. Thus, unfortunately, the Tenth Circuit’s attempt at solving the digital property warrant scope conundrum still results in general searches of digital property.

\textbf{C. Illusory Limits to the Plain View Doctrine}

The plain view doctrine is potentially circumscribed by a number of possible limitations. These potential limits include: whether file labeling or specific file types are limiting factors during a search; whether law enforcement may search deleted files; whether the search of a computer should be conducted on-site, the hard drive mirrored, or the computer seized to be searched off-site; and how much time is allowed for searches of seized computers. These limits do not effectively stop digital property warrants from becoming a type of \textit{de facto} general warrant.

\textsuperscript{104} 496 U.S. 128, 138 (1990) (6-3 opinion Stevens, J.) (emphasis added).
\textsuperscript{105} DOJ Guidelines, supra note 7.
1. File Labeling and File Types

Courts may limit police to searching only certain file types or force police to rely on the veracity of file labels.\textsuperscript{106} The advantage to limiting police searches based on file name or type is that a clear standard can be articulated. Yet there are many disadvantages to hobbling police in such a way. Criminals can easily hide evidence by mislabeling files.\textsuperscript{107} It is unlikely that a suspect will label a file \textquotedblleft evidence-of-a-crime.doc\textquotedblright{} or some other variation that clearly indicates that the file contains pertinent evidence. Additionally, evidence of a crime can be found in almost any type of file. A phone number can exist in an image, in a video, in a document, in a spreadsheet, and in any other type of digital file. There are also a dizzying number of file extensions, which continue to grow as more programs are developed, further supporting the contraindication of file type restrictions.\textsuperscript{108} If police were to rely on directory or file labels, then the police would only catch criminals who accurately label their digital property; should police only catch careless criminals? Initially, some courts attempted to restrict searches by relying on file labels and file types, but now courts generally allow the opening and viewing of almost any file within digital property.

Among the federal circuit courts, the Tenth Circuit has come the closest to addressing dependence on file types and file names. The court tangentially addressed file labeling in \textit{Carey}, where it found that an officer exceeded the scope of a warrant by opening an image file labeled \textquotedblleft .jpg\textquotedblright{} while looking for documentary evidence of drug trafficking.\textsuperscript{109} The reasoning in \textit{Carey} seems to imply that the police should have relied on the file labels. Later, in \textit{Walser}, the Tenth Circuit found that searching an \textquotedblleft .AVI\textquotedblright{} file for evidence of drug trafficking was appropriate.\textsuperscript{110} Unfortunately, the Tenth Circuit did not directly address the file type/name issue, but its treatment of the search in \textit{Walser} indicates flexibility regarding file types.

Only one court has explicitly restricted a search based on file label-

\textsuperscript{106} This article uses the terms \textquotedblleft file label\textquotedblright{} and \textquotedblleft file type\textquotedblright{} to encompass all descriptive data that describes attributes or identifies digital property or discrete parts of digital property (\textit{e.g.}, headers, directory names, file properties).

\textsuperscript{107} See DOJ Guidelines, \textit{supra} note 7 (\textquotedblleft The targeted files may be mislabeled, hidden, oddly configured, written using code words to escape detection, encrypted, or otherwise impossible to find\textquotedblright{}); see also Ziff, \textit{supra} note 83, at 864 (discussing innocuously or ambiguously named files).

\textsuperscript{108} \textsc{FILExt}, a website cataloging computer file extensions, has over 22,800 records correlating file extensions with computer programs. http://filext.com/ (last visited Oct. 24, 2006).

\textsuperscript{109} See \textit{supra} Part IV.B.

\textsuperscript{110} See \textit{supra} Part IV.B.
ing. In *People v. Carratu*, a New York state court gave great weight to the Tenth Circuit's reasoning in *Carey* and adopted much of that court's reasoning. The *Carratu* court found that the officer, during a search for evidence related to an illegal cable box operation, expected to find out-of-scope material related to fake identification when the officer opened a folder labeled "Fake I.D." The court held that a search of a folder labeled "Fake I.D." was beyond the scope of the warrant because it was unambiguously labeled and "the name of the folder clearly indicated that it likely contained false identification documents rather than documents or records concerning the sale of illegal cable boxes."

A majority of courts that have addressed file labeling acknowledge the fact that files may be mislabeled and that information may exist in various file types. The Central District of California pithily stated: "There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it." In *Gray*, the Eastern District of Virginia acknowledged the possibility that suspects may intentionally mislabel files by accepting the assertion that the agent "knew from his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories." The *Gray* court held that: "In searching for the items listed in the warrant, [the police officer] was entitled to examine all of defendant's files to determine whether they contained items that fell within the scope of the warrant." The Southern District of New York found in *Harding* that personal computers typically allow a user to assign any desired three letter file extension to any file, regardless of the nature of the content of the file. . . . A personal computer user could assign file names including file extensions, such as 'jpg,' that conventionally are used to indicate graphic data files to files that contain text.

In *United States v. Abbell*, the Southern District of Florida also addressed the issue of seized floppy disks with labels containing descrip-

---

112 Id. at 804-05. Interestingly, the *Carratu* court did not limit its holding, like the *Carey* court did, to the files opened after the officer initially discovered that there may be evidence of wrongdoing outside the scope of the warrant. Id. at 808.
113 Id. at 808-09.
116 Id.
117 273 F. Supp. 2d at 424.
tions of subjects that did not fall under the scope of the warrant. The court held that the resulting evidence discovered on those disks was admissible because the officer was not required to assume that the labels accurately described the contents of the disks. Additionally, the Indiana Court of Appeals, in *Frasier v. State*, held that a warrant that authorized an officer to search a computer for evidence relating to marijuana allowed the officer to open ambiguously labeled files because of potential mislabeling.

Most courts that have opined regarding the file descriptions debate have allowed police to search all files in a suspect’s piece of digital property. The New York Supreme Court is the only court to unequivocally hold that a search exceeds the scope of a warrant if the search extends to files labeled with descriptions that do not match the warrant’s description of evidence sought. In practice, courts will likely allow officers to search all files within a particular piece of digital property because suspects may mislabel files or otherwise attempt to hide files that may actually be within the scope of a warrant.

2. Deleted Files

Another possible limit to digital property searches occurs when suspects “delete” files; however, contained within every computer is a hidden trove of deleted files that many people believe are unrecoverable. Forensic examination by computer experts can recover many of these deleted files. It seems to be general practice for police to attempt to recover deleted files using computer programs designed to recover such files, such as EnCase®. Significantly, the DOJ and New Jersey Guidelines both contemplate the use of forensic analysis to recover deleted files.

The First Circuit directly addressed this issue in *United States v. Upham*. In *Upham*, the court held that the recovery of deleted files from

---

119 *Id.* at 1201.
121 *Id.* at 465-66.
123 The DOJ Guidelines addresses the issue of potential mislabeling in part B.1.b. and part B.1.c step 3 in the drafting section. DOJ Guidelines, *supra* note 7.
125 *See*, e.g., Rosa v. Commonwealth, 628 S.E. 2d 92, 94 (Va. Ct. App. 2006).
126 *Id.;* NJ Guidelines, *supra* note 7, at 18.
127 168 F.3d 532 (1st Cir. 1999).
a computer and from diskettes was within the scope of the warrant. The warrant authorized a search of "[a]ny and all computer software and hardware, . . . computer disks, disk drives . . . [a]ny and all visual depictions, in any format or media" of underage minors.\(^{128}\) The files from the diskettes were recovered using the undelete function of the computer, and the files from the formatted hard disk were recovered using a special utility program.\(^{129}\) The court reasoned that the recovery of deleted files "after attempted destruction, is no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."\(^{130}\) The Ninth Circuit briefly mentioned deleted files in its analysis of probable cause for a warrant in *United States v. Hay*;\(^{131}\) it held that probable cause for a warrant was still supported six months after a transmission of child pornography, in part because computer experts could recover deleted files.\(^{132}\)

In *Commonwealth v. Copenhefer*,\(^{133}\) the Supreme Court of Pennsylvania held that a defendant's "unsuccessful attempt to delete documents or files from his computer did not create a legally protected expectation of privacy which would have required a second warrant before the prosecution applied technology to elicit the content of files buried in the memory of the computer."\(^{134}\) These cases indicate that courts are likely to find that deleted files are within the scope of a search warrant. Thus, the deleterious effects of the plain view doctrine extend to digital property that people consider deleted.

3. On-site Search, Mirroring, or Seizure

Restrictions on police "seizure" of digital property are possible limits to the plain view doctrine. One possible restriction is location, *i.e.*, whether police are restricted to the site where the digital property is located. Another is whether police may mirror or merely seize the digital property for perusal offsite. If the police are permitted to search at their leisure, then the potential for abuse of the plain view doctrine increases. Among reported cases, courts have generally allowed seizure of computers

---

128 *Id.* at 535.
129 *Id.* at 537.
130 *Id.* Interestingly, the government made a novel argument attempting to analogize file deletion with "putting one's trash in the street where it can be searched by every passerby," but the court rejected this abandonment argument. *Id.* at 537 n.3.
131 231 F.3d 630 (9th Cir. 2000).
132 *Id.* at 636.
134 *Id.* at 1355-56.
for searching material off-site without reviewing the contents of the computer at the site where the computer was seized. The courts seem to be primarily concerned with the technical nature of the evidence and the difficulty of segregating files on-site.

The Sixth Circuit, in *United States v. Henson*,\(^{135}\) held that it was reasonable for law enforcement to seize a large amount of documents and computer files without first segregating the material outside the scope of the warrant.\(^{136}\) The court noted that "it was inevitable that the officers would seize documents that were not relevant to the proceedings at hand" because "the extensive seizure of records was authorized by the terms of the warrant."\(^{137}\) The court found that it was "unreasonable to require officers to sift through the large mass of documents and computer files found . . . in an effort to segregate those few papers that were outside the warrant."\(^{138}\)

In *Mahlberg v. Mentzer*,\(^{139}\) the Eighth Circuit briefly touched on the scope of a warrant to search for computer software while reviewing a district court's denial of a new trial for abuse of discretion. The warrant in question listed two programs with serial numbers as the objects of the search.\(^{140}\) The officer that executed the warrant testified that he seized all the computer disks that were found because he did not know which disks held the evidence being sought and because he was told that the defendant might booby-trap the disks to erase themselves if examined on the defendant's computer.\(^{141}\) The court held that the officer's testimony was sufficient to support the jury's verdict that the seizure of all the computer disks did not violate the Fourth Amendment.\(^{142}\)

Several federal district courts have also addressed the issue of whether police have to search computers at the site of seizure. In *United States v. Gawrysiak*,\(^{143}\) the court held that seizure of all of a defendant's

\(^{135}\) 848 F.2d 1374 (6th Cir. 1988).
\(^{136}\) *Id.* at 1383-84.
\(^{137}\) *Id.* at 1383. The warrant authorized a search of "any and all records, but not limited to modules, modems and connectors, computer, computer terminals, hard copy user documentation pertaining to files and/or programs, cables, printers, discs, floppy discs, tapes, vendor phone numbers, all original and backup tapes and discs, any other informational data input, all vendor manuals for hardware and software, printouts . . ." *Id.* at 1382. The Sixth Circuit relied on similar reasoning in *United States v. Frost*, 125 F.3d 346 (6th Cir. 1997). The *Frost* court held that the extensive seizure of paper and computer documents was authorized by the warrant because of the complex nature of a mail fraud case. 125 F.3d at 388.
\(^{138}\) *Henson*, 848 F.2d 1374, 1383-84.
\(^{139}\) 968 F.2d 772 (8th Cir. 1992).
\(^{140}\) *Id.* at 774.
\(^{141}\) *Id.* at 776.
\(^{142}\) *Id.* at 775-76.
computer files by copying the files onto disks for off-site search without prior review was appropriate because the "agents acted with good faith and with the intent to carry out the search in an appropriate and efficient manner."\textsuperscript{144} In \textit{United States v. Yung},\textsuperscript{145} the court held that a seizure of items including computer files without an individual review prior to the completion of the search did not invalidate the search because the executing officers acted in good faith in attempting to stay within the boundaries of the warrant and because the extensive seizure of the items "was prompted largely by practical considerations and time constraints."\textsuperscript{146} Clearly, courts have been giving police considerable leeway to search digital property at their leisure.

4. Time Limits

Placing time limits on searches potentially decreases the danger of abuse of the plain view doctrine. The Fourth Amendment does not place any specific time limit on how long a seized computer can be held by the government for a search. An implicit time limit can generally be extrapolated from the protection against "unreasonable searches and seizures." Rule 41 of the Federal Rules of Criminal Procedure requires that searches be executed within ten days of obtaining a warrant, but this has not been applied to searches of seized computers.\textsuperscript{147} There is very little reported case law regarding how long a computer can be held by police. The longer that police can scrutinize digital property, the greater the possibility that the police will find something that could be admissible via the plain view doctrine.

In \textit{United States v. Syphers},\textsuperscript{148} police detained a computer for seven months before completing a search of the computer. The court found that there was "an 'overwhelming backlog' in the investigation of computer crime by the state police."\textsuperscript{149} The court also found that the search was completed five months ahead of the deadline specified in the warrant extension. The court held that the seven month period of detention was constitutional because the police acted in good faith in light of the backlog and complexity of the search.\textsuperscript{150}

\textsuperscript{144} \textit{Id.} at 866.
\textsuperscript{146} \textit{Id.} at 1569 (citation omitted).
\textsuperscript{147} FED. R. CRIM. P. 41(c)(1).
\textsuperscript{149} \textit{Id.} at 58.
\textsuperscript{150} \textit{Id.} The \textit{Syphers} court cited \textit{United States v. Greene}, 56 M.J. 817 (N.M. Ct. Crim. App. 2002), to support its holding. In \textit{Greene}, consent was given to seize and search a computer and the court found that three months was a reasonable time period for examining
In contrast, the search in *United States v. Brunette*\(^{151}\) was held to be too long. The warrant had a sixty day time limit. The court held that the government failed to abide by the time limit in the search warrant when a computer was searched sixty-two days after the warrant was issued. The court allowed suppression of the evidence that was gathered after the time limit expired.\(^{152}\) *Brunette* is distinguishable from *Syphers* because the investigators in *Syphers* requested an extension of time for the warrant and kept within the time limit allowed by that extension.

The DOJ Guidelines reports that some magistrate judges have begun imposing time limitations on searches of computers:\(^{153}\)

Several magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time. Other magistrates have suggested that Rule 41's requirement that agents execute a "search" within 10 days of obtaining the warrant might apply to the forensic analysis of the computer as well as the initial search and seizure.\(^{154}\)

These time limits reportedly being imposed may significantly limit the ability of law enforcement to search for plain view evidence outside the technical scope of a warrant and may also significantly limit the ability of law enforcement to search for evidence within the technical scope of a warrant. Because of the paucity of information, the reported reluctance on the part of some magistrate judges has an uncertain impact on the application of the plain view doctrine.

---

152 Id. at 42.
D. Limited Protection Against the Plain View Doctrine

Although the plain view doctrine for digital property is generally unhindered by concerns such as file labeling, file deletion, seizure, or time limits, there are some narrow protections for certain types of digital property. These narrow limits on the plain view doctrine are professional privileges and statutory First Amendment based protections.

1. Professional Privilege

Lawyers and other professionals work with a great deal of privileged information. This material may include attorney-client correspondence, medical records, and other sensitive information. It is natural for these professionals to work with and save privileged material on their personally owned computers. Additionally, it is highly likely that clients of these professionals may have stored privileged material on their personal computers. Privileged material enjoys legal protections that may be abrogated by the broad scope of search warrants.

DOJ Guidelines provide some guidance regarding the handling of privileged material.\textsuperscript{155} The DOJ Guidelines express a slight preference for using "Taint Teams" that review material, independent from the prosecution, for privileged material. In \textit{United States v. Crim. Triumph Capital Group},\textsuperscript{156} the District of Connecticut held that "[t]he use of a taint team is a proper, fair and acceptable method of protecting privileged communications when a search involves property of an attorney."\textsuperscript{157} Though taint teams can protect privilege, the use of taint teams is neither mandatory nor uniform across jurisdictions, and privileged material may still be revealed during a search for unrelated material. There is a dearth of cases regarding privilege in connection with digital property plain view doctrine; therefore, it is very difficult to gauge whether privilege provides real protection for privileged digital property.

2. The Privacy Protection Act

The Privacy Protection Act ("PPA") protects certain classes of material that implicate the First Amendment, such as material compiled by

\textsuperscript{155} DOJ Guidelines, \textit{supra} note 7, at Part II.B.7.
\textsuperscript{156} 211 F.R.D. 31 (D. Conn. 2002).
\textsuperscript{157} \textit{Id.} at 43.
The Senate Committee report accompanying the PPA explained its purpose:

[T]he purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

Section 2000aa(a) of Title 42, United States Code provides:

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials.

The PPA contains significant exceptions. Some exceptions from PPA protection include searches of contraband, instrumentalities, or fruits of a crime. Perhaps the most significant limitation of the PPA is that it only protects third-parties, not suspects. Thus, the PPA provides very limited protection that does not adequately discourage general searches of a suspect’s digital property.

V. THE FUTURE OF THE PLAIN VIEW DOCTRINE FOR DIGITAL EVIDENCE

The plain view doctrine, as currently constructed, is a danger to personal liberty when applied to digital property searches. There are three possible paths forward. Courts could: (1) maintain the status quo, (2)
partially eliminate the application of the plain view doctrine to digital evidence, or (3) completely eliminate the application of the plain view doctrine to digital evidence.

A. Maintaining the Status Quo

Courts could maintain the status quo and apply the plain view doctrine accordingly. There are some benefits to maintaining the status quo. Courts do not have to break with precedent covering non-digital property, where applying the plain view doctrine is commonplace and unexceptional. There would be no need to alter existing jurisprudence and no need to treat digital property differently. Maintaining the status quo would allow police to search everything on a computer and use everything found as evidence. Police could then make comprehensive searches of digital property a standard operating procedure and thereby increase their ability to obtain useful evidence. In jurisdictions that follow the Tenth Circuit’s second warrant requirement, police could easily circumvent that protection by making comprehensive searches of digital property a standard operating procedure and train their officers to obtain a second warrant whenever a new crime is found. In fact, the DOJ Guidelines already suggest that approach. Moreover, society might benefit from the increased likelihood of successful prosecutions of criminals.

There is, however, a strong argument against maintaining the status quo. The negative aspects of maintaining the status quo have been discussed in detail throughout this article, most notably in Part IV. In brief, the application of the plain view doctrine to evidence found during the execution of a digital property warrant creates a species of *de facto* general warrants. General searches are bad. Courts that apply the plain view doctrine to digital evidence condone police action that violates the Fourth Amendment. Courts that apply alternative reasoning, similar to that of the Tenth Circuit, will still create a type of *de facto* general warrants. The status quo gives police great power that could possibly be abused. The cliché “absolute power corrupts absolutely” comes to mind. Under the status quo, police can easily conduct “fishing expeditions,” *i.e.*, pretextual searches where police may charge a person with a minor crime in order to get a digital property warrant, and then charge that person with any crime discovered during the search of the digital property.\textsuperscript{164}

\textsuperscript{164} It is important to note that the exclusionary rule is designed to prevent injury to the person. The Supreme Court has stated that “the [exclusionary] rule is a judicially created

---

\textsuperscript{164} note 2, at 571-76 (arguing that the application of ex ante restrictions to the digital plain view doctrine is inappropriate). The author agrees with Professor Kerr that digital property searches call for *ex post* standards, not *ex ante* rules.
Currently, child pornography is the crime that has been implicated in most of the reported cases dealing with the application of the plain view doctrine to digital evidence. In these cases, the heinous nature of child pornography masks the potential danger from general searches. In the future, however, people's use of computers for non-pornographic purposes will undoubtedly increase. Thus, as digital property and people's lives converge, the danger to privacy and liberty from general searches of digital property will grow. Although there is some merit to maintaining the status quo, the argument against the status quo is strong, especially because the status quo violates the spirit of the Fourth Amendment. Therefore, maintaining the status quo is unacceptable.

B. Partially Eliminating the Plain View Doctrine for Digital Evidence

Courts and commentators have conceived of a number of ways to limit the adverse effects of the plain view doctrine for digital evidence. This section will examine some of these possible mitigating methods, which include: (1) subjective intent limitations; (2) use of digital property search tools; (3) limiting evidence to particular forensic steps; (4) limits by the type of crime; (5) using an “immediately apparent” standard; and (6) limits based upon the type of defendant.

One possible way of mitigating the effects of digital plain view is to rely on the subjective intent of the investigating officer, i.e., whether the police expected to find evidence outside the scope of the original digital property warrant. Under a pure subjective intent standard, courts would have to divine the intent of police during a particular search. If an investigator expected to find evidence outside the technical scope of the warrant at any time during the search, then that evidence would be inadmissible. Otherwise the plain view doctrine would apply and the evidence would be admissible. The Tenth Circuit implemented a variation of this approach with an additional step of obtaining a second warrant when out-of-scope evidence was found.\footnote{United States v. Gray, 78 F. Supp. 2d 524, 526-27 (E.D. Va. 1999); see Kerr, supra note 2, at 578-79 (“Proving intent is particularly problematic in the computer context because government agencies can set policies that mandate very thorough forensic investiga-}
for not using subjective intent as a limitation is that the United States Supreme Court has specifically disapproved of subjective intent. The United States Supreme Court explicitly stated: "[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer." 

Another possible method of limiting the plain view doctrine is for courts to dictate the use of only certain search tools. Police use a variety of search tools when searching digital property such as EnCase® Forensic and Forensic Toolkit®. Without going into technical detail, these search tools are computer programs that search based on specific criteria. These utilities are flawed because computers and other digital property continue to evolve. At least one court has noted the flaws of such search tools; the Harding court notes how "carving utilities," which search based on file characteristics, are flawed because data can exist in numerous formats, e.g., text converted into images. In any case, courts would have to choose among the gamut of forensic software programs and perhaps even set up certification systems; having the courts choose which software search tools are adequate is impractical. Professor Kerr wrote about a theoretical "Perfect Tool" that could "magically locate evidence in a warrant." That Perfect Tool would help police enormously and obviate the need for searching through a suspect's property with a fine tooth comb. Unfortunately, a Perfect Tool will likely never exist because technology will continue to evolve and hackers will find ways around search algorithms. In order to adequately search digital property, police will have to examine everything.

Professor Kerr has also examined the possibility of assessing admissibility based on the reasonableness of particular forensic steps. The difficulty with limiting searches by forensic step is that courts would have to determine whether a forensic step is inappropriate on a case by case basis. Ad hoc determinations would likely cause confusion about the

---

168 Id. at 138.
172 Kerr, supra note 2, at 569-70, 579.
173 Kerr, supra note 2, at 570 ("If Perfect Tool were invented, hackers would quickly devise a counterstrategy to disable it.").
174 Kerr, supra note 2, at 579.
175 Professor Kerr dismissed using reasonableness of a forensic step as a solution be-
acceptable limits of searches because courts would likely apply this standard unevenly. Police will probably be more conservative and reduce the scope of their searches in order to not run afoul of the rule. The biggest problem with basing admission of evidence on the reasonableness of a forensic step is that police must search all of a suspect's digital property in order to properly execute a digital property warrant. Assuming that all physical aspects of the execution of a digital property warrant were reasonable, the only remaining forensic steps would be how police sifted through the bits and bytes that make up a suspect's digital property. As previously discussed, there is no Perfect Tool and police have to search all of the digital property to ensure that no data is hidden. Relying on criminals to not hide information is unwise. Therefore, any forensic step dealing with the actual search of information stored in digital property will likely be reasonable.

One intriguing possibility is to limit the plain view doctrine depending on the type of crime being tried. Perhaps the plain view doctrine should be applied to digital evidence relating to murder, but not digital evidence relating to larceny. The challenge with implementing a crime-based plain view filter is that someone will have to determine which crimes should be exempt from the plain view doctrine. If courts have to decide which crimes should be subject to digital plain view, then courts will have to make the decision that the Fourth Amendment only applies sometimes. Perhaps the legislature should decide which crimes deserve to be protected from digital plain view. The problem with that is that Congress has an incentive to expand the list over time. Professor Kerr points out that setting different rules for different crimes may become complicated and that the danger from pretextual searches would still exist.

Thus, limiting the application of digital plain view to certain crimes is extraordinarily problematic.

Another intriguing possibility is an approach advocated by David cause:

First, for reasons explored earlier, it may be difficult for courts to identify exactly when a particular step is reasonable or unreasonable. Second, this standard would require courts to apply the fruit of the poisonous tree doctrine in an unusual context in which the causal connection among steps is unclear.

Kerr, supra note 2, at 580. The author believes that courts would not have to apply the fruit of the poisonous tree doctrine because all forensic steps dealing with the actual sifting of digital data within digital property are almost certainly reasonable.

See Kerr, supra note 2, at 580-82 (building upon the premise set forth by Professor William Stuntz in Local Policing After the Terror, 111 YALE L.J. 2137 (2002), regarding restricting search practices based on whether a crime is related to terrorism).

Kerr, supra note 2, at 581 for a discussion regarding Congressional incentives.

Kerr, supra note 2, at 581.
Ziff. The Ziff approach would only allow plain view digital evidence to be admitted "if the file's incriminating character becomes immediately apparent before it can be determined that the contents of the file are outside of the scope of the warrant."

Ziff's standard is best applied when the evidence is pictorial in nature, such as child pornography. Less obvious and equally, or more, heinous crimes are not immediately apparent. Ziff gives the example of a letter to grandma and states that the Ziff standard "prohibits the officer from reading the contents of the letter." A criminal could easily exploit this limitation by labeling a file "letter to grandma.doc" and then actually having a letter to grandma with evidence of criminal activity hidden within. For example, the letter could be written in code or the criminal information could be at the end of the letter. Better yet, a criminal could also easily embed objects within a file that contain a plethora of data or hide the information in the metadata. Ziff's approach does not appreciate how easy it is to manipulate digital property into something that looks innocuous on the surface. The Ziff standard can easily be circumvented by hiding data in a number of places within a file and overlaying an innocuous layer, much like spam does today. Additionally, the "immediately apparent" standard is almost as subjective as the Tenth Circuit's standard.

Another possible solution is to limit the digital plain view to certain types of defendants. Perhaps courts could reduce protection from the digital plain view for suspects with felony convictions or non-U.S. citizens. This solution is limited because it would be difficult to justify restrictions/exceptions based on most other types of categories of a person.

Partial limitations to the conundrum posed by digital plain view results in only partial solutions. All of the methods of partially limiting the plain view doctrine as applied to digital evidence are flawed in some manner. The only solution left is to completely eliminate the application of the plain view doctrine to digital evidence.

\[179\] Ziff, supra note 83, at 869.

\[180\] Even in the limited context of child pornography, there are additional complications. There is virtual child pornography which does not capture the images of real children, there are adults that look like children, and children that look like adults.

\[181\] Ziff, supra note 83, at 869.


\[183\] Professor Kerr criticized the Ziff approach because (1) some types of evidence are more apparent than others, and (2) courts have applied the immediately apparent requirement less strictly than the Ziff approach would require. Kerr, supra note 2, at 582.
C. Completely Eliminating the Plain View Doctrine for Digital Evidence

Abolishing the application of the plain view doctrine to digital evidence is perhaps the most drastic action that can be taken to remedy the problem of digital property searches turning into general searches. Several commentators have entertained the notion of abolishing the plain view doctrine for digital evidence, but those commentators have shied away from supporting that proposition. Some courts also seem hesitant to confront the issue. Other courts seem willing to allow general searches to arise from application of the plain view doctrine to digital evidence. As discussed above, the status quo is unacceptable, as are partial limitations. The only satisfactory solution is to completely eliminate the application of the plain view doctrine to digital evidence.

The most compelling reason for eliminating the application of the plain view doctrine to digital property is that the Fourth Amendment was created to combat general warrants, yet the digital plain view currently allows for general searches of a suspect's digital property. Eliminating digital plain view will help courts avoid the dangers of gauging subjective intent that the Tenth Circuit has been engaging in. This new standard recognizes that no Perfect Tool, one that returns only the digital evidence that police are searching for, exists. This approach thus recognizes that criminals will attempt to conceal evidence. Police must comprehensively search a suspect's digital property in order to properly execute a warrant. In fact, law enforcement, including the FBI, currently trains its analysts accordingly. Eliminating digital plain view creates a bright-line rule that provides a clearer standard for police to apply. This solution obviates the need to dissemble on the part of police and deters police misconduct. Abolishing digital plain view allows police the most flexibility to conduct forensic searches of digital property. Police do not have to rely on criminals clearly labeling or otherwise categorizing their files. This will also provide society with real protection for their privacy with the added benefit that the law would be more in line with society's expectations.

Eliminating the plain view doctrine for digital evidence does have its downsides. Courts would have to distinguish digital property from other types of property and justify deviation from plain view doctrine precedent that applies to the physical world. Police would lose a valuable tool that would allow them to use any evidence of criminal conduct found during a

---

184 E.g., Kerr, supra note 2, at 583 (opining that "[i]t is too early for courts or Congress to impose such a rule" that would abolish the plain view doctrine); Ziff, supra note 83, at 868. Professor Kerr does not explain why he believes it is too early to abolish the plain view doctrine.

185 Kerr, supra note 2, at 578-79.
digital property search. Society may suffer from unintended consequences such as unpunished criminal conduct. Thus far, most digital property plain view cases seem to involve child pornography and, of course, there is nobody who wants criminal pedophiles to escape justice. Our system is, however, designed to protect the innocent and, unfortunately, this means that some guilty parties benefit.

Yet the pros outweigh the cons. The arguments in favor of completely eliminating the plain view doctrine for digital evidence have been discussed in detail throughout this article. Courts are already applying the plain view doctrine in a way that permits general searches.\textsuperscript{186} The courts benefit, the police benefit, and the people benefit from the elimination of the plain view doctrine for digital evidence. This clear standard allows more consistent application of the law. Police and prosecutors will still be able to obtain evidence of malfeasance through independent sources and inevitable discovery.\textsuperscript{187}

We should nip the problem in the bud and not let it develop into a problem with widespread impacts. Although eliminating digital plain view is drastic, it is also the only effective way of forestalling the negative effects of the plain view doctrine’s application.

VI. CONCLUSION

Digital property is an inextricable part of our lives. Warrants for digital property are transforming into a species of \textit{de facto} general warrants because police, by necessity, must perform a comprehensive search of a suspect’s digital property in order to properly execute a digital property warrant. General searches are proscribed by the Fourth Amendment and thus, are bad. Also, digital plain view increases the risk of pretextual and “dragnet” searches. The possibility of general searches of digital property is not a hollow threat; courts have already begun to apply the plain view doctrine in a manner that allows police to use anything found during a search of digital property as evidence of crimes beyond the scope of the warrant. Thus, the status quo is unacceptable. This article examined several possible solutions that avoided the elimination of digital plain view, but those solutions proved deficient. The only complete solution is to eliminate digital plain view.

The courts, police, and society will all benefit from eliminating the application of the plain view doctrine to digital evidence. Courts will be able to apply a bright-line rule. Police misconduct will be deterred. Police

\textsuperscript{186} \textit{See supra} Part IV.

\textsuperscript{187} Professor Kerr briefly discusses this. Kerr, \textit{supra} note 2, at 584.
will be able to properly execute warrants to search digital property. People's privacy will be protected. Most significantly, the spirit of the Fourth Amendment and its censure of general searches will be respected.

A forensic specialist once noted: "Most people don't think of the computer as a continually running tape recorder... But it is. It's the closest thing we have in our culture to something that's recording our every thought and every word." Digital data created by computers and other electronic devices will continue to record and penetrate more deeply into our lives. If we do not eliminate the application of the plain view doctrine to digital evidence, then general searches of digital property birthed by the plain view doctrine will become more prevalent and more dangerous to our liberty.

---
