U.S. v. Hay
(9th Cir. 2000) __ F.3d __

ISSUES

(1) Did probable cause exist for a warrant to search Hay's computer for child pornography? (2) Was the description of the computer equipment to be seized reasonably particular?

FACTS

On November 29, 1996, police in Ontario, Canada arrested a man named Evans for trafficking in child pornography. During the course of their investigation, officers determined that Evans was actively trading and exchanging child pornography with people in the United States via the Internet.

While searching Evans' computer, officers noted his File Transfer Protocol[1] (FTP) showed that on November 27, 1996 Evans transmitted 19 graphics files containing child pornography to a computer with an Internet address of 128.95.25.1. Officers subsequently traced this address to a computer "affiliated" with the University of Washington. On February 27, 1997 they forwarded this information to U.S. Customs.

Customs agents determined, by means of a Grand Jury Subpoena, that this Internet address had been assigned to Alexander Hay, a university student who lived in one of the school's housing facilities. They also learned that Hay was operating a web site in which he "described extensive contacts with children, including teaching skiing to preschoolers, working with a four-year old autistic girl, and spending 400 hours as a volunteer in early primary school classrooms."

A Customs agent posing as a researcher then phoned Hay and said she was conducting a computer usage survey. In response to her questions, Hay admitted he owned the computer to which the files were sent, that he kept the computer in his apartment, and that he was the only person who used it.

Based on this information, Customs agents on May 28, 1997 applied for a warrant to seize all of Hay's "computer hardware, software, records, instructions or documentation, and depictions of child pornography." A magistrate issued the warrant which was executed on May 29, 1997. Among other things, the warrant authorized officers to seize all of Hay's computer equipment so that it could be searched by a computer expert under controlled conditions. During the search, agents found "hundreds" of computer graphics files containing child pornography stored on a hard drive in Hay's computer. Hays was subsequently convicted of possession and distribution of child pornography by means of a computer.

DISCUSSION

Hay argued the information contained in the search warrant affidavit did not establish probable cause to believe child pornography would be found in his computer. Specifically, he argued, (1) there was no evidence he was aware that the files he received from Evans contained child pornography, and (2) because the files were sent to him about six months before the warrant was obtained, there was no probable cause to believe the files would still be stored in his computer. He also argued the search

warrant failed to describe the evidence to be seized with reasonable particularity, and that it failed to justify the seizure of Hay's entire computer system or its removal from the premises for an off-site search.

Knowledge of the files' contents

As noted, Hay argued the affidavit failed to establish probable cause because there was no proof he was aware the files he downloaded contained child pornography. He pointed out, for example, the files might have been unsolicited junk e-mail ("SPAM"), they may have been automatically downloaded by a program Hay had written for his computer, or the files may have been downloaded by someone else at the University who had access to his computer.

The court was not persuaded, however, because there was plenty of circumstantial evidence in the affidavit that Hay knew exactly what the files contained. That evidence included the following:

Not SPAM: The files could not have been SPAM because they were sent by means of FTP which, as the court noted, "has nothing to do with e-mail."

Not inadvertent: The transfer was not inadvertent inasmuch as the log in Evans' computer showed separate entries for each of the 19 file transfers, and the transfers occurred at different times over a seven-minute period.

Single-user computer: Hay admitted to a Customs agent he was the only person who used the computer.

Unusual interest in children: There was evidence of "Hay's extreme interest in young children as reflected in what Hay published on his home page."

Evans was a known trader: The graphics were sent to Hay by Evans, a known trader in child pornography.

Thus, the court ruled it was reasonable for the magistrate to conclude the 19 file transfers were neither unsolicited nor accidental.

Staleness

Hay also argued that even if the child pornography was downloaded to his computer on November 27, 1996, there was no reason to believe it would still be located there when the warrant was executed six months later on May 29, 1997. Customs agents, however, had anticipated such an argument. So they explained in the affidavit that collectors and distributors of child pornography value their sexually explicit material highly and rarely if ever dispose of it. They also explained that even if Hay had deleted the files containing child pornography, "they could nevertheless be retrieved by a computer expert."

Based on this information, the court stated, "We conclude that the magistrate judge could well believe that the files sent by Evans would be present when the search was conducted."[2]

Description of computer equipment

The search warrant in this case authorized a search of "computer hardware" and "computer software" for evidence pertaining to the sexual exploitation of children. It also authorized a search for child pornography contained in "records stored in the form of electronic or magnetic coding or on computer media." Hay argued this description of the things to be searched was too vague.

It is settled that a search warrant must describe the place to be searched and the things to be seized with "reasonable particularity."[3]

If, however, it is not reasonably possible to furnish a detailed description, the "reasonable particularity" requirement may be deemed satisfied if the evidence is described in as much detail as possible.[4] This was exactly the situation in Hay. As the court observed, "The government knew that Evans had sent 19 images directly to Hay's computer, but had no way of knowing where the images were stored."

Other issues

There were two other rulings by the court: (1) It was reasonable for agents to seize Hay's entire computer system in order to search it off-site. This was "because of the time, expertise, and controlled environment required for a proper analysis," and because the magistrate specifically authorized the officers to do so. (2) The description of the evidence to be seized--"child pornography" was sufficiently specific.

[1] NOTE: The court explained "FTP is a method of directly transferring files between two computers." At fn. 2.

[2] NOTE: The court seemed to approve of the affiant's "boilerplate" language in which she explained the significance of the transfer of files from Evans to Hay: "It sets forth relevant background information about how child pornography is traded and distributed over the Internet: through use of chat rooms to establish contacts, followed by transmission or trading of images. It points out that the computer's ability to store images in digital form makes it an ideal repository for child pornography. The affidavit also explains that thee computer has become one of the preferred methods of distribution of child pornographic materials and opines, based on [her] experience and that of colleagues, that searches and seizures of evidence from computers requires agents to seize all parts of a computer system to be processed later by a qualified computer expert."

[3] See Thompson v. Superior Court (1977) 70 Cal.App.3d 101, 109; Penal Code §§ 1525 and 1529; Andresen v. Maryland (1976) 427 US 463, 480; Maryland v. Garrison (1987) 480 US 79, 84;

[4] See People v. Tockgo (1983) 145 Cal.App.3d 635, 640; People v. Schilling (1987) 188 Cal.App.3d 1021, 1031; People v. Remiro (1979) 89 Cal.App.3d 809, 831-2; People v. Smith (1986) 180 Cal.App.3d 72, 89-90; People v. Rogers(1986) 187 Cal.App.3d 1001, 1009; People v. Alcala (1992) 4 Cal.4th 799-800; People v. Nicolaus (1991) 54 Cal.3d 551, 574-5; People v. Holmsen (1985) 173 Cal.App.3d 1045, 1048-9.