

# The Legal Intelligencer

Select '**Print**' in your browser menu to print this document.

**Copyright 2010. ALM Media Properties, LLC. All rights reserved. *The Legal Intelligencer.***

Page printed from: [The Legal Intelligencer](#)

[Back to Article](#)

## The Two Views of 'Plain View'

Leonard Deutchman

05-11-2010

*Editor's note: First of two parts*

The "plain view" doctrine of the Fourth Amendment holds that law enforcement properly authorized to be in a certain area can lawfully search and seize evidence seen in plain view from that vantage point.

It is seen as an "exception" to the Fourth Amendment because, under it, searches and seizures are authorized not by judicial power, but by limited circumstances. Typically, the doctrine comes into play when a law enforcement officer is doing something anyone can do, such as driving down a public street, or taking intermediate, investigative steps only law enforcement officers are empowered to do, such as stopping a vehicle on suspicion of having ignored a stop sign.

Sometimes, however, the doctrine applies when a law enforcement officer executes a search warrant while looking for evidence of a certain crime, such as a murder weapon, and comes across evidence of an unrelated crime, such as illegal drugs.

But application of the plain view exception when computers are being searched poses challenges to the doctrine.

The requirement that the viewer must be near what is being viewed imposed physical restrictions to the doctrine, but with a computer search, those physical limitations disappear.

The officer who has stopped the driver for ignoring the stop sign could view only the area immediately around the car, posing no worry to the courts later reviewing the officer's conduct that the officer could have somehow easily segued into searching the driver's bedroom miles away, for example. Given, however, the hundreds of thousands of files that can easily be stored on a computer, and the manner in which a computer search is conducted — looking for keywords, for example, across all files — a computer search is akin to an officer walking into the foyer of a mansion and being able to see in plain view every person and object in the entire structure. Under those circumstances, a search for files pertaining to one crime will often, and easily, yield evidence of wholly unrelated crimes.

How, then, should the plain view doctrine apply to computer searches?

Different courts have provided different answers.

In *United States v. Farlow*, *United States v. Williams*, and *United States v. Mann*, the 1st, 4th and 7th U.S. Circuit Courts of Appeal had no problem applying the doctrine to computer searches. In *United States v. Comprehensive Drug Testing et al.*, however, the 9th Circuit, worried that applying the plain view exception would eviscerate the particularity requirement of the Fourth Amendment, sought to guard against that by requiring that computer searches follow a protocol under which law enforcement officers deeply involved in the investigation would have to forswear the plain view exception and filter all search results through other officers.

In this month's column, we will examine these approaches. This week, we look at the cases that apply the doctrine to computer searches. In the next part of the column, we will look at *Comprehensive Drug Testing* and discuss the pros and cons of following or rejecting the doctrine.

## The Argument for Plain View

United States v. Farlow

In Farlow, the defendant lived in Maine and sent sexually suggestive e-mails to a Long Island, NY police detective posing online as a 14-year-old boy.

The e-mails included "explicit sexual advances and a request for an in-person meeting," in violation of New York law. It also included a non-pornographic image file of a bodybuilder which the defendant represented as himself to the undercover detective. The detective subpoenaed the subscriber information of the defendant's e-mail account and traced him to Maine. The detective then contacted local law enforcement in Maine and asked that they execute a search warrant which, *inter alia*, sought "[c]omputer records or data, whether in printed or electronic form, that are evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a child."

The search yielded images of child pornography and the defendant was charged with possession of it; apparently, though, he was not charged in New York for the crimes leading up to the search.

The defendant argued that the search for the bodybuilder picture could have been accomplished by a "hash value" comparison. A "hash value" for any given set of electronic data, from a small file to an entire hard drive, is obtained by subjecting the set of electronic data to a complex algorithm. The long, alphanumeric string that will result is unique to that data set; thus, any two files with the same hash value will be identical files.

The defendant's argument was that his computer should have been searched by creating hash values for all of his computer's files and comparing them to the hash value of the bodybuilder image. Such a search would have been far more targeted and would not have yielded the child pornography images.

The court disagreed, relying upon a sworn declaration by the Maine State Police Computer Crimes Unit's forensics examiner that a hash value comparison would not have been effective because, if the bodybuilder image residing on the defendant's computer was different from the same image as it resided on the New York detective's computer in even the smallest detail, the hash values would have been completely different.

This assertion is correct: a hash match of files from the defendant's and the New York detective's computers would mean that the matching files were identical, but the failure to obtain a hash match could mean the bodybuilder image did not reside on the defendant's machine or that it did reside there but was changed in only the slightest way, not even visible to the user.

Rejecting the defendant's argument, the 1st Circuit agreed with the prosecutors that the sole way to search for the bodybuilder image was to look at every image on the computer. If during that proper search, child pornography was uncovered, such was the inevitable result.

United States v. Williams

In Williams, a Baptist temple in northern Virginia received e-mails from someone who described himself as a pedophile, mentioned the names of boys who attended the temple school and threatened that he, the sender, would sodomize the boys. The e-mails came from numerous accounts in the names of the boys as well as others related to the temple.

An investigation revealed that at least one account from which the e-mails had been sent had been accessed "repeatedly" by another account registered to the defendant's wife; both the defendant and she were active members of the temple. Police obtained a search warrant for the couple's home, which allowed them to search for and seize all digital media for evidence of the crime of harassment by computer and different variations of the crime of making threats. Police and the FBI executed the warrant and seized "several computers, CDs, DVDs, and other electronic media devices."

A search of at least one computer revealed deleted images of "young male erotica," for example, and a search of a DVD uncovered "over a thousand images in 'thumbnail view' of minor boys, some of which were sexually suggestive and some of which were sexually explicit. Of the total number of images, approximately 39 constituted child pornography."

The defendant's argument in Williams voiced the concern of applying traditional Fourth Amendment concepts to computer searches.

He asserted that since "computers can hold so much information, touching on virtually every aspect of a person's life, the potential for invasion of privacy in a search of electronic evidence is significantly greater than in the context of a non-

computer search," and so "traditional Fourth Amendment rules cannot be successfully applied."

Relying upon an argument made by George Washington University Professor Orin S. Kerr in a 2005 Harvard Law Review article, *Searches and Seizures in a Digital World*, the defendant argued the Fourth Amendment doctrine had been directed towards the world of "physical barriers," such as to a home or a container, for the past 200 years and gave rise to the doctrines we now know. However, as the "architecture of physical searches" gives way to the "new dynamics of computer searches and seizures," we must formulate "a set of rules for digital searches and seizures that attempts to achieve the same purpose" as did the rules governing physical searches, but "in a very different factual context," the defendant argued.

Using Kerr's article as his point of departure, the defendant in *Williams* argued that a computer search warrant "must not be read to have authorized officers to view each file on the computer, but rather to have authorized a search of only those files in his computer that related to the designated state offenses," otherwise the search is a "general search" forbidden by the particularity requirement of the Fourth Amendment. Thus, the defendant argued, "the files relating to child pornography fell outside the scope of the warrant and therefore were seized without a warrant." Furthermore, the defendant argued that to apply the plain-view exception in the context of computer searches would effectively make a dead letter of "the warrant requirement out of the Fourth Amendment."

The prosecutors argued that the child pornography in question "fell within the scope of the search warrant as 'instrumentalities of the designated' crimes. It further argued that, even if the child pornography fell outside of the warrant, "its seizure was nonetheless justified under the plain-view exception to the warrant requirement." The warrant authorized the search of the DVD containing child pornography; once searched, the nature of the DVD "as contraband was clear," the prosecutors argued.

The 4th Circuit agreed that, particularly "in the context of the threats made in this case, which indicated that the person sending the e-mails to the church was a pedophile, pornographic images involving children were relevant to demonstrating the authorship and purpose of the e-mails," and thus fell within the scope of the warrant. The court also agreed with the prosecutors that even if the warrant "did not authorize a search for child pornography," seizure was, "in any event, justified by the plain-view exception to the warrant requirement."

In order to conduct the search authorized by the warrant, the court ruled, "the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."

A search based upon how files were named could not be effective, since "the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality," the ruling continued. Only a search of the actual files could accomplish the ends of the search warrant, and once that search is performed, "the criteria for applying the plain-view exception are readily satisfied." The officer is legally authorized to conduct the search; the officer opens the computer's files; the significance of the viewed evidence as evidence is "immediately apparent" and so it is seized.

The 4th Circuit ultimately found Kerr's concerns not compelling.

"At bottom," the court stated, "we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."

Citing the 1976 U.S. Supreme Court decision *Andresen v. Maryland* for the proposition that there are "grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable," the court nevertheless found that while that danger "certainly counsels care and respect for privacy when executing a warrant, it does not prevent officers from lawfully searching the documents, nor should it undermine their authority to search a computer's files."

United States v. Mann

In *Mann*, the defendant was working as a lifeguard and installed a video camera in the women's locker room to film them changing their clothes.

Presumably by accident, he also filmed himself installing the camera, which was discovered and turned over to the police, who obtained a search warrant for defendant's residence for "video tapes, CD's or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas."

The police officers seized, amongst other things, "a Dell desktop computer with a Samsung hard drive, a Dell laptop, an e-machine, and a Western Digital external hard drive."

The defendant was arrested for voyeurism and, two months later, his digital media were searched.

On the desktop computer, police discovered evidence the defendant had visited a Web site called "Perverts Are Us," where he had read and possibly downloaded stories about child molestation. Police found on the laptop "still images taken in the ... locker room, child pornography, and evidence that the external hard drive had been connected to the laptop." On the e-machine, police found additional child pornography as well as a "disturbing story," presumably authored by defendant, "about a swim coach masturbating while watching young girls swim."

Two months later, police searched the external hard drive. Well-accepted forensic tools did a hash value comparison of the files on the drive to those of known child pornography, which yielded four "Alerts" of positive hash value matches to known child pornography and 677 "flagged thumbnails," i.e., 677 images in "thumbnail" form (not full-sized views) whose contents were not identified. When the analyst opened the files, he discovered "many, many images of child pornography" as well as two videos from the locker room.

The district court denied defendant's motion to suppress.

The district court found "as a factual matter" that the police analyst "believed the search warrant authorized him to examine any digital file located on the computer hard drives or storage devices and that he never abandoned his search for evidence of voyeurism and began looking for child pornography." The district court concluded that "with limited exceptions" the search was within the scope of the warrant, and that "any images uncovered outside the scope of the warrant were discovered in plain view."

On appeal, the defendant argued the search exceeded the scope of the warrant. The court recognized Kerr's observation that computer searches require addressing a "new architecture" of things to be searched but differed with his conclusions. It rejected defendant's argument, reasoning that the "problem with applying" it "to computer searches lies in the fact that such images could be nearly anywhere on the computers. Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents." Thus, limiting the officers search did not limit them to where they could search, because the images they sought "could be essentially anywhere on the computer."

The court accepted the defendant's argument that the four files identified by the "Alert" were outside the scope of the warrant because, once so identified, the police knew that they were not evidence of the crime of voyeurism but, instead, child pornography. Admission of that evidence, however, was harmless, because even without "those images, the government still possessed ample evidence of child pornography to sustain both" the defendant's conviction and sentence.

The court, however, noted it was troubled that the police did not stop the search "and request a separate warrant for child pornography" once it was initially uncovered. Since the police did not face "a rapidly unfolding situation" or find themselves "searching a location where evidence was likely to move or change, there was no downside to halting the search to obtain a second warrant," the court ruled.

Regardless of its "distaste for the timeline of the investigation," the court nevertheless concluded that, with the exception of the four "Alert" images, the warrant authorized the search which led to the discovery of the child pornography found in plain view upon opening the 677 files in an attempt to look for evidence of voyeurism. •

**Leonard Deutchman**, *esquire is general counsel and administrative partner of LDiscovery, LLC, a firm based in New York City, Fort Washington, Pa., McLean, Va. and Chicago that specializes in electronic digital discovery and digital forensics.*