CASE NO. 3:08CR00224 (AWT)
United States District Court, D. Connecticut

U.S. v. Ganias

Decided Jun 24, 2011

CASE NO. 3:08CR00224 (AWT).

June 24, 2011

RULING ON MOTION TO SUPPRESS EVIDENCE

ALVIN THOMPSON, District Judge

Defendant Stavros Ganias ("Ganias") filed a motion to suppress evidence. For the reasons set forth below, the motion was denied.

I. FINDINGS OF FACT

In approximately September 1998, Industrial Property Management ("IPM"), a company owned by co-defendant James McCarthy ("McCarthy"), was awarded a contract to provide security for and to maintain the government-owned property at 500 Main Street, Stratford, Connecticut, formerly the Stratford Army Engine Plant ("SAEP"). The United States Army ceased operations at the plant in approximately 1998, and it engaged IPM to maintain the facility and provide security for the property pending transfer of the property to the City of Stratford.

The contract awarded to IPM was initially on a "cost-plus" basis; the Army would reimburse the contractor for all of its expenses and pay in addition a negotiated fee. However, at some point after September 2002, when the
2 contract was re-bid and IPM lost the contract, but before November 17, 2003, the contract was *2 converted into a fixed-price contract as a result of a lawsuit filed by IPM against the government in the United States Court of Federal Claims.

In approximately August 2003, Special Agent Michael Conner ("Conner") of the U.S. Army Criminal Investigation Division ("Army CID") received word that an anonymous telephone caller ("CS-1") had made allegations regarding misconduct or potential misconduct at the SAEP. In September 2003, Conner and Special Agent James Cary of the Defense Criminal Investigative Service (who had received the initial call) met with CS-1. Conner met with CS-1 on ten to 15 occasions over the next several months.

During his conversations with Conner, CS-1 made a number of allegations of misconduct at SAEP. First, he provided information regarding the theft of Army property from the facility. Second, he alleged that during the period in which IPM had the cost-plus contract with the Army, IPM employees had performed work for American Boiler, Inc. ("AB"), another of McCarthy's companies. Although AB did not have a contract with the Army, the work had been billed to the Army. Third, he alleged that the environmental subcontractor for SAEP was a company owned by IPM's operations manager, Richard Meier, and McCarthy's daughter, Megan McCarthy. Fourth, CS-1 alleged that IPM had been presented to the Army as a woman-owned business, owned

by McCarthy's wife Lyn McCarthy, but that he had rarely seen Lyn McCarthy at the facility and the company
3 was operated by *3 McCarthy on a day-to-day basis. Fifth, CS-1 alleged that Richard Meier had used personnel employed by IPM to do construction work at his residence during their regular workday, while billing the labor to the Army.

Conner investigated this information in a number of ways, including checking the companies' filings with the Connecticut Secretary of the State's office and records at the Connecticut Department of Labor. CS-1 told him that IPM and AB's books were kept by Ganias, doing business as Taxes International. Connor drove by the addresses that CS-1 gave him for the offices of AB and Taxes International, respectively, and verified that the companies were located at those addresses. Conner also met with a former employee of IPM, CS-2. CS-2 provided information similar to that provided by CS-1. CS-2 also provided evidence that suggested that James McCarthy had been signing documents requiring the signature of Lyn McCarthy, including contracts with the Army.

On November 17, 2003, Conner received authorization from a magistrate judge for three search warrants: (1) for the SAEP, 550 Main Street, Stratford, Connecticut; (2) for the offices of Taxes International, 170 North Plains Industrial Road, Wallingford, Connecticut; and (3) for AB's offices, 214 Benton Street, Stratford, Connecticut. These search warrants were executed on November 19, 2003.

4 The warrants authorized the seizure from all three locations *4 of computer hardware, software, and computer-related data relating to the business, financial, and accounting operations of IPM and AB. Because Conner sought, and was authorized to seize, computer data, he obtained the assistance of Army CID's Computer Crimes Investigative Unit ("CCIU"), a section of his agency with specialized expertise in forensics and computer imaging. Special Agents David Shaver ("Shaver"), Jennie Callahan ("Callahan"), and Harold Van Duesen of the CCIU (collectively the "CCIU Agents") assisted with the execution of the warrants. On November 19, 2003, these three agents seized the computer data on 11 computers from the three locations, including three computers from Ganias's office. Ganias was present at the time of the search and spoke to the agents.

The data on these 11 computers was copied onto blank external hard-drives brought by the agents, making "mirror images" of the hard drives of the computers, at the locations that were searched.[1] The CCIU Agents
5 chose to make mirror images *5 because they believed that it could have taken months to do a file-by-file search of the computers. Had the CCIU Agents seized the computers themselves, as they were authorized to do under the warrant, it would have prevented the people at IPM, Taxes International, and AB from using their computers for the entire time the agents were conducting their search. A full search would have taken months to complete for several reasons. First, the processing time of computers was slow enough in 2003 that a search through the full hard drive of a computer would have been time-consuming, and a search of multiple computers even more so. Second, it would also have taken a significant amount of time to search the computers because using forensic software to review documents created with proprietary software, such as QuickBooks and TurboTax, is especially difficult, and requires copies of the correct versions of the programs, which the agents did not have. Third, the search had to be conducted with care because data could have been hidden or disguised
6 through encryption of the *6 data or by simply renaming a file to have a different extension.[2]

[1] A "mirror image" of a computer is an exact copy of the data contained in a particular digital storage unit, such as a computer hard drive. Computer code is a series of zeroes and ones, each of which is called a bit; making a mirror image is copying each zero or one in sequence, bit by bit. The CCIU Agents made the mirror images in this case by removing the hard drives from the computer to be searched (the "source hard drives") and connecting them to a laptop with a

blank external hard drive (the "clean hard drive") attached. The CCIU Agents used a "write-blocker" to prevent the data from being altered in the process of making the mirror image. The write blocker can either be in the form of hardware that attaches to the source hard drive or in the form of software that has the same effect. The agents used imaging software called EnCase to copy the data from the source hard drive to the clean hard drive. The data from the source hard drive was not stored on the laptop running the imaging software; it was only saved on the clean hard drive, which had been previously checked to ensure that it contained only zeroes, i.e. contained no data. Before copying the data from the source hard drive, EnCase read the entire sequence of ones and zeroes on the source hard drive and calculated a unique number, or "hash value," that described that data. After the program had copied the data onto the clean hard drive, the program ran the sequence of ones and zeroes on that drive. The hash value was the same for both hard drives, which showed that the data on the copy was identical to the data on the source hard drive.

[2] Each computer file has a unique name identifying it on the computer, for example, "Family Photograph" and a file extension, which tells the computer the format of the document, for example ".jpg," which designates a picture. A computer user could disguise the file by changing the file extension so that "Family Photograph.jpg" becomes "Family Photograph.wpd," which would indicate a WordPerfect text document. Someone who was searching a computer for pictures by looking for the file extension ".jpg" would then fail to find the "Family Photograph" file.

The following day, November 20, 2003, the 11 mirror images were compressed onto a single hard drive, which was provided to Conner, who maintained it as evidence. The external hard drives the CCIU Agents had used in making the mirror images during the search were retained by Shaver after the search. Approximately eight days after the search, Shaver provided Conner with two 19-DVD sets made from those external hard drives; each set contained mirror images of the 11 computers. After making the two sets of DVDs, Shaver "purged" the external hard drives, erasing all data from them.[3] One of the DVD sets was maintained as evidence and the other was used as a working copy.

[3] The external hard drives were purged by filling the hard drive with zeroes, so that there was literally no more information on the drive. This process is the same one used on the hard drives before the search to make sure that the only data they contained came from the computers being searched.

On February 5, 2004, Conner prepared a request and sent one set of 19 DVDs, along with the request, to the U.S. Army Criminal Investigation Laboratory, along with a copy of one of the search warrants. The Criminal
7 Investigation Laboratory's duty was to review the computer data for information that was generally *7 pertinent to the investigation, make that information available to the case agent, and segregate the remainder of the information. Gregory Norman ("Norman"), a digital evidence examiner employed by the Army Criminal Investigation Laboratory, was assigned to conduct the review in early June 2004.

While reviewing the paper documents seized during the November 2003 search, Army CID agents found evidence of payments made by IPM to a company called Industrial Management Services ("IMS"), which was owned by an individual named William DeLorenze ("DeLorenze"). Although IPM invoiced IMS in 1998, IMS was not registered with the Connecticut Secretary of the State until 1999, notwithstanding the fact that such registration is required of military contractors and subcontractors. In addition, the Connecticut Department of Labor provided the agents with information reflecting that DeLorenze was a full-time employee of Travelers Insurance and was not receiving wages or salary from any other entity.[4] As a result, in March 2004, Conner contacted IRS Criminal Investigation. On March 26, the IRS attended a briefing at the United States Attorney's office. On the same day, Special Agent Michelle Chowaniec ("Chowaniec") replaced Conner as the primary
8 case agent for Army CID. In early May 2004, the IRS was officially authorized to join the *8 investigation. At that time, the case was assigned to Special Agent Paul Holowczyk ("Holowczyk") of the IRS, and in September 2004, Special Agent Amy Hosney ("Hosney") began working on the case as the case agent.

4 The agents came to believe that companies doing work for IPM were directed to submit their bills to IMS, which then inflated the bill and invoiced IPM.

On May 20, 2004, the set of 19 DVDs that had not been sent to the Army Criminal Investigation Laboratory was provided by Chowaniec to Holowczyk. The same day, Holowczyk turned them over to Special Agent George Francischelli ("Francischelli"), the IRS computer specialist assigned to the case, who maintained them as evidence until June 30, when he transmitted the DVDs to Special Agent Vita Paukstelis ("Paukstelis"), another computer investigative specialist for the IRS. Francischelli also provided Paukstelis with a copy of the search warrant for Taxes International, including the list of items to be seized and the affidavit submitted with the search warrant application, and a note listing companies, addresses, and key individuals relating to the investigation. On the note was a handwritten notation next to the name "Taxes International" that stated "(return preparer) do not search."

Meanwhile, in the first week of June 2004, Chowaniec asked Holowczyk about whether the IRS had begun a forensic examination of the computer data, and also had a conversation with the Army lab about whether it had begun its examination of the computer data. Neither had. The IRS examination was not commenced by
9 Paukstelis until she received the DVDs at the end of June, and *9 the Army Criminal Investigation Laboratory had not yet assigned an examiner to the project.

In mid-June 2004, Chowaniec learned that Norman had been assigned to conduct the forensic examination of the 19 DVDs. Norman and Chowaniec exchanged a number of communications in the first week of July about how to narrow the search of the data, because Norman's first attempted search had yielded too many results for a practicable review. In mid-July, Norman informed Chowaniec that he had nearly completed his examination, and suggested that she acquire a current copy of TurboTax and a Premiere Edition of QuickBooks. Around July 23, 2004, Chowaniec received a final report and a CD from Norman. Norman returned the 19 DVD set he had been analyzing to Army CID's evidence custodian in Boston.

Sometime in the next few days, Chowaniec conducted a cursory review of the categories and file titles of items extracted by Norman and saved to the CD that he had sent her. Around the same time, Conner looked at files from Norman's examination relating to AB and a company named Victory Plumbing. However, neither Conner nor Chowaniec looked at any TurboTax or QuickBooks files; they did not have the software and thus did not have the capability to do so. In early August 2004, Chowaniec received the software for TurboTax and QuickBooks and loaded it into her computer and attempted to look at TurboTax files, without success. Neither
10 she nor Conner looked at any QuickBooks files *10 at that time. The agents tracked other leads until October 2004.

Between the end of June and the beginning of October, Paukstelis conducted an examination of the subset of the 19-DVD set that contained the images of the three computers from Taxes International. After loading the data from the DVDs onto her computer's hard drive, she used forensic software called ILook, which works in a manner similar to EnCase, and like EnCase cannot open QuickBooks or TurboTax files without that proprietary software also being on the computer. Paukstelis scanned the files she could open, bookmarking and extracting any files she believed were within the scope of the warrant. She also extracted nine QuickBooks files and 18 TurboTax files that appeared to her to be within the scope of the warrant based on the information to which she had access. Paukstelis copied the files she extracted onto a CD; she sent three copies of that CD to Holowczyk or Hosney around the beginning of October 2004. She did not search any client files of Taxes International that did not appear to be directly relevant to the list of entities provided by Francischelli.

Paukstelis also prepared a "restoration" of the three images of the Taxes International computers using a program called VMware. VMware is software that enables a user to simulate the experience of using another computer. By creating the restorations, Paukstelis (and any other person with the VMware software) was able
11 to use her computer to browse the files on the *11 Taxes International computers as if she was using those computers themselves at the time the images were made. Around November 30, 2004, Paukstelis completed this restoration and sent a hard drive containing that restoration to Francischelli. Paukstelis kept the hard drive with the three images she had loaded onto her computer, as well as the 19 DVDs, in her case file and stored them there.

Around October 4, 2004, Hosney received a copy of the CD containing the material that Paukstelis had extracted from the three Taxes International computers. At the end of October 2004, Hosney and Chowaniec engaged in an initial review of the items on the CD prepared by Paukstelis. They could not open any TurboTax or QuickBooks files because they did not have the programs which would permit them access to the content of those files.

In November 2004, Chowaniec opened on her office computer two IPM QuickBooks files that had been extracted by Greg Norman and looked at the content of those two files. She only looked at QuickBooks files for IPM. That was the only time she reviewed any QuickBooks file at her own office. On December 16, 2004, Hosney met with Chowaniec and Defense Contract Audit Agency auditor Margie McEachearn ("McEachearn"). The three of them looked at QuickBooks files related to IPM, using the VMware restoration provided by Paukstelis to Francischelli. Although they were authorized to do so, they did not look at any AB files.

12 Around November 30, 2004, McEachern provided Hosney with *12 paper files taken from Ganias's office during the November 19, 2003 search pursuant to the November 17, 2003 warrant, which appeared to show that amounts earned by AB had been deposited directly into IPM's account and posted to an IPM general ledger as a loan payable to AB but never reflected in AB's gross receipts for income tax purposes. By early 2005, as a result of reviewing these documents, Hosney became aware that Ganias was the individual who had deposited a majority of the checks payable to AB into IPM's account and that, in some instances, Ganias had made these deposits within a short time after signing tax returns for AB that did not reflect income from the checks that had been deposited into IPM's account. As a result of this analysis, and knowing that Ganias did the bookkeeping for IPM and was the tax preparer for both IPM and AB, Hosney subpoenaed Ganias's bank records. As a result of the review of Ganias's bank records and his role with respect to AB's under-reported income, the IRS investigation was expanded to include Ganias on July 28, 2005.

On February 14, 2006, Ganias and his attorney had a proffer session with Hosney. That day or shortly thereafter, Hosney requested Ganias's consent to access by the IRS to his QuickBooks file and that of his business, Taxes International. Hosney received no response and on April 24, 2006, obtained a search warrant
13 issued by a magistrate judge. *13

II. DISCUSSION

The defendant challenges the search of records from his business computers pursuant to the search warrants dated November 19, 2003 (the "2003 Warrant") and April 24, 2006 (the "2006 Warrant"). He argues that the 2003 Warrant was not supported by probable cause. He also argues that the retention by the government of the Taxes International files that were eventually searched pursuant to the 2006 Warrant was unreasonable. In

addition, he argues that the 2003 Warrant did not authorize making a "mirror image" of the computers, and that the 2003 Warrant was a general warrant in which the description of items to be seized was insufficiently particular.

-A-

With respect to the argument that the 2003 Warrant was not supported by probable cause, Ganias conceded at oral argument that even if the warrant was not supported by probable cause, suppression would be inappropriate because the officers could have relied in good faith on the warrant issued by the magistrate judge. See United States v. Leon, 468 U.S. 897 (1984).

-B-

Ganias argues that the data seized from his computers was held by the government for an unreasonably long period of time and should have been returned. He contends that the protocols for search and seizure of
14 computer data set forth in United States v. Comprehensive Drug Testing, 579 F.3d 989, 1006-07 (9th *14 Cir. 2009) (en banc), should have been followed by the government here.

The en banc opinion in Comprehensive Drug Testing was not issued until August 2009, while the events at issue in this case occurred between November 2003 and April 2006. For that reason, the government should not be required in this case to follow the guidelines set forth there, particularly because they were explicitly set forth as guidelines "for the future."Comprehensive Drug Testing, 579 F.3d at 1007. In addition,Comprehensive Drug Testing does not purport to set out rigid rules, but rather guidelines that address issues that will "nearly always" be present in the course of conducting searches of electronic data and that do not "substitute for the sound judgment that judicial officers must exercise" in striking the "delicate balance" between constitutional freedoms of citizens and the legitimate effort of the government to prosecute criminal activity. Id. at 1006-07. For this reason, the analysis inComprehensive Drug Testing provides guidance in assessing what is reasonable in the context of this case, but it does not provide a rule that must be complied with.

Moreover, Comprehensive Drug Testing involved a materially different procedural posture. There, the government appealed the quashal of a grand jury subpoena and two orders granting motions for return of
15 property pursuant to Federal Rule of Criminal Procedure 41(g). The present case, by contrast, involves a *15 motion to suppress evidence. The significance of this distinction is highlighted by the Ninth Circuit's opinion inUnited States v. Tamura, 694 F.2d 591 (9th Cir. 1982), upon which the guidelines in Comprehensive Drug Testing were based, and which would have been the relevant Ninth Circuit precedent at the time of the searches in this case. In Tamura, which was decided in the context of a motion to suppress, the court explicitly declined to mandate suppression of the evidence seized, noting that "where the Government's wholesale seizures were motivated by considerations of practicality rather than by a desire to engage in `fishing,' we cannot say . . . that the officers so abused the warrant's authority that the otherwise valid warrant was transformed into a general one, thereby requiring all fruits to be suppressed."[5] Tamura, 694 F.2d at 597.

[5] The court did note that the case was a close one. See id. InTamura, however, as in one of the orders addressed inComprehensive Drug Testing, the officers conducting the search seized items that were obviously outside the contemplated scope of the warrant. See Comprehensive Drug Testing, 579 F.3d at 993 ("[T]he warrant was limited to the records of the ten players as to whom the government had probable cause. When the warrant was executed, however, the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball. . . .) "; Tamura, 694 F.2d at 595 ("When the agents seized all Marubeni's records for the relevant time

> periods, they took large quantities of documents that were not described in the search warrant."). In the present case, by contrast, the warrant expressly contemplates the seizure of Taxes International's computers and the data they contain, even if that data is not relevant to AB and IPM.

Because of the timing of the decision and the procedural posture, Tamura is the more relevant case in assessing
16 the reasonableness of the agents' actions in the present case. The *16 guidelines set forth in Tamura suggest that:

> where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search. . . . If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material. . . . The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.[6]

Id. at 595-96.

> 6 The court in Comprehensive Drug Testing, also emphasized this point:
>
> > In the end, however, we must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity. Nothing we could say would substitute for the sound judgment that judicial officers must exercise in striking this delicate balance.
>
> Comprehensive Drug Testing, 579 F.3d at 1007.

The agents in this case, unlike the agents in Tamura, did in substance what these guidelines recommend. The 2003 Warrant contained guidance as to the appropriate search procedure for data stored on things such as "floppy diskettes, fixed hard disks, or removable hard drive cartridges, software or memory in any form." (Ex. #1 (Doc. #108), at 4.) It stated that the search procedure may include any of the following techniques:

> (a) surveying various file "directories" and the individual files they contain (analogous to looking at the
> 17 outside of a file cabinet for the *17 markings it contains and opening a drawer believed to contain pertinent files);
>
> (b) "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
>
> (c) "scanning" storage areas to discover and possibly recover recently deleted files;
>
> (d) "scanning" storage areas for deliberately hidden files; or
>
> (e) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

(Ex. #1 at 5.) Further, in 2006, when the agents wished to view documents outside the scope of the 2003 Warrant, the agents obtained authorization to do so by obtaining the 2006 Warrant.

While the agents did not actually "seal" the documents that were not found pertinent to IPM and AB by computer personnel other than the case agents, the documents were encoded so that only agents with forensic software not directly available to the case agents could view the data. The one exception to this, Paukstelis's

VMware restoration of the Taxes International computer hard drive images, was used by Hosney, Chowaniec, and McEachearn to look only at IPM files; they did not even review the AB files that they were also authorized to search.

The difference between the procedural posture in Comprehensive Drug Testing and that in Tamura suggests one reason for the differences between the guidelines it offers as an "update [of]Tamura" and Tamura itself.
18 Comprehensive Drug Testing, 579 F.3d at 1006. As noted above, the opinion in *18 Comprehensive Drug Testing arose in part in the context the motion for return of property pursuant to Federal Rule of Criminal Procedure 41(g). Rule 41(g) provides that

> [a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. . . . If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

Fed.R.Crim.P. 41(g). Because Ganias was present when the mirror images were made, he was aware in 2003 that agents of the government had copied his computer data. Further, he was aware in or about February 2006 that the government was in possession of that data and wanted his permission to search it. At that time Ganias could have moved for return of the property under Rule 41(g) in response to the government's possession for more than two years of computer data that it was not entitled to search under the 2003 Warrant. This would have given a court the opportunity to consider "whether the government's interest could be served by an alternative to retaining the property," In re Smith, 888 F.2d 167, 168 (D.C. Cir. 1989), and perhaps to order the property returned to Ganias, all while enabling the court to "impose reasonable conditions to protect access to the property and its use in later proceedings." Fed.R.Crim.P. 41(g). Although Comprehensive Drug Testing
19 states that "[t]he government must destroy or, if the recipient may lawfully possess it, return *19 non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept," Comprehensive Drug Testing, 579 F.3d at 1006, here the government was never asked to destroy or return data and its agents were justifiably concerned about preservation of evidence. The government complied in good faith with the warrant issued by the magistrate and, when it expanded the scope of the investigation and wanted to search more data, it sought and obtained authorization before doing so.

In sum, government agents seized the computer data pursuant to a valid warrant. They used a means less intrusive to the individual whose possessions were seized than other means they were authorized to use, by making mirror images of the computer hard drives rather than seizing and holding the computers themselves. The forensic examination of the computers by the computer specialists was conducted within the limitations imposed by the warrant, and the case agents viewed only data that had been extracted accordingly. A copy of the evidence was preserved in the form in which it was taken. The defendant never moved for destruction or return of the data, which could have led to the seized pertinent data being preserved by other means. Finally, when other leads led the government to expand its investigation, the agents obtained the 2006 Warrant, which authorized them to search the computer data in their possession that they were not authorized to view under the
20 2003 Warrant. Cf. United States v. *20 Riley 906 F.2d 841, 845 (2d Cir. 1990) ("Having found the rental agreement [for a storage locker in a search pursuant to a warrant of the defendant's home], the agents did not proceed lawlessly to search the locker; they presented their evidence to a magistrate who justifiably found probable cause to believe that a search of the locker would uncover evidence of drug trafficking.").

The difficulty of segregating and searching computer data that is pertinent to an investigation and can be legitimately searched by the government from nonpertinent data stored with it is a proper concern. Here however, where the searches and seizures were authorized by a magistrate judge, where government agents scrupulously avoided reviewing files that they were not entitled to review, and where the defendant had an alternative remedy pursuant to Rule 41(g) to avoid the complained of injury, i.e. that the government held his data for too long without returning or destroying it, the defendant has not shown that his Fourth Amendment rights were violated.

Because the court does not find that the retention of the computer data seized from Taxes International was in violation of the Fourth Amendment, the court does not address Ganias's argument that the material covered by the 2006 Warrant must be suppressed as the fruit of the poisonous tree.

-C-

Ganias argues that, because the 2003 Warrant as drafted allowed the seizure of every business computer as a whole, rather *21 than just the data relating to AB and IPM that could be found on the computers, the 2003 Warrant was a general warrant as written.

"A failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." United States v. George, 975 F.2d 72, 76 (2d Cir. 1992). "[T]he particularity requirement guards against general searches that leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized." United States v. Riley, 906 F.2d 841, 844 (2d Cir. 1990). "In upholding broadly worded categories of items available for seizure, [the Second Circuit has] noted that the language of a warrant is to be construed in light of an illustrative list of seizable items." Id. In Riley, the court observed:

> In the pending case, the warrant supplied sufficient examples of the type of records that could be seized-bank records, business records, and safety deposit box records. No doubt the description, even with illustrations, did not eliminate all discretion of the officers executing the warrant, as might have occurred, for example, if the warrant authorized seizure of the records of defendant's account at a named bank. But the particularity requirement is not so exacting. Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment as to whether a particular document falls within the described category.
>
> It is true that a warrant authorizing seizure of records of criminal activity permits officers to examine many papers in *22 a suspect's possession to determine if they are within the described category. But allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked "drug records."

Id.

In this case, the 2003 Warrant explicitly set forth a list of items to be seized that included "[a]ll . . . computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM and AB]. . . ." (Ex. #1 at 4.) Thus, the 2003 Warrant limits the Taxes International data authorized to be seized to that relating to the business, financial and accounting operations of IPM and AB. In addition, it recognizes that even as may occur with data that is not stored electronically, see Riley, the data authorized to be seized may be intermingled with data the government is not authorized to seize. Under such

circumstances, considerations of practicality justify seizure of the nonpertinent data. The 2003 Warrant gives guidance, appropriate for such a situation, in the form of a list of techniques that are permissible to use as part of the search procedure. Thus, the agents were not left to exercise their unguided discretion. Consequently, the 2003 Warrant is not a general warrant.

For these reasons, the court also finds unpersuasive Ganias's arguments that the 2003 Warrant did not authorize taking a "mirror image" of the computers and that, because the 2003 Warrant was executed by taking "mirror
23 images" of the hard drives *23 of the computers, the warrant was a general warrant as executed. It is true that the 2003 Warrant does not state explicitly that the agents can take mirror images of the computer hard drives. However the affidavit in support of the application for the warrant submitted to the magistrate judge stated that "searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment." (Conner Aff. (Doc. No. 108-1) ¶ 34.) It also stated that "[t]he search process can take weeks or months, depending on the particulars of the hard drive to be searched." (Id.) Ganias does not dispute that the agents were authorized to seize the computers and take them back to a laboratory to search for pertinent data. In addition, the search procedure does not exclude taking mirror images as a technique and the taking of mirror images enabled the government to perform the illustrative techniques listed in the warrant without compromising the integrity of the evidence. The taking of mirror images is also a means of removing from the premises the data the government was authorized to remove from the premises to conduct its search that significantly reduced the burden on Ganias and his business. Given the agents' ability to take mirror images, it made sense for them to do so, and their doing so was within the scope of all of the limitations
24 imposed upon them in the 2003 Warrant. It would require a hypertechnical *24 reading of the 2003 Warrant to conclude that the means of transporting the data that the government was authorized to seize resulted in a violation of the limitations imposed by the warrant. See Illinois v. Gates, 462 U.S. 213, 236 (1983) (quotingUnited States v. Ventresca, 380 U.S. 102, 108-09 (1965) (citations omitted)) ("`A grudging or negative attitude by reviewing courts toward warrants,' is inconsistent with the Fourth Amendment's strong preference for searches conducted pursuant to a warrant; `courts should not invalidate . . . warrant[s] by interpreting [. . .] affidavit[s] in a hypertechnical, rather than a commonsense, manner.'"). Such a hypertechnical reading of the 2003 Warrant would also be required to conclude that the taking of mirror images converted the 2003 Warrant into a general warrant where doing so resulted in the government being permitted access only to the identical information it otherwise was permitted access to and left the government subject to the same restrictions to which it was otherwise subject.

III. CONCLUSION

For the reasons stated above, the Motion to Suppress Evidence (Doc. No. 106) was denied.