



United States v. Mann
COMPUTER SEARCH WARRANTS:
Where Can We Look?



February 2010

©2009 by Brian S. Batterton, Attorney, PATC Legal & Liability Risk Management Institute

Written For and Distributed by Public Agency Training Council. For duplication & redistribution of this article, please contact the Public Agency Training Council by phone at 1.800.365.0119.

Article Source: http://www.llrmi.com/articles/legal_update/computer_search_warrants.shtml

Printable Version: http://www.patc.com/weeklyarticles/print/computer_search_warrants.pdf

Stay up to date on these and other legal decisions by reading the weekly article updates available at patc.com

United States v. Mann, No. 08-3041, 2010 U.S. App. LEXIS 1264
(7th Cir. Decided January 20, 2010)

When executing search warrants, police are restricted to searching only areas in which the listed object of the search could be found or concealed. This is said to be the “scope” of the search warrant. For example, if an officer was executing a search warrant for a piano located in a house, the officer could only look places where a piano could be concealed. Thus, if the officer looked into a jewelry box, he would be exceeding the scope of the search warrant, and any evidence discovered in the jewelry box would likely be suppressed as fruit of an unreasonable search. On the other hand, a search warrant authorizing the search for illegal narcotics located in a house would most likely authorize the search of just about everywhere in the house because narcotics can be hidden in very small spaces. With searches for such tangible objects, it is fairly easy to determine the scope of the search. However, when we consider searches of computers and similar technology for digital media or other evidence, the scope of the search is sometimes less clear.

The Seventh Circuit Court of Appeals recently decided the *United States v. Mann*¹, where they addressed whether the discovery of child pornography was within the scope of a search warrant authorizing the search of Mann’s computers for evidence of the crime of voyeurism. The facts of the case are as follows:

While working as a life guard instructor in May 2007 for the Red Cross in Tippecanoe County, Indiana, Mann covertly installed a video camera in the women’s locker room to capture footage of women changing their clothes. Unfortunately for Mann, he also

©2010 Article published in the free PATC E-Newsletter: 800.365.0119

Link to Article online: http://www.llrmi.com/articles/legal_update/computer_search_warrants.shtml
<http://www.patc.com> | <http://www.llrmi.com> | <http://www.fsti.com> | <http://www.school-training.com> | <http://www.patctech.com/>

captured footage of himself installing the camera in an open locker. One of the female students in his class later discovered the camera. She recognized Mann in the video when she rewound and viewed the tape. She and two other women in Mann's class contacted the Lafayette Police Department and turned over the video camera and the videotape.

Three days later, an Indiana state prosecutor sought and received a search warrant for officers to search Mann'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." As relevant here, officers executing the warrant seized a Dell desktop computer with a Samsung hard drive, a Dell laptop, an e-machine, and a Western Digital external hard drive. The following day officers arrested Mann and charged him with voyeurism in violation of the Indiana Code. See [Ind. Code Ann. § 35-45-4-5\(a\)\(2\)-\(b\)\(1\)](#) (defining voyeurism and making it a class D felony when committed by means of any type of video recording device).

Nearly two months later, at the end of July 2007, Detective Paul Huff of the Lafayette Police Department began his search of Mann's computers. At the suppression hearing, Detective Huff testified that he searched the computers by first using a "write blocker" to protect the hard drives from being altered and then created an exact match of each hard drive. He then used software known as "forensic tool kit" ("FTK") to catalogue the images on the computer into a viewable format. Detective Huff explained that once this indexing process using FTK is completed, an "overview screen" is generated that lets him know how many images, videos, and documents are on the computer and whether there are encrypted documents or files that may be ignored (such as program files). The overview screen also lists files flagged by the software as "KFF (Known File Filter) Alert" and "KFF Ignorable" files. The "KFF Alert" flags those files identifiable from a library of known files previously submitted by law enforcement--most of which are images of child pornography.

On the first computer, Detective Huff discovered evidence that Mann had visited a web site called "Perverts Are Us," where he had read and possibly downloaded stories about child molestation. On the Dell laptop, Detective Huff uncovered still images taken in the Jefferson High school locker room, child pornography, and evidence that the Western Digital external hard drive had been connected to the laptop. Detective Huff then searched the final computer, where he again found child pornography, along with a disturbing story (presumably written by Mann) about a swim coach masturbating while watching young girls swim.

It was not until nearly another two months later, on September 18, 2007, that Detective Huff first searched the Western Digital external hard drive. As with the other computers, Detective Huff used FTK to index the contents of the hard drive. The FTK software identified four "KFF Alert" files and 677 "flagged thumbnails." Detective Huff proceeded to

open the files on the computer and discovered "many, many images of child pornography" as well as two videos from the Jefferson High School locker room.ⁱⁱ

Mann was charged with related crimes and filed a motion to suppress in district court. He raised two issues. First, he alleged that the search warrant lacked probable cause to authorize a search of his computers. Second, he alleged that the detective exceeded the scope of the search warrant when he discovered child pornography on the computers and external hard drive. The district court denied the motion to suppress. First, the district court held that probable cause was present for the search warrant because of the probability that evidence would be located at Mann's residence. Second, they held that the detective did not exceed the scope of the search warrant and any items that were discovered that were outside of the scope of the search warrant were in "plain view." Mann then plead guilty with the right to appeal.

The Issue

Mann then appealed to the Seventh Circuit Court of Appeals. He did not allege that the officers lacked probable cause, as he did to the district court. Instead his issue on appeal was *whether the detective exceeded the scope of the search warrant when he discovered child pornography when he utilized FTK software and the "KFF Alert" as he executed a search warrant that authorized a search for evidence of "images of women in locker rooms and other private places."*ⁱⁱⁱ

Thus, Mann argued that it was unreasonable for the detective to use the FTK software and the "KFF Alert" system, which is designed to identify known files of child pornography, when the search warrant authorized a search for "images of women in locker rooms and other private areas." The prosecution argued that the images authorized in the search warrant could be hidden almost anywhere on the computer. In fact, at the suppression hearing, the detective testified that he searched all files that he thought were necessary and might contain evidence or exculpatory information. In sum, the prosecution argued that the detective was at all times searching for images authorized in the search warrant and the search should not be invalidated just because he happened across child pornography.

Instructive Cases

The Seventh Circuit first noted United States Supreme Court precedent regarding search warrants. In *Marron v. United States*^{iv}, the United States Supreme Court held that the Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity or detail as to prevent general exploratory searches of a person's belongings. The court also noted the United States v. *Hill* where the Ninth Circuit Court of Appeals stated that

images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.^v

The Seventh Circuit then examined several other cases that are instructive. Mann urged the court to follow the *United States v. Carey*^{vi}, a Tenth Circuit case. In this case, police obtained a search warrant for Carey's computer to search for "names, telephone numbers, ledger receipts, addresses and other documentary evidence pertaining to the sale of controlled substances." The officers searched the computer using key word searches and did not find any records. They then began opening files, including JPG image files. They found child pornography in the JPG files. They then abandoned the search for drug records and opened all the JPG files; they found more child pornography. The Tenth Circuit, limiting their decision to the specific facts of this case, held that the officers exceeded the scope of the search warrant which was only for documentary (not photographic) evidence of drug dealing. As such, the evidence should have been suppressed. The Seventh Circuit distinguished *Carey* from Mann's case because the search warrant in *Carey* only involved the search for documentary evidence, and the search warrant in *Mann* involved a search for photographs.

The Seventh Circuit next considered the *United States v. Wong*^{vii}, a Ninth Circuit case. In this case, police were searching a computer pursuant to a search warrant regarding a murder investigation. In *Wong*, the police officer searching the computer remained within the scope of the search warrant and observed child pornography. He made a note of the child pornography file location and then continued with the search related to the murder investigation. The Ninth Circuit affirmed the denial of the motion to suppress, holding the evidence was admissible.

Likewise the court noted a case from the Eastern District of Virginia, the *United States v. Gray*^{viii}. In *Gray*, an agent, searching properly within the scope of the search warrant, found a subdirectory named "Tiny Teen." He opened the file, not looking for child pornography, but rather because it was the next subdirectory listed and he was opening all subdirectories as part of his routine search for the evidence listed in the search warrant. The court held that since the agent was searching within the scope of the warrant and inadvertently discovered the child pornography, it was admissible.

Lastly, the Seventh Circuit examined the *United States v. Comprehensive Drug Testing, Inc*^{ix} at the urging of Mann. In this case, the government seized hundreds of Major League Baseball player's drug testing records despite the fact that the search warrant only authorized the seizure of ten player's records, which were in the form of digital media. The Ninth Circuit then established the following four criteria regarding searches of computers:

First, the opinion directs magistrate judges to insist that the government waive reliance on the plain view doctrine. Second, the warrant application should include protocol "for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown"--preferably by requiring segregation to be done by specially trained computer personnel unconnected to the investigation who agree not to "communicate any information they learn during the segregation process absent further approval of the court." Third, the government must use search protocol tailored to uncover only information for which it has probable cause. Finally, the government must either destroy or return any non-responsive data and inform the magistrate what it has

kept,

destroyed,

or

returned.^x

The Seventh Circuit then stated that they were skeptical of the approach taken by the Ninth Circuit in *Comprehensive Drug Testing, Inc.* They declined to embrace that holding, rather choosing to allow the plain view doctrine to apply if appropriate, based on the specific facts of each case.^{xi}

The Holding

After examining aforementioned case law from other circuits, the Seventh Circuit then set out to decide if the detective in Mann exceeded the scope of the search warrant when he utilized the FTK software and the “KFF Alert.” As to the FTK filtering software, the court noted that the detective used it to index and catalogue the files into a viewable format. Reasoning that images of women in locker rooms could be hidden practically anywhere on the computers, they held that the detective did not exceed the scope of the search warrant when he utilized the FTK software. However, court took issue with the detectives use of the “KFF Alert” files. They reasoned that once the “KFF Alert” flagged a file, the detective should have known that the file was likely to be child pornography, which was not within the scope of the search warrant. Therefore, the four images obtained by the “KFF Alert” should be suppressed. Fortunately, there was still ample evidence of child pornography to uphold Mann’s conviction.

Thus, the court held

...we ultimately conclude that, with the exception of the four "KFF alert" images, the search was lawful, particularly since Detective Huff did indeed uncover further evidence of voyeurism on the external hard drive. Because Detective Huff discovered the child pornography while conducting a systematic search for evidence of voyeurism, we conclude that his actions were reasonable and within the scope of the warrant's authorization.^{xii}

Why was the Court Troubled?

In *Mann*, the Seventh Circuit also took the time to counsel officers to ensure that their search warrants for digital media (1) particularly describe the things to be seized and (2) that the officers narrowly tailor their searches to be within the scope of the search warrant. The court went on to state

Although we now hold that his actions were within the scope of the warrant, we emphasize that his failure to stop his search and request a separate warrant for child pornography is troubling...Because Detective Huff was not in a rapidly unfolding situation or searching a location where evidence was likely to move or change, there was no downside to halting the search to obtain a second warrant. Indeed, we find it problematic that nearly two months elapsed before Detective Huff began his search of the Western Digital hard drive despite having found child pornography on the Dell laptop. However, notwithstanding our distaste for the timeline of the investigation, we conclude that the original warrant authorized Detective Huff's search of the external hard drive for images of voyeurism.^{xiii}

The Bottom Line

The most important point that we can learn from *Mann* is that officers should be mindful of the permissible scope of their search under a search warrant for digital media. If an officer locates digital media in “plain view” in a computer file, and that media is evidence of a crime that is *unrelated to or not within the scope* of the search warrant, the officer should seek an additional search warrant (or amend the current search warrant if allowed by state law) in order to continue to search for additional similar evidence. The only exception would be if some exigent circumstance (such as imminent destruction of evidence) is present.

CITATIONS:

ⁱ *United States v. Mann*, No. 08-3041, 2010 U.S. App. LEXIS 1264 (7th Cir. Decided January 20, 2010)

ⁱⁱ *Id.* at 2-5

ⁱⁱⁱ *Id.* at 7 (quoting the search warrant)

^{iv} 275 U.S. 192, 196 (1927)

^v *Mann* at 8 (quoting *U.S. v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006))

^{vi} 172 F.3d 1268 (10th Cir. 1999)

^{vii} 334 F.3d 831 (9th Cir. 2003)

^{viii} 78 F. Supp.2d 524 (E.D. Va. 1999)

^{ix} 579 F.3d 989 (9th Cir. 2009)

^x *Mann* at 16 (quoting *United States v. Comprehensive Drug Testing, Inc*, 579 F.3d 989 (9th Cir. 2009))

^{xi} *Id.* at 17

^{xii} *Id.* at 19

^{xiii} *Id.* at 18-19