Recent Case Report

U.S. v. Giberson

(9th Cir. 2008) 527 F.3d 882

ISSUES

(1) While executing a warrant to search for certain documents, could officers search the defendant's computer even though the warrant did not expressly authorize a computer search? (2) During a subsequent warranted search of the computer for financial records, did a technician exceed the permissible scope of the search when he viewed files containing child pornography?

FACTS

In the course of a traffic stop in North Las Vegas, an officer discovered that the driver, Giberson, possessed a false Nevada ID card. He also learned that Giberson was wanted on outstanding warrants, so he arrested him. When the officer asked him about the fake ID, Giberson said he printed it to avoid paying child support. This comment prompted the officer to notify the U.S. Department of Health and Human Services which assigned an investigator to the case.

The investigator learned that Giberson owed $108,000 in child support, so he obtained a warrant to search Giberson's home for certain financial records that would be relevant in the child support case. Although the warrant did not specifically authorize a search of computers for the documents, investigators searched one on the premises and discovered evidence that Giberson had been printing false Social Security cards and birth certificates, among other things. This evidence included transparencies of the Nevada State Seal and photographs that were apparently used on the false IDs. The investigators notified an Assistant U.S. Attorney who advised them to secure the computer pending issuance of a warrant to search it for false government documents.

After the warrant was issued, investigators took the computer to a lab where a technician created a mirror image of the computer's hard drive. He then searched the mirror image using software that permitted him to view thumbnails of the saved files. While examining these thumbnails, he discovered that some contained child pornography. As the result, investigators obtained a warrant to search the mirror image for child pornography. The search netted more than 700 such images.

When Giberson's motion to suppress the evidence was denied, he pled guilty to receiving and possessing child pornography.

DISCUSSION

Giberson contended that the images should have been suppressed because, (1) the first search warrant did not expressly authorize a search of his computer, and (2) while executing the second warrant, the technician exceeded the permissible scope of the warrant when he viewed files containing child pornography.

THE FIRST WARRANT: Giberson argued that officers who have obtained a warrant to search for certain documents at a residence may not search for those documents in a computer on the premises unless the warrant expressly authorized a computer search. The court disagreed.

As a general rule, officers who are executing a warrant may search all places and containers in which any of the listed evidence may be found. As the United States Supreme Court explained in a car search case, "When a legitimate search is underway, and when its purpose and its limits have been precisely defined, nice distinctions between . . . glove compartments, upholstered seats, trunks, and wrapped packages in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand."[1]

Nevertheless, Giberson argued that this rule should not apply to computers because, unlike cars, they contain "massive quantities of intangible, digitally stored information," much of which pertains to "many different areas of a person's life." While this is true, said the court, "there is no reason why officers should be permitted to search a room full of filing cabinets or even a person's library for documents listed in a warrant but should not be able to search a computer."

The court also noted the practical problems that would result if digital storage was treated differently than conventional storage. Said the court, "If we permit a person's Day-Timer to be searched, what about one's BlackBerry? The format of a record or document should not be dispositive to a Fourth Amendment inquiry." In conclusion, the court observed:

> While officers ought to exercise caution when executing the search of a computer, just as they ought to when sifting through documents that may contain personal information, the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement.

THE SECOND WARRANT: In order to find computer files containing false government documents, the technician utilized computer-search software that allowed him to view thumbnail images of each file. It was while he was viewing thumbnails that he discovered the child pornography.

Giberson argued that this method of conducting a computer search is unlawful; that technicians should not be permitted to view a file unless there was some reason to believe it contained some of the listed evidence. But, as the court pointed out, this would be impractical:

> Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. 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.[2]

For this reason, the court ruled the thumbnail search was lawful because "[i]t would be unreasonable to require the government to limit its search to directories called, for example, 'Fake I.D. Documents' . . . "

Accordingly, the court ruled the evidence was seized lawfully. POV

[1] *US* v. *Ross* (1982) 456 US 798, 821-2.

[2] Quoting from *U.S.* v. *Hill* (9th Cir. 2006) 459 F.3d 966, 978.