

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
MICHAEL CLAY PAYTON,
Defendant-Appellant.

No. 07-10567
D.C. No.
CR-05-00333-OWW
OPINION

Appeal from the United States District Court
for the Eastern District of California
Oliver W. Wanger, District Judge, Presiding

Argued and Submitted
November 19, 2008—San Francisco, California

Filed July 21, 2009

Before: William C. Canby, Jr. and Kim McLane Wardlaw,
Circuit Judges, and Richard Mills,* District Judge.

Opinion by Judge Canby

*The Honorable Richard Mills, United States District Judge for the
Central District of Illinois, sitting by designation.

COUNSEL

Eric V. Kersten, Assistant Federal Public Defender, Fresno, California, for the plaintiff-appellee.

Sherrill A. Carvalho, Assistant United States Attorney, Fresno, California, for the defendant-appellant.

OPINION

CANBY, Circuit Judge:

Michael Payton appeals the district court's denial of his motion to suppress evidence of child pornography found on his personal computer. Payton pled guilty to knowingly possessing images of child pornography in violation of 18 U.S.C. § 2252(a)(4), conditioned on his right to make this appeal. We have jurisdiction pursuant to 28 U.S.C. § 1291. We reverse the judgment of the district court and remand with instructions.

BACKGROUND

In 2004, a California Superior Court judge issued a search warrant for a house in Merced County where Payton resided.

Police believed that the occupants were selling drugs. The warrant directed officers to search for any item listed in "Attachment A," which included methamphetamine and materials used to cut and package it. Attachment A also included, among other things, "[s]ales ledgers showing narcotics transactions such as pay/owe sheets" and "[f]inancial records of the person(s) in control of the residence or premises, bank accounts, loan applications, [and] income and expense records." The warrant did not explicitly authorize the search of computers.

During the execution of the search, the officers found no evidence of drug sales. Officer Horn found a computer in Payton's bedroom with the screen saver activated. He moved the mouse, which removed the screen saver, and clicked open a file. It disclosed an image that he thought was child pornography. This and images like it eventually led to Payton's charge for possession of child pornography. Payton moved to suppress the evidence, challenging the search on the two grounds he raises on appeal. First, he argued that the warrant lacked probable cause because it relied on a misrepresentation of a neighbor's complaint. Second, he argued that the search of the computer exceeded the scope of the warrant. After the district court rejected these challenges and denied the motion to suppress, Payton entered a conditional guilty plea and was sentenced.

To establish probable cause, the warrant incorporated by reference Officer Horn's affidavit, which included Officer Horn's statement of probable cause. This statement requested permission to search any computer within the residence, although Officer Horn did not have any particular reason to believe that a computer would be found in the house. The Superior Court judge testified at the suppression hearing that he had intended to authorize the search of any computer found in the residence, but the warrant as issued did not explicitly direct a search for, or search of, any computers.

Officer Horn declared in his probable cause statement that neighbors had complained of drug sales. It is uncontested, however, that only one neighbor complained, and of drug use, not drug sales. To determine the consequence of the misrepresentation, the district court held a *Franks* hearing. *See Franks v. Delaware*, 438 U.S. 154, 171-72 (1978) (requiring evidentiary hearing when defendant preliminarily shows that false statement was knowingly and intentionally, or with reckless disregard for the truth, included by affiant in search warrant affidavit). Officer Horn testified at that hearing that he suspected drug sales for a few reasons. First, the contents of a video that the neighbor had taken showed people not thought to be residents using drugs outside of the house. Second, the police had previously arrested one of the residents in the house and had found 2.7 grams of methamphetamine on her person; to Officer Horn, this quantity, and the fact that it was divided into two separate packages, evidenced an intent to sell. Officer Horn had included all of this information in his affidavit stating probable cause, as well as a statement that “based upon [his] training and experience,” drug dealers maintain records of sale on their computers.

The district court held that probable cause supported the issuance of the warrant. The district court stated that “even if [it] excised and consider[ed] the entire warrant without a complaint of neighbors of drug sales,” the warrant was still sufficient in light of the other evidence presented. The district court also held that the search of the computer was valid because the failure to include the word “computers” in Attachment A was an oversight cured by the issuing judge’s testimony of his intent. Accordingly, it dismissed the motion to suppress the evidence of child pornography obtained as a result of the search. We agree with the district court that the search warrant was supported by probable cause despite Officer Horn’s misrepresentation of a neighbor’s report. We conclude, however, that the search of the computer violated Payton’s Fourth Amendment rights. Accordingly, we reverse

the denial of the motion to suppress, and remand with instructions to permit Payton to withdraw his conditional guilty plea.

DISCUSSION

I. Probable Cause Supporting the Search Warrant

Payton contends that Officer Horn's affidavit contains a materially false statement that invalidates the warrant by destroying probable cause. We review *de novo* the district court's conclusion that probable cause existed, examining whether there was a "fair probability" of drug sales. *See United States v. Bishop*, 264 F.3d 919, 924 (9th Cir. 2001). We must "give due weight to inferences drawn from [the] facts by resident judges and local law enforcement officers." *Ornelas v. United States*, 517 U.S. 690, 699 (1996).

[1] Officer Horn's statement that neighbors had complained of drug sales was materially false. *See United States v. Stannert*, 762 F.2d 775, 780-82 (9th Cir. 1985) (affiant's statement that someone had reported the manufacturing of drugs was materially false, when report had only been of suspected drug use). There had been no complaint of drug sales, only of drug use. That fact does not end the inquiry whether there was probable cause to believe that drug sales had been occurring, however, because suppression is required only if the remaining evidence is insufficient to establish probable cause. *See Franks*, 438 U.S. at 155-56. There is no such insufficiency here. Officer Horn stated in the probable cause statement and at the suppression hearing that the quantity and packaging of the drugs recently discovered on a resident of the house indicated to him drug sale activity. This was a reasonable interpretation of the facts, and the issuing judge was entitled to rely on the training and experience of Officer Horn. *See United States v. Chavez-Miranda*, 306 F.3d 973, 978 (9th Cir. 2002). Accordingly, the district court did not err in denying Payton's challenge to the validity of the warrant.

II. Scope of the Search Warrant

[2] We conclude that the search of Payton's computer exceeded the scope of the warrant and did not meet the Fourth Amendment standard of reasonableness. There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers. Such considerations commonly support the need specifically to authorize the search of computers in a search warrant, as Officer Horn requested in the present case. Despite his request, the warrant did not explicitly authorize the search of Payton's computer, and it incorporated Officer Horn's affidavit only to support probable cause, not to describe the objects to be searched or searched for. The after-the-fact testimony of the issuing judge that he intended expressly to authorize the search of computers could not cure the failure of the warrant to authorize the search of computers, because one purpose of a warrant is to inform the person subject to the search just what may be searched. *United States v. Hayes*, 794 F.2d 1348, 1355 (9th Cir. 1986).

The search warrant did explicitly authorize a search of Payton's premises to find and seize, among other things, “[s]ales ledgers showing narcotics transactions such as pay/owe sheets,” and “[f]inancial records of the person(s) in control of the premises.” The crucial question is whether these provisions authorized the officers to look for such records on Payton's computer. We conclude that, under our recent and controlling precedent of *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008), as applied to the circumstances of this case, they did not.

In *Giberson*, officers discovered that Giberson had used false identification and was delinquent in his child support payments. They obtained a search warrant authorizing a

search of his residence for, among other things, “‘records, documents or correspondence . . . related to the use or attempted use’ of other individual’s identities.” *Id.* at 884. During the search, the officers discovered a computer on a desk in Giberson’s bedroom; the computer was connected to a printer on a dresser. Next to the printer, the officers found a sheet of what appeared to be fake identification cards that were not of high quality and looked as if they could have been printed on the adjacent printer. In and on the desk, the officers found other documents evidencing the production of false identification, including fake Social Security cards and birth certificates. Acting on the advice of an Assistant U.S. Attorney who had been contacted, one of the officers secured the computer until the agents could obtain a second search warrant authorizing search of the computers for such documents. The computer was sent to a forensic laboratory, and a now-authorized search for false identification documents revealed images of child pornography, for receipt and possession of which Giberson was later charged. He challenged the seizure of his computer in the initial search of his residence.¹

[3] We stated the question that Giberson presented and our answer to it as follows:

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 docu-

¹Giberson also challenged the first search in the forensic laboratory on the ground that it was not properly confined to the second search warrant’s authorization of a search of the computer for false identification documents. We rejected that challenge and held that under available technology a search for false identification documents could not have been conducted in a manner that would avoid possible discovery of child pornography because both types of files were “innocuously labeled.” *Giberson*, 527 F.3d at 889-90. The inadvertent discovery of child pornography led to a third search warrant directed toward those images.

ments. We hold that, *in this case, where there was ample evidence that the documents 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.

Id. at 887 (emphasis added). As we read this passage, it holds that *under certain circumstances*, computers are not an exception to the rule permitting searches of containers to find objects specified in a warrant. A reasonable negative inference is that, absent those circumstances, a search of a computer not expressly authorized by a warrant is not a reasonable search. Those circumstances are absent in the present case. The search of Payton's residence for evidence of drug sales produced none. There was nothing in the neighborhood of Payton's computer, or indeed in the entire residence, that suggested that evidence of drug sales or anything else specified in the warrant would be found on the computer in his bedroom. It is true, of course, that pay/owe sheets indicating drug sales were physically capable of being kept on Payton's computer. But a similar bare capability was present in *Giberson*; a computer is physically capable of containing false identification documents. In *Giberson*, we did not simply recite that fact and uphold the seizure; we relied quite specifically on the documents found next to the printer and the computer, in circumstances indicating a likelihood that they were created on and printed from the computer. It was the presence of those documents that rendered the search reasonable.

[4] There was an additional factor that led us to conclude that the officers acted reasonably in *Giberson*. We stated:

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 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.

Id. at 889 (citation omitted). A seizure of a computer to await a second warrant is nevertheless a Fourth Amendment seizure, but it is far less intrusive than a search. In Payton's case, however, Officer Horn searched first and seized afterwards. When he first encountered the computer, he moved the mouse, inactivating the screen saver, and opened a file. In the absence of any circumstances supporting a reasonable belief that items specified in the warrant would be found on the computer, the search did not meet the Fourth Amendment standard of reasonableness.

We recognize that there are several statements in *Giberson* to the effect that no heightened Fourth Amendment standard should be applied to computers as opposed to other containers. For example, we stated that “[w]hile 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.” *Id.* at 888. We pointed out that, in *United States v. Gomez-Soto*, 723 F.2d 649 (9th Cir. 1984), we upheld a search of a cassette tape pursuant to a warrant that authorized a search for items that might be contained in it. *Giberson*, 527 F.3d at 888. If we permit such searches, “[t]here is no reason why material stored digitally on a computer should not also be searchable.” *Id.*

These and similar statements must be placed in context, however. They were made in response to Giberson's argument that computers could *never* be searched unless that authority was specifically granted in the search warrant. Indeed, Giberson conceded that it was reasonable for the officers to conclude that false identification documents might be found on his computer. *Id.* at 887. He contended, however,

that computers were sufficiently different from other containers that they were entitled to a bright-line categorical rule of heightened Fourth Amendment protection: no search is permissible without specific authorization in the warrant. Our opinion in *Giberson* rejected this contention, stating that the support for such an argument could not be “technology-specific” to computers alone. *Id.*

Thus *Giberson* held that computers were not entitled to a special categorical protection of the Fourth Amendment. Instead, they remained subject to the Fourth Amendment’s overall requirement that searches be constitutionally “reasonable.” *Id.* at 889. And, for the second time, *Giberson* stated its rule of reasonableness for the case before it:

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.

Id. at 888.

[5] In Payton’s case, however, the legitimating facts were absent. There was no comparable evidence pointing to the computer as a repository for the evidence sought in the search. The search of the computer preceded any attempt to secure the computer and seek a second warrant. We conclude that the search in those circumstances did not meet the Fourth Amendment requirement of reasonableness.

Our confidence in our conclusion is buttressed by contemplating the effect of a contrary decision. In order to uphold the

search in this case, we would have to rule that, whenever a computer is found in a search for other items, if any of those items were *capable* of being stored in a computer, a search of the computer would be permissible. Such a ruling would eliminate any incentive for officers to seek explicit judicial authorization for searches of computers. But the nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests. *See, e.g., United States v. Adjani*, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006). We believe that it is important to preserve the option of imposing such conditions when they are deemed warranted by judicial officers authorizing the search of computers. If unwarranted searches of computers are automatically authorized by upholding the search in Payton's case, that option will be lost. Indeed, the special considerations of reasonableness involved in the search of computers are reflected by the practice, exemplified in *Giberson*, of searching officers to stop and seek an explicit warrant when they encounter a computer that they have reason to believe should be searched.

[6] For all of these reasons, we conclude that the search of Payton's computer without explicit authorization in the warrant exceeded the scope of that warrant and did not meet the Fourth Amendment standard of reasonableness illustrated by *Giberson*. We accordingly reverse the district court's denial of Payton's motion to suppress the evidence resulting from the search, and remand the matter to the district court with instructions to permit Payton to withdraw his conditional guilty plea.

REVERSED and REMANDED with instructions.