FILED
United States Court of Appeals
Tenth Circuit

April 28, 2009

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff–Appellant, v. LORETTA OTERO, Defendant–Appellee.	No. 08-2154

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO
(D.C. NO. CR-07-386-MCA)

Fred J. Federici, Assistant United States Attorney, Las Cruces, New Mexico (Gregory J. Fouratt, United States Attorney, and Terri J. Abernathy, Assistant United States Attorney, Las Cruces, New Mexico, with him on the briefs), for Plaintiff-Appellant.

Michael A. Keefe, Assistant Federal Public Defender, Albuquerque, New Mexico, for Defendant-Appellee.

Before **McCONNELL**, **HOLLOWAY** and **BALDOCK**, Circuit Judges.

McCONNELL, Circuit Judge.

While neither rain nor sleet nor snow could keep the residents along Postal Highway Contract Route 64 in Los Lunas, New Mexico from receiving their mail,

the temptations of mail fraud and credit card theft were a different story. Loretta Otero, the assigned postal carrier for that route, was identified as the culprit and charged with a number of crimes arising out of her alleged theft. At trial, she moved to suppress two incriminating documents uncovered during a search of her computer on the grounds that the warrant authorizing the search lacked sufficient particularity. The district court agreed and suppressed the evidence. The government filed this interlocutory appeal under 18 U.S.C. § 3731. While we agree with the district court that the warrant was invalid for lack of particularity, we hold that the good faith exception to the exclusionary rule should apply and, accordingly, we reverse.

I. Background

In February 2001, a number of residents along Postal Highway Contract Route 64 began to lodge complaints that their mail was not being delivered. Specifically, they complained that they were missing credit cards, personal identification numbers, and billing statements. These residents had also noticed a number of unauthorized cash withdrawals from their accounts. Ms. Otero had been the assigned postal carrier on Postal Highway Contract Route 64 for more than thirteen years.

Understandably suspicious, Postal Inspector Stephanie Herman devised an investigation. On March 13, 2002, she prepared two test letters that appeared to be from credit card companies and were addressed to residents on Ms. Otero's

route. Inspector Herman then conducted surveillance of Ms. Otero as she made her deliveries, confirming that the two test letters were never delivered. When Ms. Otero completed her route, returned to the Los Lunas Carrier Annex, gathered her personal belongings, and left the building, Inspector Herman stopped her in the parking lot and inspected her bags. Inside the bags Inspector Herman found not only the two test letters, but also six other pieces of First Class Mail, all addressed to residents on Ms. Otero's route and all from credit card companies. Ms. Otero was immediately placed on suspension and another carrier took over her route. Although Ms. Otero had been relieved of her delivery duties, residents reported that a week after her suspension she in fact continued making deliveries, though only of a very particular type of letter: credit card-related mail with outdated postmarks.

On March 27, 2002, Inspector Herman prepared a search warrant for Ms. Otero's residence. Before bringing it to the magistrate judge, she took the warrant to an Assistant United States Attorney so that he could review it and confirm "that all of the information was there, . . . [that] there was probable cause and that it was legally correct." App. 127. Only after obtaining the AUSA's approval did she submit the warrant to the magistrate judge. The key portion of the warrant outlining the scope of the search was Attachment B, which read in full:

ITEMS TO BE SEIZED:

1. Any and all mail matter addressed to residents of Highway Contract Route 064 in Los Lunas, New Mexico.

2. Any and all credit cards, credit card receipts and/or other records bearing names, addresses and/or credit card numbers of known victims and other residents from Highway Contract Route 064 in Los Lunas, New Mexico.

3. Any and all credit cards, credit card invoices, receipts, statements, affidavits of forgery, pre-approved offers, applications, correspondence, automatic teller machine (ATM) receipts and/or other records related to credit card or other accounts at financial institutions and/or businesses for individuals other than residents of 123 La Ladera Rd., Los Lunas, NM 87031 [Ms. Otero's address].

4. Any and all mail matter or correspondence addressed to individuals other than residents of 123 La Ladera Rd., Los Lunas, NM 87031.

5. Any and all materials including but not limited to letters, correspondence, journals, records, notes, data and computer logs bearing victim information and/or other information related to or pertaining to the theft of mail, the fraudulent credit cards, bank fraud and conspiracy including but not limited to credit card offers, receipts, credit card statements, financial statements, and financial transaction records.

<u>COMPUTER ITEMS TO BE SEIZED</u>

6. Any and all information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media included floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes and other media which is capable of storing magnetic coding, as well as punch cards, and/or paper tapes and all printouts of stored data.

7. Any and all electronic devices which are capable of analyzing, creating, displaying, converting, or transmitting electronic or

> magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, cables, printers, plotters, encryption circuit boards, optical scanners, external hard drives, external tape backup drives and other computer-related electronic devices.
>
> 8. Any and all instructions or programs stored in the form of magnetic or electronic media which are capable of being interpreted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.
>
> 9. Any and all written or printed material which provides instructions or examples concerning the operation of the computer systems, computer software and/or any related device, and sign-on passwords, encryption codes or other information needed to access the computer system and/or software programs.

App. 63–64. Inspector Herman attached an affidavit in which she stated that, in her experience, "people engaged in this type of criminal activity often keep records on the computers, including the hard drive and disks," App. 69, and in which she explained the process for off-site recovery of such records and said that the search would "make every effort to review and copy only those programs, directories, files, and materials that are instrumentalities and/or evidence of the offenses described herein." App. 70. That affidavit, however, was not explicitly incorporated into the warrant.

The magistrate judge signed the warrant and Inspector Herman executed it on March 28, 2002. She seized a computer hard drive, eighty-eight floppy disks,

and two compact disks, all of which she sent to Robert Werbick, a forensic computer analyst with the Postal Inspection Service. Inspector Herman also sent a copy of the warrant, the application and affidavit in support of the warrant, and a cover letter explaining that the "search warrant was for items relating to the theft of credit cards and related correspondence from the mail on Highway Contract Route (HCR) 064." App. 72. The letter instructed Inspector Werbick to ascertain "[w]hether information described in Attachment B of the search warrant exists within the files on the hard drive, the floppy disks or the CDs." *Id.* She also included a list of known victims and a list of the names and addresses of persons along the delivery route.

Inspector Werbick conducted a keyword search of the hard drive and disks, using the list of victim names and credit card information that Inspector Herman had provided him. He did not, however, place a date restriction on his search that would limit the search only to files created during the time of the suspected credit card fraud. When the search generated a "hit," Inspector Werbick would examine the hit to determine whether or not it fell within the scope of the warrant. Most of the hits turned out to be "false hits." For example, a search based on a resident with the last name "Arnold" would also pull up files associated with "Arnold Schwarzenegger" or "Arnold Palmer." Two of the hits, however, uncovered highly pertinent information that someone had tried to delete from the hard drive. One was a credit card log that listed fourteen names, some of whom were known

victims, with accompanying headings such as "Pin," "Account Number," "Credit Limit," and "Address." The second was a list of names and addresses of individuals along Ms. Otero's route. Both of these files were found in the "unallocated space" of the hard drive, where deleted data is stored before it is then overwritten with new data. According to Inspector Werbick, a date restriction could not have been used in a search of unallocated space.

Ms. Otero was charged with a number of crimes, including theft or receipt of stolen mail in violation of 18 U.S.C. § 1708, theft of mail by an officer or employee of the postal service in violation of 18 U.S.C. § 1709, obstruction of correspondence in violation of 18 U.S.C. § 1702, and devising a scheme or artifice to defraud in violation of 18 U.S.C. §§ 1341 and 1346. At trial she moved to suppress, as the fruits of an invalid warrant, the two files uncovered from her hard drive. The court granted her motion, finding that the warrant was facially defective because it "purports to authorize the search and seizure of 'any and all' computer items—without limitation." Op. 12. The court rejected the government's argument that under a natural reading of the warrant the portion authorizing the computer search was limited to information pertaining to the alleged mail fraud and credit card theft. The court also rejected the government's assertion that the good faith exception applied. The government filed this interlocutory appeal.

II. Discussion

A. Particularity of the Warrant

The Fourth Amendment requires not only that warrants be supported by probable cause, but that they "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). *See also Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."). The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important. *See, e.g. United States v. Riccardi*, 405 F.3d 852, 863 (10th Cir. 2005) (warrant authorizing general search of computer invalid as it permitted officers to search anything "from child pornography to tax returns to private correspondence"); *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999) (computer search for files pertaining to

distribution of controlled substances uncovered child pornography). Because of this, our case law requires that "warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material." *Riccardi*, 405 F.3d at 862 (emphasis added).

Wisely, the government does not contest that a warrant authorizing a search of "any and all information and/or data" stored on a computer would be anything but the sort of wide-ranging search that fails to satisfy the particularity requirement. Its claim, rather, is that under a natural reading of the warrant the computer search is limited to uncovering only evidence of the mail and credit card theft along Ms. Otero's delivery route. In other words, paragraphs six, seven, eight, and nine, which fall under the heading "COMPUTER ITEMS TO BE SEIZED," are limited by paragraphs two, three, and five, which fall under the separate heading of "ITEMS TO BE SEIZED" and restrict the search to "information related to or pertaining to the theft of mail, the fraudulent credit cards, bank fraud and conspiracy." App. 63.

It is true that "practical accuracy rather than technical precision controls the determination of whether a search warrant adequately describes the place to be searched." *United States v. Simpson*, 152 F.3d 1241, 1248 (10th Cir. 1998) (quoting *United States v. Hutchings*, 127 F.3d 1255, 1259 (10th Cir. 1997)). A warrant need not necessarily survive a hyper-technical sentence diagraming and comply with the best practices of *Strunk & White* to satisfy the particularity

requirement. Nor is it beyond comprehension that the inspectors in this case would subjectively read the provisions pertaining to the computer search as being subject to the same limitations as the rest of the warrant, as the district court found they did. We agree with the district court, however, that the warrant describes the items to be seized with neither technical precision nor practical accuracy, and it therefore lacks sufficient particularity.

Attachment B is quite neatly divided into two subsections: "ITEMS TO BE SEIZED" and "COMPUTER ITEMS TO BE SEIZED." Each paragraph under the first section takes pains to limit the search to evidence of specific crimes or evidence pertaining to specific persons along Ms. Otero's delivery route. Each paragraph under the second section, in contrast, has no limiting instruction whatsoever. Read alone, they each authorize a search and seizure of "[a]ny and all" information, data, devices, programs, and other materials. There is no explicit or even implicit incorporation of the limitations of the first five paragraphs. The computer-related paragraphs do not even refer to the rest of the warrant. In fact, the presence of limitations in each of the first five paragraphs but absence in the second four suggests that the computer searches are *not* subject to those limitations. Even when read in the context of the overall warrant, therefore, the paragraphs authorizing the computer search were subject to no affirmative limitations.

The government contends that the warrant in this case is comparable to the warrant in *United States v. Brooks*, which we upheld. 427 F.3d 1246 (10th Cir. 2005). That warrant authorized officers to search for "evidence of child pornography," including "photographs, pictures, computer generated pictures or images, depicting partially nude or nude images of prepubescent males and or females engaged in sex acts," as well as "correspondence, including printed or handwritten letters, electronic text files, emails and instant messages." *Id.* at 1252. A technical reading of that warrant might suggest that the search of correspondence was wide-ranging and not limited to correspondence that related to child pornography. In context, however, we found that while "the language of the warrant may, on first glance, authorize a broad, unchanneled search through [the] document files, as a whole, its language more naturally instructs officers to search those files only for evidence related to child pornography." *Id.* (emphasis omitted). The warrant authorizing the search of Ms. Otero's computer, however, has significant structural differences from the warrant in *Brooks*. In *Brooks*, the portion authorizing the text search was not separated by paragraphs and headings from the portion authorizing the image search; the two portions were contained in a single paragraph, with no separation, and appeared under the same heading, namely, "evidence of child pornography." The structure of the warrant in *Brooks* thus suggested that the image and text searches were subject to the same

limitations, whereas the structure of the warrant in this case, with its clearer divisions and stark contrasts between the two sections, suggests the opposite.

Differences such as subject headings and paragraph formation might seem insignificant, but if we are to follow our command of reading each part of the warrant in context, these structural indicators are useful tools. Affording the government a practical rather than a technical reading does not require us to indulge every possible interpretation. Though a reasonable person might be forgiven for reading the entire warrant as subject to limitations, we believe that the most practical reading authorizes a wide-ranging search of Ms. Otero's computer. The warrant as it pertained to the computer search was therefore invalid.

B. The Good Faith Exception

Finding that a warrant is invalid does not automatically require application of the exclusionary rule, and the motion to suppress should still be denied if the government can avail itself of *United States v. Leon*'s good faith exception. 468 U.S. 897 (1984). As the Supreme Court recently reemphasized, the exclusionary rule is a judicially-fashioned super-compensatory remedy whose focus is not on restoring the victim to his rightful position but rather on general deterrence. *See Herring v. United States*, --- U.S. ----, 129 S. Ct. 695, 699–700 (2009). Because of this underlying purpose, "evidence should be suppressed 'only if it can be said that the law enforcement officer had knowledge, or may properly be charged with

knowledge, that the search was unconstitutional under the Fourth Amendment.'" *Id.* (quoting *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987)). In this case, the officers testified that they read the second half of the warrant as limited by the first, and the district court explicitly credited their testimony. They therefore did not have subjective "knowledge . . . that the search was unconstitutional." *Id.*

Even if an officer lacks subjective knowledge that a warrant is legally deficient, however, pre-*Herring* precedent holds that "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923; *see also Massachusetts v. Sheppard*, 468 U.S. 981, 988 (1984) ("[T]he only question is whether there was an objectively reasonable basis for the officers' mistaken belief."). The test is an objective one that asks "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n. 23. Not every deficient warrant, however, will be so deficient that an officer would lack an objectively reasonable basis for relying upon it. "Even if the court finds the warrant to be facially invalid . . . it 'must also review the text of the warrant and the circumstances of the search to ascertain whether the agents might have reasonably presumed it to be valid.'" *Riccardi*, 405 F.3d at 863 (quoting *United States v. Leary*, 846 F.2d 592, 607 (10th Cir. 1988)). We must "consider all of the circumstances," not only the text of the warrant, and we "assume that

the executing officers have a reasonable knowledge of what the law prohibits." *Id.* (internal quotations omitted).

In this case, Inspector Herman attempted to craft a warrant that would authorize a search for evidence of mail and credit card theft that had been hidden on Ms. Otero's computer. While the actual drafting did not accomplish her goals, one can see how a reasonable officer might have thought that the limitations in the first portion of Attachment B would be read to also apply to the second portion. Inspector Herman did not stop at her own understanding of the warrant, but sought the assistance of the Assistant United States Attorney, who ensured her that it satisfied the legal requirements. The magistrate judge then added his own approval. The affidavit that accompanied the warrant limited the computer search to those federal crimes for which there was probable cause. In enlisting Inspector Werbick's help in searching the disks and hard drive, Inspector Herman sent him not only the warrant but her affidavit, as well as instructions to search for items related to the theft of mail and credit card-related materials from Ms. Otero's mail route. She also provided him with information pertaining to known victims that would assist him in this search. Inspector Werbick understood his search as being limited to evidence of mail and credit card theft along Ms. Otero's route, and accordingly conducted a keyword search geared toward information about the known victims. Both Inspectors Herman and Werbick therefore had reason to believe that the warrant was subject to limitations, and they conducted their

search accordingly. This is not the kind of "flagrant or deliberate violation of rights," *Herring*, 129 S. Ct. at 702 (quoting Henry J. Friendly, *The Bill of Rights as a Code of Criminal Procedure*, 53 Cal. L.R. 929, 953 (1965)), that the exclusionary rule was meant to deter.

This case is quite close to that of *United States v. Riccardi*, where we applied the good faith exception to a computer search that uncovered child pornography, despite the fact that the warrant lacked particularity. 405 F.3d at 863–64. The warrant in that case was even more obviously deficient than in the present case, with no argument that context prevented the warrant from authorizing seizure of "all electronic and magnetic media stored [in the computer]." *Id.* at 862. We nonetheless found a number of factors that indicated the good faith of the officers: the attached affidavit limited the search to the crime for which there was probable cause; the officers executing the warrant were involved in the investigation throughout, and one of them wrote the affidavit to support the application; the officer received assurances that the warrant was legally sufficient; the search methodology was limited to uncovering evidence of the crimes identified in the affidavit; and the officers seized only evidence relevant to those crimes. These factors showed that the officers "did not conduct a 'fishing expedition' beyond the scope of the authorized investigation," making it an "example of the more 'usual' case in which the executing officers acted in good faith." *Id.*

The present case does not precisely mirror the facts of *Riccardi*—here, the officer who wrote the affidavit was not directly involved in the forensic analysis of the computer, but instead instructed another officer on what to search for—but we nonetheless find them substantially similar. The fact that the officer conducting the computer search had not been involved from the beginning of the investigation does not alone militate against good faith when that officer received—and, more importantly, followed—search instructions that limited the scope of his search to crimes for which there was probable cause. Moreover, one of the more important facts that the two share in common is the officers' attempts to satisfy all legal requirements by consulting a lawyer. *See id.* at 864. ("By consulting the prosecutor, they showed their good faith in compliance with constitutional requirements."). Indeed, a frequent criticism of the good faith exception is that it encourages officers *not* to make these consultations and "risk that some conscientious prosecutor . . . will say the application is insufficient when, if some magistrate can be induced to issue a warrant on the basis of it, the affidavit is thereafter virtually immune from challenge[.]" WAYNE R. LEFAVE, 1 SEARCH AND SEIZURE 68 (4th ed.). The fact that Inspector Herman, like the officer in *Riccardi*, made this step is an important indicator of her good faith. If more officers took such precautions we would have greater rather than less protection of Fourth Amendment rights.

The district court questioned whether Inspector Werbick's search methodology was in fact limited in scope to items for which there was probable cause. Dist. Op. 21. Specifically, it noted that the search did not include a date restriction and also generated false hits, which required him to view non-relevant information. The search methodology, however, does not seem to have been motivated by any belief that the warrant gave Inspector Werbick free rein over Ms. Otero's computer, but by the fact that "[g]iven the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science." *Brooks*, 427 F.3d at 1252. A date restriction, for instance, would have been impossible to apply in the search of the unallocated space where the two pertinent documents were found, and even in other portions of the hard drive and disks we do not know how effective the restrictor would have been. This search was reasonably constructed to limit the amount of irrelevant data while still effectively uncovering relevant evidence. The fact that some irrelevant information was viewed resulted more from the ease of electronically storing (and hiding) vast amounts of invisible information than any overreaching on the part of the officers.

The inspectors in this case had reason to believe the warrant was valid, considered themselves authorized to search only for evidence of crimes for which they had probable cause, and conducted their search accordingly. We therefore

hold that the good faith exception should apply and the evidence should not be excluded.

III. Conclusion

Though we agree with the district court that the warrant authorizing the search of Ms. Otero's computer lacked particularity, because we find that the good faith exception applies, we **REVERSE** the district court's order to suppress and **REMAND** for further proceedings consistent with this opinion.

No. 08-2154, United States v. Loretta Otero

BALDOCK, J., concurring in part and concurring in the judgment.

In my view, the slender criticisms lodged against the warrant's particularity pale in comparison to the good faith of the officers involved in this case. Accordingly, I would not reach the validity of the search warrant and do not join Part II.A of the Court's opinion. See United States v. Leon, 468 U.S. 897, 925 (1984) (recognizing that reviewing courts possess the discretion to immediately turn to "a consideration of the officers' good faith"). I gladly concur in Part II.B of the Court's opinion, excepting the language which references the invalidity of the warrant, and in the Court's judgment reversing the district court's suppression order.