Plain View

Priscilla M. Grantham
Sr. Research Counsel
Nat’l Center for Justice and the Rule of Law

Copyright © 2010 National Center for Justice and the Rule of Law

NCJRL.org
Objectives

1. List factors necessary to satisfy requirements of the plain view doctrine

2. Evaluate whether conditions have been met to uphold seizure of evidence under the PVD

3. Identify & analyze issues inherent in applying the PVD to seizure of evidence located in digital devices
While the plain view doctrine is often considered an exception to the general rule that warrantless searches are presumptively unreasonable, an officer’s observation of an item left in plain view generally does not constitute a search under the Fourth Amendment.


One generally does not have a legitimate expectation of privacy in contraband left out in the open which is viewed by an officer from a lawful vantage point.


A *seizure* of property in plain view does not implicate the individual’s privacy interests; rather, it “deprives the individual of dominion over his or her property.”


Discussing the definition of *seizure* in the context of property, the Court in *United States v. Jacobsen*, 466 109 , 114 (1984) stated that “a seizure of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.”

*Notes:*

__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
Although the parameters of the plain view exception were first established in *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), the Court refined the requirements which must be met to uphold plain view seizures in *Horton v. California*, 496 U.S. 128 (1990).

*Horton* sets out the three conditions which must be satisfied in order to uphold a seizure under the plain view doctrine:

1. the item must be in plain view of the officer,
2. the officer must lawfully be in the place where he discovered the evidence, and
3. the incriminating nature of the evidence must be immediately apparent.


Notes:
Prior Valid Intrusion:
Police must not have violated 4/A in arriving at place from which evidence can be plainly seen.

- Police have search warrant
- Intrusion supported by recognized exception to warrant requirement
  - exigency, consent, etc.

A seizure is proper under the plain view doctrine only if the officer did not violate the constitutional guaranty concerning searches and seizures in arriving at the place from which the item could be plainly viewed.


Whether property in plain view may be seized turns on the legality of the intrusion that enables officers to perceive and physically seize the property.


In order to be deemed a “prior valid intrusion,” the search or seizure that enabled to police to be in the location from which he made his or her observation must be reasonable within the meaning of the Fourth Amendment.


The initial intrusion by the police may be supported by a search warrant or one of the other recognized exceptions to the warrant requirement.

*Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971). See also *State v. Venzen*, 649 S.E.2d 851, 853-54 (Ga. App. 2007) (exigent circumstances existed for officers to seize contraband without search warrant when they were at location to serve arrest warrant and defendant opened door holding marijuana cigarette; if officers retreated to obtain search warrant, the contraband would have likely been destroyed); *Baker v. State*, 802 So.2d 77 (Miss. 2001) (exigency); *State v. Eady*, 733 A.2d 112 (Conn. 1999) (incriminating evidence observed during warrantless entry into residence to extinguish a fire is admissible); *State v. Malady*, 672 S.W.2d 171, 173 (Mo. Ct. App. 1984) (initial search enabling police to see stolen property was conducted with consent of the defendant).

Notes:
Whether an exigency exists justifying a warrantless entry is determined by the particular facts of the case.

The Court of Appeals of Alaska reiterated the findings of a number of other courts in setting forth these three elements necessary to justify a warrantless entry under the emergency aid doctrine.


If it has been determined that an emergency existed and that the officer’s conduct was motivated by the need to render aid, officers judgment as to the method of dealing with the emergency should be accorded wide latitude.


Officer’s subjective motives are irrelevant in determining whether a warrantless entry is justifiable under the exigent circumstances exception to the warrant requirement.

_Brigham City, Utah v. Stuart_, 547 U.S. 398, 404 (2006). See also _Scott v. United States_, 436 U.S. 128 (1978) (an action is “reasonable” under the Fourth Amendment, regardless of the individual officer’s state of mind, if the circumstances, viewed objectively, justify the action); _Bond v. United States_, 529 U.S. 334, 338, n. 2 (2000) (subjective intent of law enforcement is irrelevant in determining whether that officer’s actions violate the Fourth Amendment ...; “the issue is not his state of mind, but the objective effect of his actions”); _Whren v. United States_, 517 U.S. 806 (1996) (“[W]e have been unwilling to entertain Fourth Amendment challenges based on the actual motivations of individual officers”); _Graham v. Connor_, 490 U.S. 386 (1989) (“[O]ur prior cases make clear” that “the subjective motivations of the individual officers ... ha[ve] no bearing on whether a particular seizure is ‘unreasonable’ under the Fourth Amendment”).

_Notes:
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
While searches and seizures inside a home without a warrant are presumptively unreasonable, Groh v. Ramirez, 540 U.S. 551, 559 (2004) (quoting Payton v. New York, 445 U.S. 573 (1980) the ultimate touchstone of the Fourth Amendment is “reasonableness,” and as such, the warrant requirement is subject to certain exceptions.


Police are not required to obtain a search warrant to enter a home if the gravity of the situation makes the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.”


There may be situations in which a police officer gains entrance to a home because of the existence of an exigent circumstance requiring swift action without first obtaining a warrant or consent. State v. David, 502 S.E.2d 494 (1998). The presence of an emergency justifies the officer’s failure to comply with the warrant requirement thus rendering his entry reasonable under the Fourth Amendment. As such, any contraband or evidence of a crime that he sees in plain view may be lawfully seized.


Notes:
The Eighth Circuit employs an “antecedent inquiry,” which focuses on “the reasonableness and propriety of the investigative tactics that generated the exigency.” The Court explicitly stated that officers need not be acting in bad faith to run afoul of this standard.

*United States v. Duchi*, 906 F.2d 1278, 1284 (8th Cir. 1990).

Likewise, the Third Circuit examines the reasonableness and propriety of police action and tactics that preceded their warrantless entry.

*United States v. Coles*, 437 F.3d 361, 370 (3rd Cir. 2006).

The proper analysis is whether, regardless of good faith, it was reasonably foreseeable that the investigative tactics used by the police would create the exigent circumstances relied upon to justify their warrantless entry.


The Fifth Circuit employs a two part test:

1. Did the police deliberately create the exigent circumstances with the bad faith intent to intentionally avoid the warrant requirement, and
2. even if they did not act in bad faith, were their actions that created the exigency so unreasonable or improper so as to preclude an exemption from the warrant requirement?


In *King v. Commonwealth*, 302 S.W.2d 649, 656 (Ky. 2010) the Supreme Court of Kentucky adopted a two part test (essentially a hybrid of the Fifth Circuit’s two part test and the standard employed by the Arkansas Supreme Court) holding that

1. Courts must determine if the officers deliberately created the exigent circumstances with the bad faith intent to avoid the warrant requirement. If so, police cannot rely on the resulting exigency.


2. If police have not acted in bad faith, courts must determine “[w]hether, regardless of good faith, it was reasonably foreseeable that the investigative tactics employed by the police would create the exigent circumstances relied upon to justify a warrantless entry.” If so, then the exigent circumstances cannot justify the warrantless entry. *Mann v. State*, 161 S.W.3d at 834.

Notes:
While not requiring a showing of bad faith, the Sixth Circuit requires “some showing of deliberate conduct on the part of the police evincing an effort intentionally to avoid the warrant requirement.”

United States v. Chambers, 395 F.3d 563, 566-69 (6th Cir. 2005) (quoting Ewolski v. City of Brunswick, 287 F.3d 492, 504 (6th Cir. 2002)).

The Second Circuit gives a great deal of deference to law enforcement, holding that police do not impermissibly create exigent circumstances when they are acting in an entirely lawful manner. An inquiry into the reasonableness of the investigative tactics that preceded the exigency does not appear to be a part of the analysis employed by the Second Circuit.

United States v. MacDonald, 916 F.2d 766, 772 (2nd Cir. 1990).

Notes:

___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
___________________________________________________________________________________
Exigent circumstances may be deemed to exist when there are real, immediate, and serious consequences that would occur if police were to delay action to obtain a warrant. *Estate of Bing v. City of Whitehall, Ohio*, 373 F. Supp. 2d 770 (S.D. Ohio 2005). This emergency doctrine permits a warrantless entry into a home when the circumstances call for immediate entry incident to the service and protective functions of the police as opposed to, or as a complement to, their law enforcement functions.


Officers do not need iron-clad proof of a likely serious, life-threatening injury to invoke the emergency aid exception as long as there is an objectively reasonable basis for believing that medical assistance was needed or that persons were in danger. In *Michigan v. Fisher*, police responding to a report of a disturbance approached the home of defendant and noticed a truck in the driveway with its front smashed, damaged fence posts along the side of the property, broken house windows with the glass still on the ground outside of the home, and blood on the hood of the pickup as well as on the door of the house. Through the window the officers saw defendant (who had a bloody hand) screaming and throwing things. Defendant did not respond to officer’s knocks or inquiries as to whether he needed assistance; instead, he shouted at officers to get a warrant. The officer pushed the front door open, ventured inside then withdrew when defendant pointed a gun at him. The Supreme Court held that the officer’s entry was reasonable under the emergency aid exception, as it was objectively reasonable to believe that the defendant had hurt himself and needed treatment or that he might hurt, or had already hurt, someone else.


Notes:
The “hot pursuit” of a fleeing suspect (accompanied by probable cause) is an exigent circumstance that justifies the warrantless entry into a home.


An important element of the hot pursuit exception is the suspect’s knowledge that he is being pursued.

United States v. Santana, 427 U.S. 38, 43 (1976) (once defendant saw police, there was a realistic expectation that any delay would result in destruction of evidence); King v. Commonwealth, 302 S.W. 3d 649, 653 (Ky. 2010); see also State v. Nichols, 484 S.E.2d 507, 508 (Ga. 1997) (key to hot pursuit is that defendant is aware he is being pursued by the police and is therefore likely to destroy evidence if officer takes time to get a warrant).

The warrantless entry into an apartment was upheld under the emergency doctrine based on officer’s belief that the occupant was operating a meth lab, which could explode at any moment and endanger many lives.

United States v. Cervantes, 219 F.3d 882 (9th Cir. 2000).

Notes:

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
A plurality of the Court in Coolidge stated that the warrantless seizure of evidence of crime in plain view is prohibited by the Fourth Amendment if the discovery of the evidence was not inadvertent. This requirement was not accepted by a majority of the Court and was rejected altogether in Horton v. California. The Horton Court noted that a determination as to whether a discovery was inadvertent focuses the inquiry on the officer’s subjective state of mind instead of the objective standard adopted under the totality of the circumstances approach in which reasonableness is measured.


Despite the fact that the Supreme Court abandoned the inadvertency requirement in Horton, some states still require that in order to be admissible under the plain view doctrine, an item must have been inadvertently discovered.

United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. VA. 1999) (clearly incriminating images of child pornography inadvertently discovered in the course of a lawful search admissible under plain view doctrine); Hunt v. Commonwealth, 304 S.W.3d 15, 27 (KY. 2009) (“law enforcement officials may seize evidence without a warrant when the initial entry was lawful, the evidence was inadvertently discovered, and the incriminating nature was readily apparent”); Commonwealth v. Balicki, 762 N.E.2d 290, 298 (Mass. 2002) (declining to eliminate the inadvertency requirement finding that such a requirement protects the possessory interests conferred on its citizens under article 14.); State v. Meyer, 893 P.2d 159, 165 (HI 1995) (court adopted all three of the requirements set forth in Coolidge, including inadvertent discovery.)

In United States v. Carey, the Tenth Circuit seemed to read a requirement of inadvertence into the plain view doctrine. In Cary, the police was searching defendant’s computer for evidence of drug trafficking and noticed several JPG files with sexually explicit file names. He opened one of the JPG files and upon discovering child pornography, viewed approximately 95 more files. According to the officer’s testimony, each time he opened an additional JPG file he expected to find child pornography. The court reasoned that the contents of these files were not inadvertently discovered, and therefore not admissible under the plain view doctrine.

United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

Notes:
The “immediately apparent” requirement mandates that there be a nexus between the viewed object and illegality before the police can seize the object. The officer need not possess certain knowledge as long as the facts available to the officer would warrant a man of reasonable caution in the belief that the item was contraband or evidence of a crime. Police may rely on his expertise and experience to determine that an object is incriminating.


Generally, the more effort the police use to “discover” the additionally incriminating evidence, the less likely it is that the immediately apparent” requirement will be met. In *Arizona v. Hicks*, the police entered an apartment after a shot was fired from within. While in the apartment, the police saw stereo equipment they suspected was stolen and therefore moved the components in order to find and record the serial numbers. The Court found that moving the equipment constituted a search, separate from the search for the shooter, victims and weapons that predicated the officer’s entry into the apartment. Stating that the plain view doctrine can apply to a search as well as a seizure, the Court addressed the issue as to whether the search was reasonable. The Court concluded that the separate search would be valid as long as the plain view doctrine would have sustained a seizure of the stereo equipment; however, since the officer did not have probable cause to believe the stereo equipment was stolen, the plain view doctrine was not applicable.


Seizure of defendant’s computer was not justified under the plain view doctrine; discovery by police of bookmarks with references to teenagers might constitute reasonable suspicion that the computer contained child pornography, but did not rise to the requisite level of probable cause.


That is, while police might have some degree of suspicion that something they see in the course of a lawful search is contraband or evidence of criminality, they may not do anything that constitutes a new search to gain the requisite probable cause.


*Notes:*
The permissible scope of a search is usually determined by the objects sought. In the case of a search authorized by a warrant, an officer is permitted to search anywhere that the items particularly described in the warrant could be located. If an officer is looking for a bloody knife, he can look anywhere that the knife could be hidden, e.g., the medicine cabinet, kitchen drawer, between the mattresses. If he is looking instead for a stolen 72 inch flat screen television, he is limited to searching only in those places where an item of this size could be located. As long as the police is within the scope of his search when he sees in plain view an item that is contraband or evidence of a crime, the item is admissible under the plain view doctrine. What this means, practically speaking, is that only the objects that are visible from a lawful vantage point are considered to be “in plain view.”

Notes:

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

_________________________________________
Application to Digital Evidence

- If police is validly in position to see computer and sees material on screen that's clearly incriminating, it's considered plain view.
- As to observation of contents of unopened files, depends on how court defines a search for data in a computer.

Material on the Computer Screen

If police are lawfully in a place and see an image or document on a computer screen and its incriminating nature is immediately apparent, their observations will be considered in plain view and the evidence may be seized under the plain view doctrine.

See United States v. Tanksley, 50 M.J. 609 (N.M. Ct. Crim. App. 1999); State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604-05 (Okla. Ct. App. 1994) (during execution of a search warrant based on allegations that the suspect was distributing pornographic material, police observations of computer monitor “displaying the words ‘viewing’ and/or ‘copying’ with descriptions such as ‘lesbian sex’ and/or ‘oral sex’” established that the equipment and its possible criminal use were in plain view).

Contents of Unopened Files:

Courts adopting the “computer as container” approach view data in a computer as simply another form of document; therefore, a search warrant for writings or records encompasses a search of computer files. If a search for computer data is merely a document search, police are bound by the same rules whether the information is in a computer, a desk, or a filing cabinet.


Other courts reject the filing cabinet analogy, finding that it is too simplistic in light of the variety and vast quantity of information that is stored in computers; therefore law enforcement must take a “special approach” when searching for data on a computer.

United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

Notes:
Defendant was arrested for disorderly conduct for videotaping children at the zoo. Officers went to the defendant’s home where they were met by defendant’s father. The officers told the father about the arrest of his son and received consent to search defendant’s computer. The officer discovered “bookmarks with references to teenagers and so forth.” This discovery and the fact that defendant had been arrested for disorderly conduct would not warrant a person of reasonable caution to believe that the computer contained child pornography. At most, defendant’s behavior at the zoo and the unqualified references to teenagers constitute reasonable suspicion. Such ambiguous facts, however, do not rise to the level of probable cause.


_Notes:_

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
Caveat

Police might believe the contraband... Might be reasonable suspicion, but not PC for teenagers.

Notes:

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

Material on Computer Screen:

U.S. v. Tanksley
(U.S. Navy-Marine Corps Ct. Crim. Appela)

• Appellant authorized to use office & computer for pending legal case

• While editing document on computer, he was called away, apprehended for confinement

_______________________________________________________________________________
Material on Computer Screen:

Confidential Background Information on Accusations Made Against Me in Regards to Child Abuse While My Family and Me Were House Guests of MP on Aug 25 & 26
Tanksley
Agent was legitimately securing office used by appellant.

Contents of document appeared on the computer screen in plain view.

An examination of this document by the agent gave him probable cause to seize it and it was proper to do so.

Notes:

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
In *State v. Mays* police were lawfully in defendant’s home to investigate the claim made by the defendant that the victim had assaulted her. The defendant invited the officers in, and in the course of looking for signs of a struggle, police saw the message “[H]e will die today” on the computer screen. The court held that the warrantless seizure of the computer was justified under the plain view doctrine, as the message was clearly indicative of criminal activity.


**Notes:**

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

On Computer Screen

*State v. Mays*

- D. calls 911 twice re: domestic dispute
- Next day, D.’s bf hospitalized after calling 911
- Police at hospital asked officers to visit D.’s home
- D invites officers in – shows them “evidence” of assault

-- (22)
Material on Computer Screen:

He will die today.
• Valid intrusion?

• Plain View?

• Incriminating nature immediately apparent?

Notes:

__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
What is a computer?
The question as to what constitutes plain view in the context of computer files is an issue that has not been resolved by the courts. The determination rests largely on how the court views computers and searches of computers. Many courts view computers as containers capable of storing information (albeit in digital form) just as a filing cabinet stores paper records and documents. Courts adopting the “computer as container” approach view data in a computer as simply another form of document; therefore, a search warrant for writings or records encompasses a search of computer files. If a search for computer data is merely a document search, police are bound by the same rules whether the information is in a computer, a desk, or a filing cabinet.


Relying on analogies to closed containers or file cabinets oversimplifies the complexities of applying the doctrines of the Fourth Amendment to the realities of emerging technology and the massive storage capacity of computers. The file cabinet analogy may be inadequate due to the fact that electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, and as such, computers make “tempting targets in searches for incriminating information.”


Notes:
When applying the plain view doctrine in situations where evidence was discovered during the course of a search of a computer or other digital device, the admissibility of said evidence hinges on the manner in which a court classifies a search for data in a computer.

If the court determines that the search of a computer is akin to a traditional document search, traditional rules apply and an officer conducting a search of a computer can look anywhere in the computer in which the data could be stored. If in the course of his search he discovers evidence that is clearly incriminating on its face, the evidence will be admissible under the plain view doctrine, as the officer did not violate the Fourth Amendment in arriving at the vantage point from which he saw the evidence.

If, however, a court is of the opinion that traditional Fourth Amendment doctrine does not apply to searches of computers because of their ability to store massive amounts of data, (including personal information) the applicability of the plain view doctrine will be considerably restricted. Courts employing the “special approach” to searches of computers require officers to employ special methods, such as searching according to file types, titles, dates, etc. to avoid searching files not of the type specified in the warrant. What this means in practical terms is that an officer who is authorized only to look at files of a certain type, (i.e., “.wpd” or “.doc”) while conducting a search of a computer may not examine a file titled “preteensex.jpg.” If he does so and discovers child pornography, the image will not be admissible under the plain view doctrine since he was not within the scope of the authorized search, therefore, the image was not discovered from a lawful vantage point.

Notes:
The Tenth Circuit in *Carey* held that when searching computers, officers should employ special methods, such as searching according to the file types or titles listed in the directory, to avoid searching files not of the type specified in the warrant. Furthermore, when police come across intermingled documents, they must engage in the intermediate step of sorting the documents and searching only those specified in the warrant.

*United States v. Carey*, 172 F.3d at 1276.

**Notes:**

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

“Special Approach”

*Carey* (10th Cir. 1999)

Police must employ methods to avoid searching files not specified in warrant; e.g., limit search by:

- File types / titles listed on directory
- Key words
- Dates
In *Carey*, an investigator was searching a computer pursuant to a warrant to search for records of drug distribution when he came across an image that appeared to be child pornography. The detective continued to open additional JPG files in order to confirm that they contained child pornography. The court found that the *first* image of child pornography was admissible under the plain view doctrine because the investigator had to open the file and examine the contents to determine what the file contained. By opening the additional JPG files in which he expected to find child pornography, the detective abandoned his original authorized search for evidence of drug trafficking and began a new search for evidence of child pornography. The court held that the additional images of child pornography were inadmissible since they were not authorized by the warrant. Although declining to rule on the issue of what constitutes plain view in the context of computer files, the Tenth Circuit said that the images of child pornography were not in plain view because they were located in closed files.

*United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999).

**Notes:**

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
A requirement that police limit their searches to files that are labeled in a certain way “would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled ‘flour’ or ‘talcum powder.’ 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. The ease with which child pornography images can be disguised – whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated-forecloses defendant’s proposed search methodology.”

*United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006) (citing *United States v. Hill*, 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004); see also *United States v. Adjani*, 452 F.3d 1140, 1149 (9th Cir. 2006) (in executing a search of a computer, officers not required to restrict search to specified key words within particular email programs; to do so would likely result in failure to acquire evidence sought).

*Notes:*
In *Osorio*, agents had a search warrant to search appellant’s laptop computer for photos relating to an alleged sexual assault that occurred at a party. The appellant was not under any suspicion of wrong doing. The magistrate limited the scope of the search warrant by the date of the photos. The agent hard drive then confirmed the copy was an exact mirror image of the hard drive by using forensic software to view all photos as thumbnail images.

Like in *Carey*, the *Osorio* court found the agent’s intent to be a significant factor on the issue of scope. That is, the agent saw what appeared to be nude people in the thumbnail images but was unable to confirm that the images contained children until she double clicked an image to enlarge it. According to her testimony, she opened the image not to verify it was a mirror image of the other computer but, to make sure it wasn’t contraband. The court found that the agent’s acts ran afoul of the well-settled principle that that the plain view doctrine may “not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” Agent was outside the scope of the warrant; images not admissible under plain view doctrine.


Notes:
The Court held that the inspection of the files which contained child pornography exceeded the authorized scope of the authorized search. In rejecting the argument that the images of child pornography were admissible under the plain view doctrine, the Osorio court noted that opening thumbnails was on par with moving an object, and the “distinction between looking at a suspicious object in plain view and moving it even a few inches is much more than trivial for the purpose of the Fourth Amendment.”


There are several interesting facts at play in Osorio. The first relates to the language of the search warrant that authorized the agent to search for photos relating to a certain date. Such a search would miss any relevant photos if the image had been accessed after its date of creation. For example, the agent would likely miss any photos that were pulled up for printing, editing, or viewing unless these acts occurred on the day that the pictures were created.

**Notes:**
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
See, e.g., *United States v. Gray*, 78 F. Supp. 2d 524, 531 n.11 (E.D. Va. 1999) (when an agent is engaged in a “systematic search” of computer files pursuant to a warrant, and, as long as he is searching for the items listed in the warrant, any evidence discovered in the course of that search could be seized under the “plain view” doctrine); *Commonwealth v. Hinds*, 768 N.E.2d 1067, 1072 (Mass. 2002) (police had right to open file that officer believed contained child pornography based on the file’s name during valid search of computer for email; accordingly, child pornography was in plain view); *State v. Schroeder*, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (rejecting limitations on a search based on file names and concluding that, during systematic search of all user-created files in executing a search warrant for evidence of online harassment and disorderly conduct, opening file containing child pornography in plain view); *Frasier v. State*, 794 N.E.2d 449, 462-66 (Ind. Ct. App. 2003) (rejecting limitations on a search based on file names and extensions, and concluding that the plain view doctrine applied when the police opened a file and observed child pornography during the execution of a warrant permitting the police to examine notes and records for evidence of drug trafficking). Cf. *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (under warrant permitting search of graphic files for evidence of murder, observations of files containing child pornography were in plain view); *United States v. Tucker*, 305 F.3d 1193, 1202-03 (10th Cir. 2002) (parole agreement authorized search of computer; upon viewing child pornography on it, plain view doctrine permitted warrantless seizure).

Notes:
In *United States v. Gray*, agents executed a search warrant at defendant’s home in connection with a hacking violation. The agent conducting the search opened a directory in order to see a list of the individual files and subdirectories located within. Pursuant to his usual practice, he began systematically opening the files and subdirectories within the directory. The agent opened a subdirectory entitled “Teen,” that contained pornographic images. Continuing his search for items listed in the warrant, the agent subsequently opened a file entitled “Tiny Teen,” that also contained images the agent suspected were child pornography.

In denying the motion to suppress the images of child pornography, the court began its analysis by taking note that the Fourth Amendment requires the items sought by the warrant to be listed with particularity sufficient to enable an officer to determine with reasonable certainty the items he is authorized to seize. Whereas an officer might have little problem making this determination when he discovers weapons during a search for weapons, the same cannot be said when the search is for documents or records. When it is not immediately obvious if a certain item is within the scope of the warrant, the officer must examine the object to make the determination.

The Court analogized searches of computers to searches for paper documents located in files, and noted that a warrant authorizing agents to search a home or office for documents containing certain information entitles the agents to examine all of the documents at the site to determine if it’s responsive to the warrant.

The court held that the evidence found in the subdirectories was admissible under the plain view doctrine: the agent was entitled to examine all of the defendant’s files to determine if they contained the information specified by the warrant, and in doing so discovered images that were clearly incriminating on their face.


Notes:
In *Schroeder*, investigators had a search warrant to seize defendant’s computer in order to search for evidence of online harassment. As was his usual procedure, the agent began systematically opening all user created files and in the course of doing so opened a file containing what appeared to be child pornography. The court said the procedure used by the agent was a sensible one; limiting a search to the types of evidence sought would enable a defendant to easily hide computer evidence; i.e., police would not be authorized to search for child pornography in a file labeled “1986.taxreturn.”

The court in *State v. Schroeder* rejected the idea that computer searches require a special approach. The court held that the image was admissible under the plain view doctrine finding that the discovery of child pornography “… was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks.”


**Notes:**

__________________________________________________________

__________________________________________________________

__________________________________________________________

__________________________________________________________

__________________________________________________________

__________________________________________________________

__________________________________________________________

__________________________________________________________
**Better Safe than Sorry ...**

When searching computer for data specified in warrant (i.e., evidence of tax fraud) investigator discovers evidence of a *different* crime (i.e., CP), *safest* practice:

1. Suspend search,
2. Get 2d warrant encompassing new evidence,
3. Then resume search

---

**Notes:**

__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
“When the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium in searching for certain incriminating files, or when a search for evidence could result in the seizure of a computer … magistrate judges must be vigilant in observing the guidance we have set out throughout our opinion, which can be summed up as follows:

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

_U.S. v. Comprehensive Drug Testing_, is interesting, perhaps even astonishing, for many reasons. It has the effect of banning plain view in the context of computer searches through the creation of a set of prophylactic rules. The guidelines ensure that the government can never be in position from which it could discover evidence in plain view. Will magistrates now refuse to sign otherwise valid search warrants, i.e., based on probable cause and comporting with the particularity clause, if they are not satisfied with the government’s explanation as to manner in which the warrant will be executed?

**Notes:**
Balco

2. Segregation and redaction must either be done by specialized personnel or an independent third party. If segregation is to be done by government computer personnel, it must agree in warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
Balco

3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
**Balco**

4. The government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
Balco

5. The government must destroy or, if the recipient may lawfully possess it, return the non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.
Chief Judge Kozinski’s opinion in CDT is quite a departure from that which he issued in 2004 in *United States v. Hill*, a case that also dealt with issues relating to the execution of search warrants for computers and other digital media. The Ninth Circuit agreed with Kozinski’s opinion that (1) due to fact that computer searches often involve intermingled materials that are difficult and time consuming to separate on-site, it is reasonable to seize all media and take it off-site for examination by an expert. The Ninth Circuit relied on Judge Kozinski’s language in addressing the question of search methodology, holding that it is unreasonable to force police to limit their searches to files that the suspect has labeled in a particular way.

“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.”


**Notes:**

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

_____________________________________________________
2. Warrant NOT overbroad based on failure to define “search methodology.”

It is unreasonable to force police to limit their searches to files that the suspect has labeled in a particular way.

“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.”

Ease w/ which c.p. images can be disguised forecloses D’s proposed search methodology.

States v. Comprehensive Drug Testing, 2009 WL 2605378 (9th Cir. (Cal.)).
United States v. Hill, 322 F. Supp.2d 1081 (C.D. Cal. 2004), aff’d, 459 F.3d 966 (9th Cir. 2006).
United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006).

Id. at 978, quoting, United States v. Hill, 322 F. Supp.2d 1081, 1089-91 (C.D. Cal. 2004).
ReCap

1. Factors necessary to satisfy requirements of the plain view doctrine

2. Have conditions been met to uphold seizure of evidence under the PVD?

3. Analyzed issues inherent in applying the PVD to the seizure of evidence located in digital devices
Thank You

Priscilla M. Grantham
pgadams@olemiss.edu
(662)915-6929

NCJRL.org