No. 07-10100
United States Court of Appeals, Ninth Circuit

U.S. v. Giberson

527 F.3d 882 (9th Cir. 2008)
Decided May 30, 2008

No. 07-10100.

Argued and Submitted January 15, 2008.

883 Filed May 30, 2008. *883

Franny A. Forsman, Federal Public Defender, and Jason F. Carr, Assistant Federal Public Defender, Las Vegas, NV, for the appellant.

Steven W. Myhre, Acting United States Attorney, Robert L. Ellman, Appellate Chief, and Elizabeth A. Olsen, Assistant United States Attorney, Reno, NV, for the appellee.

Appeal from the United States District Court for the District of Nevada; Brian E. Sandoval, District Judge, Presiding. D.C. No. CR-04-00299-BES.

Before: J. CLIFFORD WALLACE and MARY M. SCHROEDER, Circuit Judges, and ROGER T. BENITEZ,– District Judge.

– The Honorable Roger T. Benitez, United States District Judge for the Southern District of California, sitting by designation.

884 *884

WALLACE, Senior Circuit Judge:

Giberson appeals from the district court's denial of his motion to suppress evidence of child pornography found on his personal computer, which led to his conviction for receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). He also appeals from his sentence, arguing the district court erred in sentencing him for both possession and receipt of child pornography. We have jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a)(1). We affirm his conviction, vacate his sentence, and remand.

I.

On February 24, 2003, a North Las Vegas Police Department officer stopped Giberson because his license plates had expired. During the stop, the officer discovered that Giberson had a false Nevada identification (I.D.) card in the name of Charles F. Walsh, III. After learning that Giberson had three outstanding arrest warrants for traffic violations and no valid driver's license, the officer arrested Giberson. A search incident to the arrest revealed a "Play Cash" card from a casino in Walsh's name. Giberson told the officer that he used the fake I.D. for work and to avoid paying his child support obligation.

United States Health and Human Services (HHS) Agent David Kiesow began an investigation into Giberson's child support obligations and discovered that, in 1991, a Minnesota state court had ordered Giberson to make monthly payments to his ex-wife for the support of their two children. Ironically, Giberson, who at one point had served as Deputy Commissioner of the Minnesota Department of Human Services and had supervised the child support enforcement division, failed to make the required payments and, as of July 2003, was $108,000 behind. Law enforcement efforts to collect Giberson's child support arrearage had been unsuccessful.

As a result of this investigation, Agent Kiesow obtained a warrant to search Giberson's residence in Nevada. The search warrant authorized HHS agents to search for: (1)"records or documents that appear to show ownership of assets or property"; (2) "records or documents from financial institutions" in Giberson's name or the names of any known or unknown aliases; (3) "records and correspondence relating to identification cards"; (4) "records, documents or correspondence . . . related to the use or attempted use" of other individual's identities; (5) "correspondence, records and documents" relating to Giberson's or his aliases' earnings and employment; (6) tax records; (7) documents or records showing receipt of income or expenditure of funds; and (8) records referring to Giberson's employer. Prior to executing the warrant, Agent Kiesow had no evidence that Giberson owned a computer or used a computer in the commission of his suspected crimes.

On September 11, 2003, the day after they obtained the warrant, HHS agents searched Giberson's home. In one of the bedrooms, they discovered a personal computer. The computer was on a desk and was connected to a printer that was on an adjacent dresser. Next to the printer, on the dresser, the agents found a sheet of what appeared to be fake Nevada I.D. cards. The agents observed that the cards were not high quality and looked like they could have been printed from the adjacent printer. On the desk with the computer, agents found
885 transparencies depicting the *885 Nevada State Seal. In the drawers of the computer desk, on the desk, and on the dresser next to the desk, they found a number of other documents evidencing the production of false I.D.s, including fake Social Security cards and State of New York birth certificates in the name of Charles Walsh III, one of Giberson's known aliases, and in other names.

Believing that many of the I.D. materials had been printed off of Giberson's computer, Agent Kiesow contacted an Assistant U.S. Attorney, who advised him to secure the computer until the agents could obtain a search warrant for it. Kiesow then sent the computer to a forensics laboratory in Chicago. There, HHS forensic computer specialist David Rehms made a mirror image of the computer's hard drive before shipping the computer back to Giberson's wife in Nevada.

On September 29, 2003, Kiesow obtained a second search warrant. The second warrant authorized a search of the mirror image of Giberson's hard drive for records relating to I.D. cards or the creation of I.D. cards, including driver's licenses, state seals, and pictures of individuals that might be placed on I.D. cards, as well as records related to Giberson's assets, property, employment, and income.

The next day, computer specialist Rehms began his search of the mirror image using a law enforcement utility software package called ILOOK. ILOOK pulls computer files based on file type, and dumps all similar file types into separate folders. For example, ILOOK retrieves all graphics or images files and puts them into one folder. An analyst can then open that folder and view multiple thumbnails (reduced-sized versions) of the images on the computer screen at one time without opening individual files. In this case, after sorting the computer files with ILOOK, Rehms used another software package to view the files because it enabled him to view more thumbnails of graphic images on the screen at a time, making his search more efficient.

While Rehms was scanning the thumbnail images for images and photographs related to the production of fake I.D.s, he discovered images he believed to be child pornography. Rehms immediately stopped his search and telephoned Agent Kiesow, who directed Rehms to stop his search while Kiesow determined the proper course of action. Either later that day or the next day, Kiesow telephoned Rehms and told him to continue searching for the items in the search warrant, but that, if Rehms came across more child pornography, he was to print it out. However, Rehms did not specifically search for child pornography. He continued his search for items related to fake I.D.s, and as he came across images of child pornography, he printed out a sampling. Rehms also found images related to the production of fake I.D.s and seals for the State of Nevada. Following Rehms' discovery, Kiesow contacted FBI Special Agent Andrew Gruninger, who obtained a search warrant to search the mirror image of Giberson's hard drive. A subsequent forensic search of the hard drive pursuant to the third warrant revealed more than 700 images of child pornography.

Giberson was indicted on July 21, 2004, and charged with receiving child pornography in violation of 18 U.S.C. § 2252(a)(2) and possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). In November, Giberson filed a motion to suppress evidence, arguing that law enforcement officers exceeded the scope of the first search warrant when they seized his computer, and that they exceeded the scope of the second search
886 warrant when they "searched for" child pornography on the computer. After *886 an evidentiary hearing, the magistrate judge recommended that the motion be denied. The district court, after receiving objections to the magistrate judge's recommendation and hearing oral argument, accepted the recommendation and denied Giberson's motion to suppress.

Later, Giberson entered conditional guilty pleas to both counts in the indictment. The district court sentenced Giberson to concurrent terms of sixty months on each of the two counts, to be followed by three years of supervised release on count one, concurrent with a life term of supervision on count two. Giberson appealed, arguing the district court erred in denying his motion to suppress and in failing to merge the counts of conviction at sentencing.

II.

Giberson challenges the seizure of his computer pursuant to the first search warrant and the search of the mirror image of his hard drive pursuant to the second search warrant, arguing the evidence of child pornography obtained from the seizure and subsequent search should have been suppressed. We review the district court's denial of his motion to suppress *de novo* and the district court's underlying factual findings for clear error. *United States v. Summers*, 268 F.3d 683, 686 (9th Cir. 2001).

A.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Generally, in a search made pursuant to a warrant, only specifically enumerated items may be seized. *See United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

One issue we can put to the side. Giberson's brief twice states that "[t]he warrant was not specific enough." His argument, however, seems limited to the claim that the warrant did not specify the computer and the computer was therefore unlawfully seized; he does not suggest that the warrant itself failed to specifically describe items to be seized and was therefore facially invalid. In any event, the warrant was based on probable cause and clearly limited the types of documents and records that were seizable, "objectively describ[ing] the items to be searched and seized with adequate specificity and sufficiently restrict[ing] the discretion of agents executing the search." *See United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006). The warrant also "described the

items to be searched and seized as particularly as could be reasonably expected given the nature of the crime and the evidence [the government] then possessed." *See id.* at 1149. Thus, the warrant was not a "general warrant" and was not facially invalid under *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986).

Giberson does argue that, because the first search warrant did not specify that the officers could search or seize a computer, the seizure of his computer exceeded the scope of the warrant. The question, then, is whether a warrant that describes particular documents authorizes the seizure of a computer where, as here, the searching agents reasonably believed that documents specified in the warrant would be found stored in the computer.

We have long held that a search warrant authorizing the seizure of materials also authorizes the search of objects that could contain those materials. In *United States v. Gomez-Soto*, officers were conducting a search
887 pursuant to a warrant authorizing the seizure of "[b]ooks, papers, records, *887 receipts, documents, notations, diaries, journals or ledgers" related to the defendant's unlawful business dealings. 723 F.2d 649, 652 fn.** (9th Cir. 1984). During the search, officers found a locked briefcase and a microcassette tape. *Id.* After the defendant refused to open the briefcase, the officers cut it open and seized its contents, which included cocaine. *Id.* The microcassette tape contained incriminating statements about the defendant. *Id.*

The defendant challenged the search, arguing that the search and seizure of the briefcase, the microcassette, and their contents were not permitted because they were not particularly described in the warrant. *Id.* at 654. We rejected that argument, reasoning:

> The search and seizure of both the microcassette and the briefcase were proper. It is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant.

Id. Because the briefcase would be a logical container for many of the items described in the warrant, and the microcassette tape is "by its very nature a device for recording information . . . which come[s] clearly within the specific authority of the warrant," we held that the "failure of the warrant to anticipate the precise container in which the material sought might be found" was not fatal. *Id.* at 655.

Later, in *United States v. Reyes*, we reaffirmed this principle, holding that a search warrant authorizing the seizure of drug trafficking records, ledgers, or writings related to drug trafficking also permitted agents to seize a cassette tape. 798 F.2d 380, 383 (10th Cir. 1986). We recognized that, "in the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take," and that, "the seizure of a specific item characteristic of a generic class of items [items that record information] defined in the warrant did not constitute an impermissible general search." *Id.*

Computers, like briefcases and cassette tapes, can be repositories for documents and records. We have not yet had occasion to determine, in an opinion, whether computers are an exception to the general principle that a warrant authorizing the seizure of particular documents also authorizes the search of a container likely to contain those documents. We hold that, in this case, where there was ample evidence that the documents authorized in the warrant could be found on Giberson's computer, the officers did not exceed the scope of the warrant when they seized the computer.

Giberson does not deny that it was reasonable in this case for the agents to believe that the documents specified in the warrant might be found on his computer. Rather, he argues that the analogy between a computer and other "containers" is not appropriate because computers are somehow entitled to heightened protection, and are

searchable only when specified in the warrant. We observe at the outset that Fourth Amendment exceptions and distinctions based solely on a type of technology are "unwise and inconsistent with the Fourth Amendment." *See Kyllo v. United States*, 533 U.S. 27, 41, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (Stevens, J., dissenting). Technology changes. To be acceptable, Giberson's argument must be based on a principle that is not technology-specific. Though Giberson offers several rationales for treating computers differently from storage
888 mediums such as filing cabinets and briefcases, none is persuasive. *888

Giberson's principal argument is that computers are able to store "massive quantities of intangible, digitally stored information," distinguishing them from ordinary storage containers. But neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context. While it is true that computers can store a large amount of material, 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. Giberson's purported exception would also create problems in analyzing devices with similar storage capacities. If we permit cassette tapes to be searched, then do we permit CDs, even though they hold more information? If we do not permit computers to be searched, what about a USB flash drive or other external storage device? Giberson's purported exception provides no answers to these questions.

Similarly, attempting to limit Fourth Amendment searches based on the format of stored information would be arbitrary. We have already held that microcassettes, which store data differently from traditional paper, are seizable in a search for "records." *See Gomez-Soto*, 723 F.2d at 652. There is no reason why material stored digitally on a computer should not also be searchable. Once again, Giberson's purported exception generates more questions than answers: 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.

Giberson's purported rule creates a brightline exception to the Fourth Amendment that provides no principles by which to evaluate whether a search is reasonable. The Supreme Court has consistently eschewed such brightline rules. *See Ohio v. Robinette*, 519 U.S. 33, 39, 117 S.Ct. 417, 136 L.Ed.2d 347 (1996). Here, the only principle upon which we can anchor this analysis is the one already articulated by this court: that to search a container, it must be reasonable to expect that the items enumerated in the search warrant could be found therein. If it is reasonable to believe that a computer contains items enumerated in the warrant, officers may search it. Here, numerous documents related to the production of fake I.D.s were found in and around Giberson's computer and were arguably created on and printed from it. It was therefore reasonable for officers to believe that the items they were authorized to seize would be found in the computer, and they acted within the scope of the warrant when they secured the computer.

Giberson offers two other bases upon which to distinguish computers from other objects in the Fourth Amendment context. First, he argues that computers have a great potential for the intermingling of relevant and irrelevant (and personal and private) material. Indeed, a court has recognized that "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the `intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001). However, we have already rejected this reasoning in *Adjani*, when we pointed out that "[t]he fear that agents searching a computer may come across . . . personal information cannot alone serve as the basis for excluding evidence of criminal acts." 452 F.3d at 1152 n. 9. While officers ought to exercise caution when executing the search of a computer, just as they
889 ought to when sifting *889 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.

Second, Giberson suggests that because computers store material protected by the First Amendment, they should be subject to heightened protection. But, as this court observed in *United States v. Weber*, 923 F.2d 1338, 1343 n. 6 (9th Cir. 1990), the Supreme Court has already rejected the proposition that a stricter probable cause standard should apply when the First Amendment is implicated. *See also New York v. P.J. Video, Inc.*, 475 U.S. 868, 875, 106 S.Ct. 1610, 89 L.Ed.2d 871 (1986). We therefore reject Giberson's First Amendment argument.

In the circumstances underlying this appeal, it was reasonable for the officers to believe that seizable items were stored on Giberson's computer, and to secure the computer and obtain a specific warrant and search it. Their failure to anticipate that the items would be stored on a computer and to specify computer files in the warrant was not unreasonable because they had no reason to believe that Giberson owned a computer. *See United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) ("A warrant describing a category of items is not invalid if a more specific description is impossible"). Their actions were particularly appropriate because the agents merely secured the computer while they waited to get a second warrant that would specifically authorize searching the computer's files. The seizure of the computer was therefore reasonable.

The government argues, and the district court agreed, that the seizure of the computer was also justified by the plain view exception to the warrant requirement. Because we decide that the seizure was authorized by the warrant itself, it is unnecessary to decide whether the plain view doctrine or any other exception to the warrant requirement applies here.

B.

Giberson also argues that the evidence obtained from the search of his computer should have been suppressed because the government did not sufficiently limit its search to relevant documents. The second warrant authorized the government to search Giberson's computer for records relating to I.D. cards or the creation of those cards, including driver's licenses, state identification cards, state seals, and photographs that could be used for fake I.D.s. Giberson argues that computer specialist Rehms should have limited his search to files likely to contain those documents, and vaguely asserts that Rehms could have done so by looking at the computer's directories instead of sorting files through ILOOK.

Giberson's argument is foreclosed by *Hill.* There, the defendant argued that a search of his computer files should have been limited to files likely to be associated with those identified in the search warrant. *Hill*, 459 F.3d at 977. We rejected that argument, reasoning that the defendant's methodology was unreasonable, because:

> 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.

Id. at 978 (internal quotation marks and citation omitted); *see also Adjani*, 452 F.3d at 1150 ("Computer files
890 are easy to *890 disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of [the defendant's] labeling of the files documenting [his] criminal activity. The government should not be required to trust the suspect's self-labeling when executing a warrant").

This argument applies with equal force to Giberson's case. The records for which the government was authorized to search, including images of the Nevada State Seal and photographs that might be used to create fake I.D.s, could have been graphics files. There was no reasonable way to sort relevant and irrelevant graphics

files because the fake I.D. files and the pornography files were innocuously labeled. It would be unreasonable to require the government to limit its search to directories called, for example, "Fake I.D. Documents," and Giberson does not claim that there was such a folder.

We acknowledge that "[n]ew technology may become readily accessible . . . to enable more efficient or pinpointed searches of computer data," and that, "[i]f so, we may be called upon to reexamine the technological rationales that underpin our *Fourth Amendment* jurisprudence in this technologysensitive area of the law." *Hill*, 459 F.3d at 979 (emphasis added). However, in this case, based on the technology available to him for searching Giberson's computer, Rehms' search was reasonable; the pornographic material he inadvertently discovered while searching for the documents enumerated in the warrant was properly used as a basis for the third warrant authorizing the search for child pornography.

Our holding is not inconsistent with *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999). There, the Tenth Circuit suppressed evidence found when an officer, who was supposed to be searching a computer for drug-related documents, stumbled upon child pornography and began to search for more. *Id.* at 1276. Based on the officer's own testimony, the court found that the child pornography was not "inadvertently discovered" because the officer had temporarily abandoned the search authorized by the warrant in order to look for child pornography, contravening the limitations of the search warrant. *Id.* at 1273. The court was careful to state that the result in the case (suppression of the evidence) was "predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result." *Id.* at 1276 (footnote omitted). A concurring opinion stated that "if the record showed that [the officer] had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, . . . a different result would be required." *Id.* at 1277 (Baldock, B., concurring).

As the district court concluded, this case "is vastly different from *Carey.*" Rehms was authorized to look at images and photographs; after discovering the pornographic images, Rehms continued with his search for evidence of fake I.D. documents and only inadvertently came across more child pornography. The government only searched for pornographic files after obtaining the third search warrant authorizing it to do so, and the search was therefore reasonable.

C.

The government acted reasonably at all stages in its investigation into Giberson's production of fake I.D.s and, later, his possession of child pornography. The seizure of the computer was justified because the computer was
891 reasonably believed to contain items enumerated in the first *891 search warrant. The search of the computer was conducted pursuant to a valid second search warrant and proceeded in a reasonable manner. Pornography was not searched for until authorized by the third warrant. We affirm the district court's denial of Giberson's motion to suppress.

III.

Giberson contends that the district court erred when it sentenced him for both receipt and possession of child pornography, arguing that the sentencing is multiplicitous. He failed to object in the district court, and we review for plain error. *See United States v. Smith*, 424 F.3d 992, 999-1000 (9th Cir. 2005).

By a divided panel, and subsequent to Giberson's sentencing, we recently held, on plain error review, that entering judgment against a defendant who had pled guilty to both the receipt and possession of child pornography was multiplicitous and violated the Fifth Amendment's prohibition against double jeopardy. *United States v. Davenport*, 519 F.3d 940, 2008 WL 732491 (9th Cir. 2008). In *Davenport*, we accepted the

argument, similar to the one Giberson makes, that "the offense of possessing child pornography is a lesser included offense of the receipt of child pornography," and that conviction and punishment for both is therefore constitutionally impermissible. *Id.* at 947. We held that, though the defendant's sentences (like Giberson's) were to run concurrently, "[t]he district court's error was plain, and it affected [the defendant's] substantial rights by imposing on him the potential collateral consequences of an additional conviction." *Id.* We concluded that "because the prohibition against double jeopardy is a cornerstone of our system of constitutional criminal procedure, this error threatens the fairness, integrity, and public reputation of our judicial proceedings," and vacated the defendant's sentence. *Id. Davenport* is materially indistinguishable from this case, and we therefore vacate Giberson's sentence and remand to the district court for resentencing.

CONVICTION AFFIRMED; SENTENCE VACATED AND REMANDED.