# Computer Searches and Plain View

**Author :** Jeff Welty

**Categories :** Uncategorized

**Tagged as :** computer searches, digital evidence, fourth amendment, plain view, Search and Seizure

**Date :** November 21, 2013

Whether the plain view doctrine makes sense in the context of computer searches, and if it doesn't, what courts should do about it, are controversial issues. We don't have any North Carolina case law on point but decisions are piling up around the country. This post summarizes the controversy.

**Computer searches may be very thorough.** Generally, courts have held that when an officer is entitled to search a computer for evidence of a crime, the officer may review every file on the computer. This is because of the ease with which files can be camouflaged or disguised through misleading file names or extensions. *See, e.g., United States v. Stabile,* 633 F.3d 219 (3rd Cir. 2011) (searching video files pursuant to search warrant for financial crimes was "objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband," and "the plain view doctrine applies to seizures of evidence during searches of computer files, [though] the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner"); United States v. Williams, 592 F.3d 511 (4th Cir. 2010) (stating that a computer search requires "at least a cursory review of each file on the computer").

**Broad computer searches may bring evidence of other crimes into view.** Because of the broad scope of computer searches, they require officers to sift through large amounts of information unrelated to the crime under investigation. As a result, officers executing computer search warrants often encounter evidence of crimes other than those based on which the warrants were issued. Commentators have suggested for years that computer searches are different in degree, and perhaps in kind, from other types of searches in this regard. *See, e.g.,* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L.Rev. 531 (2005) (stating that "computer technologies may allow warrants that are particular on their face to become general warrants in practice"); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L.Rev. In Brief 1 (2011) ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic.").

**Some courts apply the plain view doctrine.** When an officer searches a physical location pursuant to a search warrant and stumbles upon evidence of a crime other than the one that motivated the search, the evidence is said to be in "plain view," and it may be seized by the officer and used to support a criminal prosecution. Many courts have simply applied the plain view doctrine to computer searches. For example, imagine that an officer is searching a computer under a warrant for evidence related to a homicide, but encounters files containing child pornography. These courts would rule that the plain view doctrine applies to the discovery of the child pornography, and that the officer may continue searching the computer under the original warrant, even though the officer may now subjectively expect to find additional child pornography. *See, e.g., United States v. Williams*, 592 F.3d 511 (4th Cir. 2010) (the defendant sent anonymous emails to a church expressing a sexual interest in some boys who attended school at the church; police obtained a search warrant for "computer systems and digital storage media" indicative of computer harassment or communicating threats; during search, police found child pornography; the court found no Fourth Amendment violation, in part because a computer search requires "at least a cursory review of each file on the computer," bringing the child pornography into plain view); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) (officer obtained search warrant to search the defendant's computer for evidence of voyeurism; he properly searched the image files on the computer systematically, even though he thereby uncovered child pornography; however, the court found it "troubling" that the officer did not stop and seek a second warrant for child pornography).

**Other courts seek to limit plain view as it applies to computer searches.** Other courts have concluded that because computer searches bring so much information to officers' attention, the plain view doctrine must be limited. These cases generally have arisen in the context of searches pursuant to search warrants, and courts have expressed a concern that computer search warrants may amount to general warrants that allow officers to rummage through a suspect's computer for evidence of any wrongdoing.

The cases reflect two main strategies for limiting the effect of the plain view doctrine. One is to require, as a condition of issuing the warrant, that the prosecution forswear reliance on the plain view doctrine. The second is to order that the warrant be executed by a search team behind a "firewall" and that the search team report out to investigators only evidence related to the crime in connection with which the warrant was obtained. *See, e.g., In re Search Warrant*, 71 A.3d 1158 (Vt. 2012) (holding that a judicial official who issued a computer search warrant lacked the authority to prohibit law enforcement from relying on the plain view doctrine, but had the authority to accomplish the same result by requiring that the search be conducted by third parties behind a "firewall," and that the search team provide to investigators only information relevant to the offense that gave rise to the search warrant); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (noting that "over-seizing is an inherent part of the electronic search process" and suggesting that magistrate judges issuing search warrants should take steps to limit the government's access to data for which it has no probable cause, such as requiring an on-site assessment of the feasibility of seizing only responsive data; requiring data segregation to be done by someone other than the case agent; and perhaps limiting the government's plain view rights; Chief Judge Kozinski's concurrence provides more detailed suggestions); *In re United States's Application For A Search Warrant To Seize and Search Electronic Devices From Edward Cunnius*, 770 F.Supp.2d 1138 (W.D. Wash. 2011) ("Because the government, in this application, refuses to conduct its search of the digital devices utilizing a filter team and foreswearing reliance on the plain view doctrine, the Court denies the application as seeking an overbroad or general warrant in violation of the Fourth Amendment"). I would be interested to learn whether any judicial officials in North Carolina have imposed any such requirements on computer search warrants, and if so, how those requirements played out in practice.

**Seeking a second warrant.** Finally, a few courts have attempted to chart a middle ground, holding that the plain view doctrine applies to the initial discovery of unexpected evidence, but that if the officer wishes to continue looking for additional evidence in the same vein, a second warrant is required. *See, e.g., United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (officer obtained search warrant for "evidence pertaining to the sale and distribution of controlled substances"; officer opened .jpg file with sexually suggestive name, apparently because the file could contain a photograph related to drug activity; it contained child pornography; officer continued viewing other .jpg files with sexually suggestive names, finding more child pornography; although the first image was in plain view, by "the officer's own admission . . . each time he opened a subsequent [image] file, he expected to find child pornography and not material related to drugs," so the plain view doctrine did not apply). *But see United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (noting that "we have not required a specific prior authorization along the lines suggested in *Carey* in every computer search"). The courts' focus on the subjective intentions and expectations of the officer is inconsistent with the Supreme Court's repeated emphasis on the objective nature of Fourth Amendment analysis, so this middle ground may be a sinking island. Nonetheless, because North Carolina's appellate courts have yet to rule on the application of the plain view doctrine as it relates to computer searches, a cautious officer may wish to seek a second warrant whenever the focus of his or her search moves away from the crime that gave rise to the warrant.