12-240

To Be Argued By:
SANDRA S. GLOVER

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 12-240

UNITED STATES OF AMERICA,
Appellee,

-vs-

STAVROS M. GANIAS,
Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF CONNECTICUT

BRIEF ON REHEARING EN BANC FOR THE UNITED STATES OF AMERICA

DEIRDRE M. DALY
United States Attorney
District of Connecticut

SANDRA S. GLOVER
SARALA V. NAGALA
ANASTASIA ENOS KING
JONATHAN N. FRANCIS
Assistant U. S. Attorneys

WENDY R. WALDRON
Senior Counsel
Computer Crime &
Intellectual Property Section
U.S. Department of Justice

Table of Contents

Table of Authorities

Pursuant to "Blue Book" rule 10.7, the Government's citation of cases does not include "certiorari denied" dispositions that are more than two years old.

Cases

Statutes and Rules

Other Authorities

Statement of Jurisdiction

The United States District Court for the District of Connecticut had subject matter jurisdiction over this criminal case under 18 U.S.C. § 3231. Judgment entered on January 18, 2012, Joint Appendix 26 ("JA__"), and the defendant filed a timely notice of appeal pursuant to Fed. R. App. P. 4(b) on January 18, 2012, JA26. This Court has appellate jurisdiction pursuant to 28 U.S.C. § 1291.

Statement of Issues Presented for Review

I. Whether the Fourth Amendment was violated when, pursuant to a warrant, the government seized and forensically imaged three computer hard drives containing both responsive and non-responsive files, retained the imaged hard drives for approximately two-and-a-half years, and then searched the non-responsive files pursuant to a subsequently issued warrant.

II. Considering all relevant factors, whether the government agents in this case acted reasonably and in good faith such that the files obtained from the imaged hard drives should not be suppressed.

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 12-240

UNITED STATES OF AMERICA,
Appellee,

-vs-

STAVROS M. GANIAS,
Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF CONNECTICUT

BRIEF ON REHEARING EN BANC FOR THE UNITED STATES OF AMERICA

Preliminary Statement

In 2003, the government began an investigation into allegations of defense contracting fraud by two companies. Acting pursuant to a search warrant, the government made forensic images of three computers belonging to Stavros Ganias, the accountant who provided payroll and accounting services for those companies. The agents executing that warrant were careful to

stay within the parameters of the search warrant, looking only at information related to the two companies suspected of the contracting fraud. As the investigation continued, however, it became clear that Ganias himself may have been involved in criminal activity. Thus, in 2006, the government obtained a second warrant to search the forensic images in its possession for Ganias's business files. Evidence from that second review ultimately was introduced against Ganias in his tax evasion trial.

The government's actions in this case were reasonable and complied with the Fourth Amendment. The Fourth Amendment permits the seizure of computers to execute search warrants and further permits the retention of those computers—even if they contain non-responsive files—for legitimate government reasons, including, *inter alia*, evidence authentication and compliance with discovery obligations. Because the government legitimately holds the forensic images, a subsequent search of those images is generally reasonable where, as here, the search is authorized by a search warrant. But even if the government agents failed to comply with the Fourth Amendment in some respect, they acted in good faith, in reliance on two warrants, and with the goal of respecting the defendant's Fourth Amendment rights. Accordingly, there is no basis for suppression in this case.

Statement of the Case

On October 31, 2008, a federal grand jury returned an indictment against James McCarthy and Stavros ("Steve") Ganias. JA3. Ganias was the accountant and bookkeeper for McCarthy and two of his companies.

The grand jury returned a superseding indictment against McCarthy and Ganias on December 21, 2009. JA8; JA29-46. It alleged five counts under 18 U.S.C. § 371 and 26 U.S.C. § 7201: one count of conspiracy to defraud the United States in connection with taxes owed by McCarthy and one of his companies, one count of tax evasion against both defendants for evading McCarthy's taxes, one count of tax evasion against McCarthy for evading his own taxes, and two counts of tax evasion against Ganias for evading his own taxes. JA29-46.

In February 2010, Ganias moved to suppress evidence seized from the computers of his accounting business. JA10. Judge Alvin W. Thompson held a two-day hearing and ultimately denied the motion on April 14, 2010. JA12. The case was later transferred to Judge Ellen Bree Burns for trial. JA12.

In May 2010, Judge Burns severed the charges regarding Ganias's tax returns from the other

counts. JA13.[1] Ganias's trial began March 8, 2011. JA16. On April 1, 2011, the jury found Ganias guilty on both counts of tax evasion. Special Appendix ("SA__") 3; JA18.

On January 5, 2012, the district court sentenced Ganias to 24 months' imprisonment, followed by three years of supervised release. SA3-5; JA25-26. The remaining counts against Ganias were dismissed on the government's oral motion. JA25-26.

On June 17, 2014, a divided panel of this Court reversed the district court's denial of the motion to suppress, and thus vacated the judgment of conviction. *United States v. Ganias*, 755 F.3d 125 (2d Cir.). On June 29, 2015, the Court ordered that this appeal be heard *en banc*.[2] *United States v. Ganias*, 791 F.3d 290 (2d Cir.).

---

[1] McCarthy subsequently pleaded guilty to a substitute information, and the counts against him were dismissed. *United States v. McCarthy*, D. Conn. Crim. No. 3:08cr224 (EBB), Docket Entry 171.

[2] In the original appeal, Ganias challenged not only the denial of his suppression motion but also the denial of his new trial motion. *See Ganias*, 755 F.3d at 131-33. Although this Court's order granting *en banc* invited the parties to brief all issues relevant to the appeal, Ganias has elected not to pursue his challenge to the new trial motion.

Ganias's voluntary surrender date has been stayed pending resolution of this appeal. JA26.

A. The investigation into American Boiler and IPM begins.

This case began as an investigation into allegations of defense contracting fraud by two companies: Industrial Property Management ("IPM") and American Boiler. JA59-60. IPM, a corporation controlled by James McCarthy, had a contract with the United States Army to perform security and maintenance at a closed Army engine plant in Stratford, Connecticut. JA54; JA441-43. In August 2003, a confidential source told government investigators, *inter alia*, that IPM was stealing government property and improperly billing the Army for work done for American Boiler, another company controlled by McCarthy. JA58-60. Further investigation revealed that accounting and bookkeeping functions for both IPM and American Boiler were performed by Ganias, a former IRS agent with his own accounting business, "Taxes International." JA64; JA72; JA445. Ganias also submitted IPM's requests for payment to the Army. JA329; JA343.

Armed with this and other information from the investigation, on November 17, 2003, agents from the Army Criminal Investigation Command ("CID") obtained a search warrant for the offices of Taxes International, as well as for the shut-

tered Army plant and American Boiler's office. SA8; JA72-73. The warrants authorized the seizure of computers, computer hardware and software, and other materials relating to American Boiler and IPM. JA432-34; *see also* JA73-74.

Agents from Army CID and its specialized computer crimes unit executed the warrant at Taxes International on November 19, 2003. SA8-9; JA73; JA76. As pertinent here, the computer specialists made forensic images (sometimes called "mirror images") of three computers found at Taxes International, leaving the computers themselves there. SA9; JA79. A forensic image of a computer is an exact copy of the data contained on the computer, and is created with specialized forensic imaging software that copies each bit of computer code—a series of ones and zeroes—in sequence, "bit by bit." JA154-55; JA157-59; JA192; SA9 n.1. The computer specialists used a "write-blocker" to prevent the data from being altered in the process of making the forensic image. JA156; JA192-93. To ensure that the original and the image were forensically identical, a computer program calculated a unique number, or "hash value" for the original and, later, for the image. SA9-10, n.1; JA158-59. The hash values for the originals here matched the hash values for the forensic images, reflecting that the images were identical to the originals. SA9-10, n.1; JA159-60.

The computer specialists made forensic images of the computers because a full on-site search at Taxes International would have taken months to complete. SA10; JA181-82; JA449-50. Computer processing speed was substantially slower in 2003, which would have resulted in a very long on-site process. SA10; JA181-82. In addition, the agents did not have the proprietary software needed to access much of the data. SA10; SA14; JA177; JA185-86. Finally, as with many computer searches, there was a possibility that data within the scope of the warrant could have been hidden or disguised through encryption, which made on-site searching practically infeasible. SA10-11; JA162; JA194-96; *see also* JA448-50 (warrant affidavit explaining difficulties with searching computers on-site).

The forensic images of the three Taxes International computers were ultimately copied—along with the images of computers from the other two search locations—onto a hard drive secured in evidence and onto duplicate sets of 19 DVDs for use as working copies. JA84-86; JA161-63. In February 2004, the Army CID case agent sent one set of the 19 DVDs to the Army's forensic computer lab for analysis.[3] SA11; JA86-

[3] As explained by the Army CID agent, investigators typically do not delete data stored in evidence for an ongoing investigation; rather, they protect the evi-

87. At around the same time, as Army CID agents reviewed the paper documents seized during the November 2003 searches, they began to suspect that some of the companies involved might be engaged in tax fraud as well, and so the IRS joined the investigation. JA416. In June 2004, the Army provided the IRS with the other set of 19 DVDs. JA240-41.

The forensic examination of the computer evidence thus proceeded on parallel tracks by the Army and the IRS. In June and July 2004, an Army forensic computer examiner performed several different searches for potentially relevant information on the images, and ultimately copied several files onto a separate DVD that was provided to the Army CID case agent for assessment of relevance in late July 2004. SA14; JA213-15; JA223-29; JA292-93. Among the copied data were four files from "QuickBooks," a type of accounting and bookkeeping software. JA229; JA231-33.

At around the same time, an IRS computer specialist received a copy of the forensic images. JA240-41. Between June and October 2004, the IRS computer specialist examined the three forensic images of the computers from Taxes International. SA15; JA240-49. She bookmarked

---

dence in its original state for the life of the investigation. JA122; JA137-38; JA147.

and copied files that appeared to be within the scope of the warrant, including 18 TurboTax files and 9 QuickBooks files. SA15; JA245-46. She gave the copied files to IRS agents in October 2004. JA253; JA418-19.

In October 2004, the Army CID and IRS agents met to review computer files sent to them by their respective computer specialists, but they could not view any TurboTax or QuickBooks files because their computers did not have the appropriate proprietary software. SA16; JA293-94; JA337-38. In November 2004, the Army CID agent was finally able to access QuickBooks files, but she only reviewed two of those files related to IPM. SA16; JA295-96; JA314-15.

In late November 2004, the IRS computer specialist prepared a "restoration" of the three computers from Taxes International through VMWare, a software program that allows an investigator to boot up and view a forensic image in the way that the computer's owner would have viewed the information at the time of the seizure. SA15-16; JA251-52. This restoration was ultimately provided to the case agents, SA15-16; JA251-53; JA338, and thus in mid-December 2004, the agents had access to the IPM and American Boiler QuickBooks files. SA16; JA297-98.

B. The investigation expands to Ganias's tax violations.

At around the same time, the agents expanded their investigation to include possible violations of the tax laws by Ganias. In particular, they began to question—based on a review of paper documents seized from Taxes International and subpoenaed bank records—whether American Boiler's income was being reported properly on the tax returns prepared by Ganias. JA339; JA341-46; SA16-17. In addition, they began to question whether Ganias was properly reporting his *own* income. Bank records revealed, for example, that Ganias had signed, on behalf of IPM, more than $1 million in checks made out to himself from IPM. SA17; JA345-46; JA461. As a result of these and other questions, the investigation was officially expanded to include Ganias on July 28, 2005. SA17.

The government met with Ganias in a proffer session in February 2006, during which the government asked Ganias for consent to access the QuickBooks file he kept for himself and Taxes International, "Steve_ga.qbw". SA17; JA346-47. Thus, at that time, Ganias was aware that the government still possessed the Taxes International computer data that was seized in November 2003 (contrary to his later claim that he believed the government would purge the images, *see* JA428). SA23; JA347-48. Nevertheless, Ganias neither asked the government to return or

destroy that data nor filed a Rule 41(g) motion for return of property. SA23. Furthermore, Ganias did not respond to the government's request for consent to search his files.[4] JA347-48; JA372.

Without word from Ganias, the government obtained another search warrant in April 2006, authorizing it to search the three forensic images obtained at Taxes International while executing the November 2003 warrant. JA454-72. The 2006 warrant—signed by the same magistrate judge who authorized the 2003 search, *compare* JA430 with JA454—authorized the agents to search for data related to the "business, financial, and accounting activities" of Ganias and Taxes International existing on the images of computers seized on November 19, 2003, from the offices of Taxes International. SA17; JA454-56; JA463-64. The application noted that, in the process of accessing the QuickBooks files for

---

[4] Although the government did not know it at the time, the Taxes International computer data that it had seized in November 2003 only existed on the images that it had in its possession. As Ganias admits, had the government not retained the forensic images of the computers obtained from Taxes International in 2003, the original data (which showed the fraud) would have been irretrievable, as Ganias "corrected" at least 93 "errors" in his QuickBooks file just two days after execution of the November 2003 search warrant. Def. Br. at 15 n.7.

American Boiler and IPM earlier in the investigation, the agents could see a menu of the QuickBooks files, among which was "Steve_ga.qbw," which likely contained "the financial transactions for Steve S. Ganias dba Taxes International." JA464; JA467. It is undisputed, however, that the agents only opened the QuickBooks files for American Boiler and IPM before obtaining the 2006 warrant. JA314-15; JA340; JA464; SA22; SA25.

After obtaining the 2006 search warrant, the agents examined the "Steve_ga.qbw" file and found evidence that Ganias was manipulating QuickBooks to conceal taxable income he received. In particular, Ganias mischaracterized payments made to him by IPM as owner's contributions (*i.e.*, infusions of personal capital into his accounting business) or as cash-on-hand, omitted all or a portion of the checks he had received, and failed to apply payments received from clients to open invoices, thus preventing QuickBooks from recognizing the payments as income. JA349-50.

C. The district court denies Ganias's motion to suppress.

On February 27, 2010, Ganias moved to suppress the evidence seized from his accounting business. JA10. As relevant here, Ganias argued that the government violated his Fourth Amendment rights by retaining the images of

his computers for an unreasonably long period of time, and that the government should have followed the protocols established by *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009) (*en banc*)[5] in this case. SA18. He also argued that because the 2003 warrant was drafted to allow the seizure of his entire computer, and not just the data relating to IPM and American Boiler, it was equivalent to an unlawful general warrant. SA25-26.

The district court rejected both of Ganias's arguments. SA18-29. First, the district court held that the Ninth Circuit's decision in *Comprehensive Drug Testing* was inapposite because it was decided long after the searches in this case and involved a different procedural posture. SA18-24. Moreover, given that Ganias never moved for return of the data and that the government obtained the 2006 warrant, the district court found no Fourth Amendment violation. SA23-24. The district court also rejected Ganias's contention that the 2003 warrant was a general warrant, holding that "considerations of practicality" justified the seizure of the entire computer image and that the warrant was sufficiently particular to guide the agents in their review. SA25-29.

---

[5] This opinion was subsequently revised and superseded by *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (*en banc*).

Summary of Argument

I. The government complied with the Fourth Amendment in this case. The government reasonably made forensic images of Ganias's computers for subsequent off-site review. Indeed, the government's two-step approach not only complied with the prevailing standard for searches of computer data, but also was the only practical approach for search of that data. Moreover, this approach, as applied in this case where the agents scrupulously adhered to the terms of the indisputably particular warrant, did not violate the prohibition against general warrants.

In addition, the government reasonably retained the forensic images for the duration of the investigation and prosecution. The government's retention of the complete images allowed it to preserve its evidence, authenticate the computer data, comply with its discovery obligations, and continue the authorized search of the data in an evolving investigation. These legitimate government interests overcome any possessory interest Ganias has in his computer data.

Because the government acted reasonably in obtaining and retaining the forensic images in this case, its subsequent search of those images for evidence of tax violations by Ganias—under the authority of a new search warrant—was also reasonable. The images were legitimately in the government's possession, and the government

developed probable cause (based largely on evidence outside the retained forensic images) to believe that the images contained evidence of another crime. Thus, it is entirely reasonable for the government to obtain a subsequent search warrant to review a retained image anew. The individual's privacy interest is protected effectively by the issuance of a second warrant.

II. But even assuming, *arguendo*, a Fourth Amendment violation, suppression is not warranted because the government acted reasonably and in good faith throughout this investigation. To begin, the agents acted in good faith reliance on the first warrant and case law that supported their continued retention of the forensic images during the pendency of this criminal investigation. At a minimum, they acted with an objectively reasonable belief—in a new technological landscape—that their actions were justified. Suppression would serve no purpose here.

Moreover, the agents also reasonably relied on the issuance of the 2006 warrant to support their search. They fully informed the magistrate judge of all pertinent facts, and thus, under *United States v. Leon*, 468 U.S. 897 (1984), their conduct falls squarely within the good faith exception to the exclusionary rule. Finally, the costs of suppression in this case outweigh the benefits of suppression.

Argument

On review of the denial of a motion to suppress, this Court reviews the district court's legal conclusions *de novo* and its factual findings for clear error. *United States v. Bershchansky*, 788 F.3d 102, 108-10 (2d Cir. 2015).[6]

I. The search and seizure of the forensic images pursuant to two search warrants was consistent with the Fourth Amendment.

The Fourth Amendment protects both the property and privacy interests of an individual whose property is seized or searched. *Soldal v. Cook County, Ill.*, 506 U.S. 56, 62 (1992). The hallmark requirement of that Amendment is that searches and seizures must be reasonable. U.S. Const., amend. IV; *Ohio v. Robinette*, 519 U.S. 33, 39 (1996). "Reasonableness, in turn, is measured in objective terms by examining the

---

[6] In some cases, this Court has suggested that in review of a ruling on a motion to suppress, the Court views the evidence in the light most favorable to the prevailing party. *See, e.g.*, *United States v. Andino*, 768 F.3d 94, 98 (2d Cir. 2014); *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013); *United States v. Ramos*, 685 F.3d 120, 128 (2d Cir. 2012). *Bershchansky* calls that practice into question, but the question is ultimately inconsequential to the result here.

totality of the circumstances." *Id.* Indeed, the Supreme Court has "eschewed bright-line rules, instead emphasizing the fact-specific nature of the reasonableness inquiry." *Id.*

The government's actions here were reasonable. The seizure[7] and retention of the forensic images pursuant to a warrant was reasonable given the government interests served by that seizure as balanced against the limited impact on Ganias's possessory interests. The 2006 search was likewise a reasonable intrusion into Ganias's privacy given the judicial finding of probable cause.

A. The Fourth Amendment allowed the government to make forensic images of the computers and retain them for the duration of the case.

A "seizure" impacts an individual's property, or possessory, interests. *Segura v. United States*, 468 U.S. 796, 806 (1984). Thus, the reasonableness of a particular seizure is assessed by weigh-

---

[7] For purposes of this appeal, the government assumes that the collection of the forensic computer images was a "seizure." Consistent with this Court's order granting *en banc* review, the government uses the phrase "non-responsive data" to refer to data on a computer that was not specifically responsive to the 2003 search warrant that authorized the search of the computers.

ing the impact on the individual's possessory interests against the government's competing interests in seizing the property. *See, e.g., id.* at 806-10; *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1988). Where the government obtains an order or a warrant before a seizure, demonstrating unreasonableness is a "laborious task indeed." *Soldal*, 506 U.S. at 71.

1. The government's seizure of the forensic images—including both responsive and non-responsive data—for subsequent off-site review complied with the Fourth Amendment.

As a matter of first principles, it is undisputed that the government may obtain a computer or make a forensic image of the entire computer when executing search warrants for electronic evidence. In other words, an image of the whole computer, including both responsive and non-responsive data, may be collected for off-site review to identify information that is subject to seizure. This "two-step" method of first obtaining the forensic image of the computer, followed by an off-site search, is not only the prevailing standard for searches of electronic data, but also the only practical one.

Where the volume of material to be collected and reviewed is extraordinarily large, where responsive data is intermingled with large quanti-

ties of non-responsive data, or where other practical considerations would render on-site review difficult or impractical, it is reasonable for government agents to collect the materials for later off-site review. That rule, which first developed in cases involving searches of voluminous paper documents,[8] has particular relevance in the digital era, where searches of computers and other electronic devices—devices that hold exceedingly large quantities of data and that are particularly difficult to search on-site—have become more prevalent. *See*, *e.g.*, Brief of *Amici Curiae* Electronic Privacy Information Center at 4-10; *see also Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (describing "immense storage capacity" of modern cell phones, which "are in fact minicomputers"); *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006) ("Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be

---

[8] *See, e.g.*, *United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir. 1997); *United States v. Schandl*, 947 F.2d 462, 465-66 (11th Cir. 1991); *United States v. Santarelli*, 778 F.2d 609, 616 (11th Cir. 1985); *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) (noting that agents may apply for specific authorization to remove material where onsite sorting is "infeasible").

protected, the latter discovered.") (footnote omitted).

The volume of information contained on a computer is not the only factor that makes off-site review of computers necessary and reasonable in the majority of cases. Computer searches also require specialized skills and investigative techniques to protect the integrity of the evidence and to identify data responsive to a warrant—which could be encrypted or hidden on a computer. SA9-11; JA448-50; *see generally* Orin Kerr, Searches and Seizures in a Digital World ("Digital World"), 119 Harv. L. Rev. 531, 538-39 (2005). This specialized search process can take weeks or months. Kerr, Digital World, 119 Harv. L. Rev. at 538; JA450. Thus, the imaging process serves the dual function of leaving the actual computer at the business or residence—so as to minimize the intrusion on the business or individual—and allowing government agents to examine the computer in a controlled environment. SA10-11; SA24.

Indeed, neither Ganias nor his *amici* seriously dispute that making a forensic image of a computer for later off-site review is reasonable for computer searches. *See* Def.'s Brief at 27 ("[T]hese blanket seizures must now be tolerated . . . ."); *see also Ganias*, 755 F.3d at 135 ("[T]he creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers

would not be."). Moreover, the 2003 warrant in this case specifically authorized the seizure of computers and computer hardware. JA437.

In fact, the current version of Rule 41 specifically provides that a warrant seeking electronically stored information authorizes the seizure or copying of electronic data to be followed by "a later review of the media or information consistent with the warrant," unless otherwise provided. Fed. R. Crim. P. 41(e)(2)(B).[9]

Furthermore, every Court of Appeals to consider this issue has endorsed the two-step approach of removing or imaging a computer to be followed by an off-site review of computer data. *See, e.g.*, *Ganias*, 755 F.3d at 135-36 (collecting cases); *United States v. Balon*, 384 F.3d 38, 48

---

[9] This particular provision was added to the Rules in 2009. Prior to 2009, the Rules did not speak explicitly on seizure, copying, or review of electronically stored information. The 2009 Advisory Committee Notes recognized that a "substantial amount of time can be involved in the forensic imaging and review of information . . . due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of computer labs." Notably, the Committee stated that it was "not the intent of the amendment to leave the property owner without . . . a remedy" and explained that a "person aggrieved" by government seizure of property could file a Rule 41(g) motion for return of property.

(2d Cir. 2004) (recognizing, in the context of a condition of supervised release requiring review of a defendant's computer, that off-site review may allow for more comprehensive searches than on-site review); *see also United States v. Beckman*, 786 F.3d 672, 681 n.6 (8th Cir. 2015); *United States v. Huart*, 735 F.3d 972, 974 n.2 (7th Cir. 2013), *cert. denied*, 134 S. Ct. 1907 (2014); *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012); *United States v. Stabile*, 633 F.3d 219, 233-34 (3d Cir. 2011); *United States v. Grimmett*, 439 F.3d 1263, 1268-70 (10th Cir. 2006); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999); *see also In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxxx@gmail.com* ("*The Google Case*"), 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) (Gorenstein, M.J.).

2. The collection of forensic images did not violate the prohibition against general warrants.

Seizing or forensically imaging an entire computer for later off-site review does not transform properly drafted search warrants into general warrants. The term "general warrant" does not refer to warrants that merely provide agents with broad search and seizure authority; a "general warrant" instead is a warrant that fails to specify the scope of an authorized search and

seizure at all. Historically, the term was used to describe the "indiscriminate searches and seizures" conducted by the British in colonial times, pursuant to warrants that "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which . . . places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The particularity requirement of the Fourth Amendment was intended to prevent such searches, by requiring that a warrant specify: (1) the offenses for which probable cause has been established; (2) the places to be searched; and (3) the items to be seized as related to the specified offenses. *See United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013).

Although this Court has recognized the importance of a "heightened sensitivity to the particularity requirement in the context of digital searches," *Galpin*, 720 F.3d at 447, it has acknowledged that whether the particularity requirement has been met will turn on whether the warrant provides officers with sufficient guidance as to the type of evidence sought. *Compare id.* (warrant authorizing search of computer and other electronic devices simply for evidence of violations of "NYS Penal Law and or Federal Statutes" violated the particularity requirement) *and United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (warrant authorizing seizure of electronic equipment without specifying the legal vi-

olation "provided [officers] with no guidance as to the type of evidence sought" and constituted a general warrant) *with United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990) (rejecting particularity challenge to a warrant and explaining that "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").

That agents executing warrants for computers must seize or forensically image the entire computer, thus collecting both responsive and non-responsive data, does not transform an otherwise proper warrant into an impermissible general search warrant. *See United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir.) (noting that federal courts have "rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers"), *petn for cert. filed*, No. 15-5136 (July 10, 2015); *United States v. Fries*, 781 F.3d 1137, 1151 (9th Cir.) (search warrant "sufficiently circumscribed the agents' discretion" in computer search and affidavit sufficiently explained reasons for off-site analysis), *petn for cert. filed*, No. 14-10447 (June 26, 2015); *Schesso*, 730 F.3d at 1046 (warrant sufficiently particular, given challenge of identifying illicit files without knowing where or how they might be stored); *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000)

(affidavit that established "why it was necessary to seize the entire computer system" and "justified taking the entire system off site . . . makes inapposite *United States v. Tamura*"). To hold otherwise would treat nearly every computer warrant as a general warrant, regardless of whether the warrant itself—or its execution—was reasonable. That is not the law.

The warrants at issue here did not remotely resemble "general warrants." The warrants specified the offenses for which the accompanying agent affidavits established probable cause; they specified the premises to be searched; and they specified numerous categories of evidence the agents were authorized to seize. *See United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992) (no general warrant where warrant "identif[ies] with reasonable certainty those items that the magistrate has authorized [the agents] to seize").

Indeed, Ganias concedes that the warrants were sufficiently specific and gave adequate direction to the executing agents. *See* Def.'s Br. at 11 ("No one, at that point, was under any misconception about the warrant's scope."). That concession forecloses his argument that the 2003 warrant was an impermissibly general warrant, and makes his reliance on cases like *Stanford v. Texas*, 379 U.S. 476 (1965), largely irrelevant. The district court, too, found that the 2003 warrant was sufficiently specific to satisfy the particularity requirement. SA25-29.

Further, as Ganias properly recognizes, in determining what is responsive to the warrant, the government has significant latitude to review the collected data to determine what materials fall within the scope of the warrant. *See* Def. Br. at 22; *see, e.g.*, *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (noting that "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are" among the papers to be seized). The search of the computer "may be as extensive as reasonably required to locate the items described in the warrant," *Grimmett*, 439 F.3d at 1270, and this aspect of a properly executed computer search will not transform such a search into an unconstitutional general search.[10] *Id.*; *see also United States v. Johnston*, 789 F.3d 934, 942 (9th Cir.) (no general search where agents used searches "related directly to th[e] mandate" of the search warrant), *petn for cert. filed*, No. 15-5642 (Aug. 14, 2015); *United States v. Williams*, 592 F.3d 511, 521-22 (4th Cir. 2010) (warrant authorized agents to open each file on computer and review contents, at least cursorily,

[10] This Court has previously declined to impose specific search protocols. *See Galpin*, 720 F.3d at 451. Because Ganias has not challenged the government's search methods here, the advisability of such protocols is not before the Court.

to determine whether file fell under scope of search warrant).

The government's review of seized materials here was "confined to the terms and limitations of the warrant authorizing it," and was "conducted in a manner that minimize[d] unwarranted intrusions upon privacy." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) (citations omitted); JA314-15; JA340; JA464; SA22; SA25. As the district court found—and in stark contrast to the agents' behavior in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1169 (9th Cir. 2010) (*en banc*)—the agents here were careful to adhere to the limitations of the warrant and to avoid any searches of the forensic images outside the boundaries of the warrant.[11] SA25; SA27. In short, the 2003 warrant

[11] Some decisions rejecting a defendant's contentions that the search of the computer was an unconstitutional general search have also held that the seizure of data outside the scope of the warrant was permissible under the plain view doctrine. *See, e.g.*, *Williams*, 592 F.3d at 521-22; *Stabile*, 633 F.3d at 241-42. The facts of this case do not involve the plain view doctrine, further weakening Ganias's reliance on cases such as *Comprehensive Drug Testing*. *See Schesso*, 730 F.3d at 1047 (noting that "Schesso's scenario did not implicate the real concern animating the court in [*Comprehensive Drug Testing*] and *Tamura*: preventing the government from overseizing data and then using the process of identifying

satisfied the particularity requirement and was not converted into a general warrant or search by its manner of execution.

3. The government's retention of the forensic images during the pendency of the case served several legitimate government purposes.

After making the forensic images of Ganias's computers pursuant to the warrant authorizing seizure of those computers, the government reasonably retained those images during the pendency of the case. This Court has recognized that a defendant's "right to the return of lawfully seized property is subject to the Government's legitimate continuing interest in that property." *Lavin v. United States*, 299 F.3d 123, 128 (2d Cir. 2002). This rule is consistent with the general principle that the government's retention of property is reasonable if the government needs the property for an ongoing investigation or prosecution. *See Krimstock v. Kelly*, 464 F.3d 246, 251-52 (2d Cir. 2006) (noting that the government's need to retain evidence should be evaluated for reasonableness and that the government may have a continuing need to hold ev-

---

and segregating seizable electronic data 'to bring constitutionally protected data into . . . plain view'") (quoting *Comprehensive Drug Testing*, 621 F.3d at 1171)).

idence); *United States v. Christie*, 717 F.3d 1156, 1167 (10th Cir. 2013) (holding that after the government found incriminating evidence on a computer pursuant to a search warrant, it was "presumptively entitled" to retain the computer until the criminal proceedings terminated); *Ramsden v. United States*, 2 F.3d 322, 326 (9th Cir. 1993) (government's retention of property is generally reasonable if the government "has a need for the property in an investigation or prosecution"); *see also* 1989 Amendments to Advisory Committee Notes to Federal Rule of Criminal Procedure 41(e) (now Rule 41(g)) ("If the United States has a need for the property in an investigation or prosecution, its retention of the property generally is reasonable."); *In re Application of Madison*, 687 F. Supp. 2d 103, 117-18 (E.D.N.Y. 2009) (holding that an ongoing grand jury investigation justifies the government's continuing interest in retaining property).

There are legitimate governmental interests that support the preservation and retention of computer evidence in its original form for the duration of a pending case—through prosecution, appeal and collateral attack—and that make a "return or destroy" rule[12]—as proposed by Ganias and his *amici*—unworkable.

---

[12] From the government's perspective, there is little practical difference between a rule requiring "de-

First, the retention of a forensic image of a computer permits the authentication of that evidence by computer specialists. The creation of a forensic image of a computer, and the calculation of a "hash value" for the original and that image, generally allows a computer specialist to authenticate computer evidence as an exact copy of the original computer, a critical fact for authenticating evidence from that computer under Federal Rules of Evidence 901 and 1001-1006. *United States v. Scully*, __ F. Supp. 3d __, No. 14-CR-208(ADS)(SIL), 2015 WL 3540466, *40 (June 8, 2015) (recognizing that "it may be necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for trial") (internal quotations omitted); *The Google Case*, 33 F. Supp. 3d at 399 (same). *See also generally* SA9-10; JA158-60; JA172; Government's Second Supplemental Appendix ("GSSA__") 19-20. If even one small piece of data is altered on the image, the hash value of the original computer hard drive and the image will no longer match. *See* Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 39 (2005); *see also* JA122 (deleting

---

struction" of non-responsive data, and a rule requiring "return" of non-responsive data. As set forth in the text, either rule would be unworkable.

data would alter original evidence); GSSA7-8; GSSA11-12; GSSA19-38.

Ganias's suggestion that computer evidence, like paper evidence, can be authenticated simply through a witness with personal knowledge ignores the complex nature of computer evidence, and the increased difficulty that any computer specialist would have in authenticating data without the ability to compare a copy to the original. At the same time, Ganias's argument ignores the benefits to *defendants*—and the criminal justice system, more generally—of the maintenance of electronic evidence in its original form. The government's retention of a forensic image allows a defendant to verify and replicate the government's analysis if he so chooses. *See, e.g.*, *United States v. Kimoto*, 588 F.3d 464, 480 (7th Cir. 2009) (recounting defendant's request for a "forensically sound copy" of digital evidence so that defense team could verify integrity of data); *United States v. O'Keefe,* 461 F.3d 1338, 1341, 1344 (11th Cir. 2006) (discussing opposing testimony from government expert and defense expert at trial on whether a computer virus may have been responsible for uploading and downloading child pornography found on defendant's computer).

Similarly, the ability to authenticate computer data allows the government to refute claims—and the court to resolve claims—of data tampering by the government. And defense claims of

data tampering are not theoretical. *See United States v. Boisvert*, D. Conn. Crim. No. 3:13cv1878 (VLB), Docket Entries 2, 5 (motion under 28 U.S.C. § 2255, including request to examine computer, claiming that government had manipulated evidence of his chat logs with a government agent posing as a young girl); *United States v. Belitsky*, 566 Fed. Appx. 777, 781 (11th Cir. 2014) (rejecting claims of FBI tampering and a virus downloading child pornography). The government's ability to respond to claims of tampering, and the courts' ability to resolve such claims, is preserved by the maintenance of the original evidence as it was collected.

Second, the retention of computer evidence in its original form preserves the integrity and usefulness of computer evidence during a criminal prosecution. This case itself provides an object lesson on this point. In 2009, an IRS computer forensics agent discovered that the 19-DVD set containing a copy of the computer data seized in 2003 had degraded, a not uncommon problem. *See* GSSA31-32. Here, because the government had retained the original forensic images, the agent was able to return to the images for copying and further analysis. GSSA32-34. In short, the retention of forensic images allowed the case to proceed despite the degradation of the temporary storage media.

Similarly, the retention of forensic images preserves the evidentiary value of computer evi-

dence itself. Information on a computer is stored throughout the computer, and given the way data is stored, "responsive" data is often interspersed with non-responsive data. *See* Kerr, Digital World, 119 Harv. L. Rev. at 539-42 (explaining organization of computer hard drives into different clusters); Josh Goldfoot, The Physical Computer and the Fourth Amendment, 16 Berkeley J. Crim. L. 112, 127 (2011); *see also United States v. Triumph Capital Group*, 211 F.R.D. 31, 62 (D. Conn. 2002) (forensic examiner lawfully reviewed active files, deleted files, free space, slack space (unused space), internet cache files, image files, directory structures, and link files); *United States v. Richards*, 659 F.3d 527, 536 (6th Cir. 2011) (describing need to image and examine entire server for deleted files, log records, relevant e-mails, and other information within the scope of warrant).[13] Certain paper

[13] *See also CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 n.2 (11th Cir. 2013) (describing how metadata "can be supplied by applications, users or the file system" and noting that [s]ome metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept"; further explaining that "[m]etadata is generally not reproduced in full form when a document is printed to paper or electronic image") (internal quotations omitted); *see generally* Craig Ball, Computer Forensics for Lawyers

documents provide a rough analogue—think of a ledger with entries that cross-reference other entries, giving context to one-another, *see United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979)—but the way in which data is stored on a computer makes it difficult to separate or delete data without affecting, and reducing the evidentiary value of, vital data that exists in other parts of the computer.

Again, this case provides an example on that point. In November 2004, an IRS computer specialist prepared a "VMware restoration" of the three computers from Taxes International. This restoration allowed the investigative agents to "boot up" and view the forensic image in the way that the computer's owner would have viewed the information at the time of the seizure. SA15; JA251-52. This type of "restoration" of a computer can be crucial to understanding how evidence was viewed on a computer at the time, and is most effective if the entire forensic image, including files, operating systems, and programs, is available. *See* JA258; GSSA26-29; GSSA40-43.

Third, the retention of complete forensic images allows the government to comply with its

---

Who Can't Set a Digital Clock, Georgetown Univ. Law Center Continuing Legal Education E-Discovery Training Academy, 2009 WL 2005124, *6-7, 12-13, 17 (2009).

discovery obligations, including those obligations imposed by the Constitution. If the government were to delete data, or only maintain small portions of computer data that it seized, it could be accused of destroying exculpatory evidence in violation of *Brady v. Maryland*, 373 U.S. 83 (1963). *See, e.g., Kimoto*, 588 F.3d at 480 (defendant argued that emails allegedly missing from electronic materials were "clearly exculpatory" and that the government's failure to produce a forensically sound copy of evidence resulted in *Brady* violation). Courts have recognized the government's "valid" concern about deleting potentially exculpatory data. *See, e.g.*, *In re Search of Information Associated with [Redacted]@Mac.com* ("*In re [Redacted]@Mac.com*"), 13 F. Supp. 3d 157, 167 n.10 (D.D.C. 2014) (also recognizing government's legitimate unease about being able to authenticate computer data if it is forced to delete non-responsive data).

Finally, the retention of forensic images allows the government to conduct reasonable searches of the images—for material responsive to the warrant—as the case evolves. Almost without exception, a computer search occurs in phases over time, depending on lab priorities, the nature of the investigation, and the stage of the investigation or prosecution, including whether a case is proceeding to trial. This type of phased search reflects a reasonable use of government resources; to require a full and compre-

hensive search at the beginning would expend considerable resources, often for little value, and may well be impossible at early stages of an investigation.

The Ninth Circuit's recent decision in *Johnston*, 789 F.3d 934, describes a common and illustrative scenario. There, the government obtained a warrant in September 2006 to search Johnston's computer for child pornography and other materials involving the sexual exploitation of children. *Id.* at 941. The case agent performed an initial scan of the computer on-site and a "bare minimum" forensic scan a few days later in order to confirm that the computer contained child pornography images and videos. *Id.* at 942. It did, leading to Johnston's arrest in September 2007. *Id.* at 938. In 2011, after the defendant declined to accept a plea offer, the government further reviewed the computer data—which had been lawfully retained in evidence—for more evidence relating to child pornography, this time looking beyond image and video files to Internet browsing history and email files contained on the computer. *Id.* at 942. The third, and "most exhaustive" phase of the search began later that year in anticipation of trial, when the agent conducted keyword searches across all the data on the computer, and searched previously unreviewed data on the computer, such as unallocated space on the hard drive, which yielded additional evidence of Johnston's involvement in

producing child pornography. *Id.* The Ninth Circuit affirmed the district court's denial of suppression, finding no issue with the government's search methods. *Id.* at 942. The Court noted that the agent's search methods were "related directly to his mandate," and did not constitute a general rummaging. *Id.* Although the Court did not directly address the government's triaged review of the computer, it found no reason to question the search methods, which reflected a rational allocation of investigative resources based on the government's expanding evidentiary needs at different stages of the case. *Id.*

District courts both within and outside of this circuit have also recognized the government's need to return to the data to collect other responsive documents. *See The Google Case,* 33 F. Supp. 3d at 398 (recognizing that the government "has a need to retain materials as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant"). The court in *The Google Case* explained its decision with the following hypothetical, which is not uncommon: in a drug investigation, one code word for cocaine ("dolls") may be uncovered early in the investigation, while another ("potatoes") may not be learned by investigators until much later. *Id.* As the court noted, the government must retain the ability to search the computer data for the new code word, or valuable evidence of drug trafficking may become unreachable. *See*

also United States v. Lustyik, No. 2:12-CR-645-TC, 2014 WL 1494019, *5, 13-14 (D. Utah Apr. 16, 2014) (upholding search where government's knowledge of criminal activity developed over time and government went back to retained data to conduct targeted searches for additional relevant documents). Thus, the nature of computer evidence supports the government's return to retained computer data to perform additional inquiries—within the scope of the original search warrant—at various stages of the investigation and prosecution.

Ganias and his *amici* point to several decisions by magistrate judges that purport to require the return or destruction of non-responsive electronic data, but they fail to mention that those decisions have largely been overruled by subsequent district court decisions. For instance, Ganias and his *amici* rely heavily on decisions issued by Magistrate Judge Facciola in the District of the District of Columbia, but fail to note that Chief Judge Roberts' opinion in *In re [Redacted]@Mac.com*, 13 F. Supp. 3d 157, effectively overruled those prior rulings.[14] The same is true

[14] *In re Search of Apple iPhone*, 31 F. Supp. 3d 159 (D.D.C. Mar. 26, 2014) (Facciola, M.J.) (denying application to search Apple iPhone through two-step method); *In re Search of Black iPhone 4*, 27 F. Supp. 3d 74 (D.D.C. Mar. 11, 2014) (Facciola, M.J.) (denying application to search through two-step method

in the District of Kansas. *See United States v. Deppish*, 994 F. Supp. 2d 1211, 1221 (D. Kan. 2014) (rejecting analysis of magistrate judge who held that two-step collection and review process for email accounts violated the Fourth Amendment). And *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) is simply inapposite because the court's decision to suppress electronic evidence there was based on the government's failure to begin its review of computer data for fifteen months and its intention to disseminate the full computer images to all defendants prior to searching for responsive documents.[15]

---

and strongly suggesting that any warrant application not requiring destruction of non-responsive data would be denied); *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) (requiring return or destruction of all non-responsive electronic communications collected through two-step search method).

[15] *Doane v. United States*, No. 08 Mag. 0017 (HBP), 2009 WL 1619642, *10, 15 (S.D.N.Y. June 5, 2009), is likewise irrelevant because it involved the seizure of paper documents that were easily segregable by date into items that fell within the scope of the warrant (items from 2002 and later) and items that did not (items that predated 2002).

4. The government's imaging of the computers and retention of the forensic images was reasonable.

Balancing the relevant interests here, the government's conduct was reasonable. The government's legitimate interests in collecting forensic images for off-site review and in retaining computer evidence for the duration of a case, as set forth above, are crucial to the orderly administration of the increasing number of criminal cases that rely on electronic evidence. In addition to facilitating the government's prosecution of wrongdoers, retention of computer evidence aids defendants. As the district court found, the government preserved the computer images for appropriate reasons while the investigation and prosecution were ongoing.[16] SA24.

---

[16] During the suppression hearing, one computer specialist stated that he viewed the computer evidence as "the government's property." *See* JA146; *see also* JA122 (same agent stated "you never know what data you may need in the future"). These were merely inartful ways of expressing the point that the government may maintain evidence through the completion of an investigation, which the agent also explained. *See* JA122 (agent testified that computer evidence maintained because deletion would "alter[] the original data that was seized"); JA137 ("We would never delete any evidence from the original

Ganias's possessory interest is outweighed by these legitimate government purposes. The possessory interest is lessened because of the imaging process, a "less intrusive means" of collecting the computer evidence.[17] SA24. Further, the government was acting under authority of a warrant, making the showing of unreasonableness particularly "laborious." *Soldal*, 506 U.S. at 71.

And finally, as the district court further recognized, Ganias could have voiced his possessory interests through the filing of a Rule 41(g) motion for return of the computer images, at which point the district court could have weighed the government's continued need for the evidence against his possessory interests. The Rule 41(g) remedy is not an empty one, as Ganias argues. If the government has completed its investigation, for example, the court may order return of the computer evidence. Fed. R. Crim. P. 41(g); SA23; *see also In re Smith*, 888 F.2d 167, 168 (D.C. Cir. 1989) (remanding for findings as to whether the government's interests in retaining seized money outweighed the defendant's interest in return

---

state which we obtained it to protect the integrity of the evidence through the life of our investigation.").

[17] This case involves the retention of forensic images. An individual's possessory interests may well vary when the government retains the physical computer, instead of just an image of the computer.

of the funds); *cf. Henderson v. United States*, 135 S. Ct. 1780, 1784 (2015) ("A federal court has equitable authority, even after a criminal proceeding has ended, to order a law enforcement agency to turn over property it has obtained during the case to the rightful owner or his designee.").

The government is not suggesting, as argued by Ganias, that the failure to file a Rule 41(g) motion amounts to the waiver of a right to file a motion to suppress. The government merely notes that Rule 41(g) provides an alternative mechanism for protecting personal rights and that the availability of this mechanism is a fact that can be considered in weighing the reasonableness of the government's continued retention of electronic data. *Cf. United States v. Johns*, 469 U.S. 478, 487 (1985) (considering whether person whose possessory interest affected asked for return of property); *Stabile*, 633 F.3d at 235-36 (same for consent seizure); *Christie*, 717 F.3d at 1163 (same).

In sum, the balance weighs in favor of the government's imaging and retention of computer evidence during the ongoing investigation and prosecution in this case. The government's actions thus comported with the Fourth Amendment. *See Martin*, 157 F.3d at 54.

B. The government's search of the retained forensic images—conducted pursuant to a search warrant—complied with the Fourth Amendment.

1. The government's search of retained forensic images pursuant to a search warrant is reasonable.

Where, as here, the government has reasonably retained forensic images in connection with an ongoing investigation, it will generally also be reasonable for the government to access those images to search for new information when that search is authorized by a properly issued search warrant.[18] As with a seizure, the reasonableness of a search requires a court to assess "the degree to which the search intrudes upon an individual's privacy and the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). The privacy interests of the computer owner are appropriately protected by the government's obtaining of a search warrant from a neutral and detached magistrate, the well-worn

---

[18] Under many circumstances, it may also be reasonable for the government to search or seize nonresponsive data under the plain view or exigent circumstances doctrines. Those doctrines are not at issue in this case.

and principal means of protection against government intrusion.

The existence of probable cause for a search or seizure generally is a strong indicator of reasonableness, "because . . . 'probable cause to believe the law has been broken outbalances private interest in avoiding police contact.'" *United States v. Wilson*, 699 F.3d 235, 242 (2d Cir. 2012) (quoting *Whren v. United States*, 517 U.S. 806, 818 (1996)). And the issuance of a warrant authorizing the intrusion weighs heavily in favor of the reasonableness of the government's conduct. *See United States v. Ross*, 456 U.S. 798, 823 (1982) ("A container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause.").

As the Supreme Court described thirty years ago, an individual's privacy rights become secondary to the general community interest in crime detection when probable cause is established:

> Putting to one side the procedural protections of the warrant requirement, the Fourth Amendment generally protects the 'security' of 'persons, houses, papers, and effects' against official intrusions up to the point where the community's need for evidence surmounts a specified standard, ordinarily 'probable cause.' Beyond this

> point, it is ordinarily justifiable for the community to demand that the individual give up some part of his interest in privacy and security to advance the community's vital interests in law enforcement; such a search is generally 'reasonable' in the Amendment's terms.

Winston v. Lee, 470 U.S. 753, 759 (1985).

Consistent with the Fourth Amendment, the government may obtain a search warrant for nearly any person, place, or thing if the government establishes probable cause for the search and did not engage in an illegal seizure of the item to be searched. Although there are some limits to this principle, *see id.* at 765-66 (finding that invasion of suspect's body under general anesthesia to obtain bullet through surgery was unreasonable when the personal invasion was weighed against the Commonwealth's failure to demonstrate a compelling need for the evidence), a determination by a neutral, detached magistrate judge of probable cause to search is typically enough to overcome the individual's interest in safeguarding his property from government intrusion. *See Georgia v. Randolph*, 547 U.S. 103, 117 (recognizing the "law's general partiality toward" police action taken with a warrant and describing magistrates' determinations as "informed and deliberate") (citing *United States v. Ventresca*, 380 U.S. 102, 107 (1965) and *United States v. Lefkowitz*, 285 U.S. 452, 464 (1932)).

The magistrate judge thus serves as the check on the parade of horribles Ganias portends. *See* Def. Br. at 36. Indeed, it would turn years of Fourth Amendment jurisprudence on its head if the presumption was that the government *cannot* search a particular place despite obtaining a valid warrant to do so, where its conduct leading up to issuance of the warrant was reasonable.

An example from outside the electronic search context demonstrates the reasonableness of this rule. If the police seize a car, pursuant to a warrant, based on evidence suggesting that a suspect murdered a victim in the car, and they find a blood stain matching the victim's DNA on the car's seat, they could reasonably hold the entire car, not just the portion of the seat containing the blood stain, for the same reasons that the government is entitled to retain an entire forensic image of a computer. At some point later, if the police develop evidence that the car's owner was a drug trafficker and concealed cocaine in a hidden trap within the car, it would defy logic and law to suggest that the police could not obtain a subsequent search warrant to search the car for evidence of drug trafficking. In short, the retention of the car for one purpose should not preclude its search for another purpose pursuant to a later-issued warrant.

In this example, there is no improper government conduct; instead, the government acts reasonably at every step. The retention of the ev-

idence is justified by law enforcement's need to preserve it and overcomes the defendant's possessory interest in the property. The defendant's privacy interest in the property is adequately protected by the officer of the court who assesses the government's probable cause and issues a warrant only if the legal standard has been met.

Indeed, just last year, in *Riley v. California*, the Supreme Court reaffirmed the basic principle that a warrant suffices to protect privacy interests in electronically stored data. The Court acknowledged the vast types of personal information—photographs, browsing history, calendars, phone books—a cellular phone could hold, emphasizing that the storage capacity of a phone affords both breadth and depth to the personal records stored therein. 134 S. Ct. at 2489-90. Nonetheless, it went on to conclude that an individual's privacy interests in this vast wealth of personal information did not render a cell phone "immune from search." *Id.* at 2493. Rather, those privacy interests were effectively protected by the warrant requirement, which the Court described as an "'important part of our machinery of government.'" *Id.* (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).

2. Because the government reasonably held the forensic images and obtained a new search warrant, the 2006 search was reasonable.

Here, the government acted reasonably at every turn. Its imaging of the Taxes International Computers in 2003 pursuant to a search warrant authorizing seizure of those computers accommodated both Ganias's need for limited business interruption and the government's need to review the computers off-site. SA9-11; SA24. When the government searched the images, it did so in a targeted manner aimed at identifying documents that fell within the scope of the warrant—not in a manner that would in any way resemble indiscriminate rummaging. JA87-88 (discussing keyword searches); JA213-15 (same); JA244-46 (discussing bookmarking of relevant files); JA295-97 (discussing review of two IPM QuickBooks files); JA314-15; JA340; JA464; SA22; SA25; SA27. Ganias concedes as much. Def.'s Br. at 10-11.

Further, the government reasonably retained the forensic images to serve legitimate government interests. The retained images preserved evidence in an ongoing criminal investigation and allowed the government to use and authenticate its evidence at trial and to fulfill its constitutional discovery obligations. JA137-38; JA158-60; GSSA19-20; GSSA31-32.

Finally, when the need arose to search the retained images for evidence of another crime, the government returned to the same magistrate judge and obtained a new warrant to authorize the second search. JA454-72; *see, e.g. United States v. Abbell*, 963 F. Supp. 1178, 1184, 1201-1202 (S.D. Fla. 1997) (issuance of second warrant to search material, including computer data, that had been seized and held for two years was reasonable). Thus, because the 2006 warrant effectively protected Ganias's privacy interests, the government's conduct was reasonable. Under the totality of the circumstances here, the government complied with the Fourth Amendment.

II. Because the agents acted reasonably in this case, any violation of the Fourth Amendment does not require suppression of the evidence.

A. Governing law

1. The exclusionary rule

Although it is often referred to as an exclusionary "rule," the evidence resulting from a Fourth Amendment violation is not automatically excluded. A defendant has no right to demand suppression of evidence as a remedy for an unconstitutional search. *Herring v. United States*, 555 U.S. 135, 141 (2009) (exclusion "not an individual right"); *Stone v. Powell*, 428 U.S. 465, 486 (1976) (exclusion is neither a "personal constitutional right," nor meant to "redress the injury"); *United States v. Janis*, 428 U.S. 433, 454 n.29 (1976) (suppression "unsupportable as reparation or compensatory dispensation to the injured criminal") (internal quotation marks omitted); *United States v. Julius*, 610 F.3d 60, 66 (2d Cir. 2010) ("[A] search that is found to be violative of the Fourth Amendment does not trigger automatic application of the exclusionary rule.").

Instead, exclusion is appropriate only where it would "result[] in appreciable deterrence" of future Fourth Amendment violations. *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909). While plausible deterrent effect is a "necessary condition for exclusion," it is not "a sufficient

one." *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) (internal quotation marks omitted). Because suppression imposes a "costly toll upon truth-seeking and law enforcement objectives" and "offends basic concepts of the criminal justice system" by "letting guilty . . . defendants go free," a court must also find that "the benefits of deterrence . . . outweigh the costs," which are heavy. *Herring*, 555 U.S. at 141 (internal quotation marks omitted); *Davis*, 131 S. Ct. at 2427; *Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998) (exclusionary rule's costs "present[] a high obstacle for those urging [its] application"); *Julius*, 610 F.3d at 66. Accordingly, while "society must swallow this bitter pill when necessary," the Supreme Court has cautioned that exclusion of evidence should be used "only as a last resort." *Davis*, 131 S. Ct. at 2427 (internal quotation marks omitted).

Whether the benefits of deterrence outweigh the costs of exclusion will "var[y] with the culpability of the law enforcement conduct" in question. *Id.* at 2427 (alteration in original, internal quotation marks omitted). Deterrence is appropriate where the law enforcement action in question constitutes "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Id.* at 2427 (internal quotation marks omitted); *Herring*, 555 U.S. at 144 (same).

2. The good faith exception

On the other hand, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful," or when their conduct involves only simple, isolated negligence, "the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Davis*, 131 S. Ct. at 2427-28 (internal citations and quotation marks omitted).

The Supreme Court originated this "good faith exception" in *Leon*, 468 U.S. at 922, where the Court declined to exclude evidence obtained from searches conducted in "objectively reasonable reliance" on ultimately invalid warrants. Since that time, the Court has applied its exclusionary rule analysis to find that, in a variety of factual circumstances, suppression of unconstitutionally obtained evidence either serves no deterrent purpose or cannot outweigh the attendant "heavy cost." In *Illinois v. Krull*, the Court refused to exclude evidence gathered through searches conducted in reasonable reliance on a later invalidated statute. 480 U.S. 340, 349-50 (1987). *Arizona v. Evans* further applied this logic to permit introduction of evidence from a search conducted in reasonable reliance on erroneous information in a court's arrest warrant database. 514 U.S. 1, 14 (1995). Years later, *Herring* excused an unconstitutional search conducted in good faith reliance on an error in the police's own warrant database. 555 U.S. at 137.

Most recently, in *Davis*, the Court refused to apply the exclusionary rule to evidence gathered via a search conducted in reliance on binding precedent that was later overturned. 131 S. Ct. at 2428-29; *see also United States v. Aguiar*, 737 F.3d 251, 261-62 (2d Cir. 2013) (applying *Davis* to excuse agents' failure to obtain warrant before attaching GPS tracking device to vehicle), *cert. denied*, 135 S. Ct. 400 (2014).

B. Discussion

1. The agents acted in good faith in retaining the computer images under the 2003 warrant.

Pursuant to the 2003 warrant, the government imaged the computers for off-site review and retained the forensic images to serve the legitimate ends of preserving evidence during an active criminal case and providing a means for authenticating that evidence at trial. JA158-60; JA137-38; GSSA19-20; GSSA31-32. As discussed above, these actions were well within the Fourth Amendment's boundaries.

First, the government relied in good faith on the 2003 warrant to obtain the computer images and retain the seized images. *See United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) ("[I]n *Leon*, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within its protection."). The 2003 warrant did not include any restrictions

concerning the time period for review and analysis of the images. *See* JA430-53. Where there were limitations, such as scope restrictions, the agents acted "scrupulously" to "avoid[] viewing files they were not entitled to review." SA25. Absent specific proscriptions in the warrant regarding retention, however, the government acted reasonably. *See* SA24 (district court held that "the government complied in good faith with the warrant issued by the magistrate" in 2003); *cf. United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012) (where officers "knowingly ventured beyond the clear confines of their warrant" to search an apartment not listed in the warrant, they did not rely in good faith on it). The agents here did not knowingly venture beyond the confines of the warrant; rather, they stayed within its explicit terms.

In addition, under *Davis*'s rule, the agents' behavior accorded with then-prevailing appellate case law in both the contexts of paper documents and motions for return of property. *See Beusch*, 596 F.2d at 876-77 (finding ledgers not separable); *Ramsden*, 2 F.3d at 326 (government's retention of property is generally reasonable if the government "has a need for the property in an investigation or prosecution"); *see also Krimstock*, 464 F.3d at 251 (recognizing that retention of seized property even before a criminal proceeding is instituted may be reasonable). The agents also relied—and were entitled to rely—on

the prevailing law in the District of Connecticut. *See Triumph Capital Group*, 211 F.R.D. at 62 (noting that the "seizure of any documents not named in the warrant [for a computer] resulted from a good faith response to the inherent practical difficulties of searching a computer's hard drive for evidence of deleted data and files" and holding that the computer agent acted in good faith).

In any event, even if the authority upon which the agents relied did not constitute "binding precedent," as the Supreme Court envisioned in *Davis*, 131 S. Ct. at 2428, the government has satisfied the ultimate test of good faith underlying *Leon* and its progeny: the law enforcement officers acted "with an objectively 'reasonable good faith belief' that their conduct [was] lawful." *Davis*, 131 S. Ct. at 2427 (quoting *Leon*, 468 U.S. at 909).

In the good faith context, the Supreme Court's decisions have focused on whether the agents' conduct was reasonable and whether the purposes of the exclusionary rule would be served. *See, e.g., Leon*, 468 U.S. at 918 (good faith exception requires only "objectively reasonable belief that . . . conduct did not violate the Fourth Amendment"); *Evans*, 514 U.S. at 13-14 (suppression appropriate "only if the remedial objectives of the rule are thought most efficaciously served"); *Herring*, 555 U.S. at 137 (suppression "turns on the culpability of the police

and the potential of exclusion to deter wrongful police conduct"). And the Supreme Court has never held that the exclusionary rule *only* applies in the limited fact patterns that have arisen in its cases. *See, e.g.*, *Davis*, 131 S. Ct. at 2435 (Sotomayor, J., concurring); *see also id.* at 2439 (Breyer, J., dissenting).

In a recent *en banc* opinion, the Third Circuit held that, even absent binding appellate authority, the good faith analysis requires consideration of "the totality of the circumstances to answer the 'objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal.'" *United States v. Katzin*, 769 F.3d 163, 177 (3d Cir. 2014) (*en banc*) (quoting *Leon*, 468 U.S. at 906-07), *cert. denied*, 135 S. Ct. 1448 (2015). The Third Circuit's decision is consistent with the fact-specific balancing analysis required by the Supreme Court's exclusionary rule jurisprudence, which dictates that every proposed application requires a "rigorous weighing of its costs and deterrence benefits." *Davis*, 131 S. Ct. at 2427; *see also United States v. Bah*, __ F.3d __, Nos. 14-5178, 14-5179, 2015 WL 4503253, *13 (6th Cir. July 24, 2015) (excusing unconstitutional warrantless cell phone search where officers' conduct "suggest[ed] a desire to afford [the defendants] their Fourth Amendment protections").

This Court has also excused agents' conduct when they rely on a validly issued warrant in

the face of an aspect of Fourth Amendment law that is "not yet settled" or "otherwise ambiguous." *Clark*, 638 F.3d at 105 (holding that because the need to support a specific allegation in a warrant application with descriptive facts was not previously established in precedent, the *Leon* good faith rule applied and suppression was inappropriate). *Clark* noted that although strands of prior case law may have suggested the new rule the Court adopted, the Court "could not fault police officers for failing to make these same connections in advance of the courts." *Id.* The Court had previously taken the same approach in *United States v. Buck*, 813 F.2d 588, 592-93 (2d Cir. 1987), where the officers "made considerable efforts to comply with the dictates of the Fourth Amendment" and so could not be chastised for failing to "anticipate" the Court's new holding. In such a case, where the law is unsettled, "a reasonably well-trained police officer could not be expected to know" that the warrant violated the Fourth Amendment, and the exclusionary rule's deterrent purpose would not be served "by penalizing officers who rely upon the objectively reasonable conclusions of an issuing judge." *Id.* at 593.

Thus, to the extent that the law about retaining computer evidence was in any way unsettled, the agents here could not have known that their conduct violated the Fourth Amendment, and they should not be blamed for a lack of presci-

ence of courts' views on the parameters of computer searches. *See Katzin*, 769 F.3d at 176-77; *Clark*, 638 F.3d at 105; *Buck*, 813 F.2d at 593. The agents reasonably worked from an assumption—based on the Federal Rules of Criminal Procedure and case law interpreting them—that it was reasonable to maintain evidence in a criminal proceeding until the conclusion of that proceeding. Moreover, the agents were operating in an uncertain legal and technological environment, applying cases decided in the context of paper file searches in a new context without any perfectly-fitted appellate precedent. The sole case in this jurisdiction that guided agents on the contours of computer searches was a case that supported the agents' actions here. *See Triumph Capital Group*, 211 F.R.D. at 62.

With no directly governing Second Circuit precedent on the constitutionality of searches of imaged computers at the time of the 2003 or 2006 searches, the agents, in consultation with the United States Attorney's Office, relied on their reasonable interpretation of existing Fourth Amendment law to retain the forensic images and to obtain the two warrants at issue here. At the time, no case or statute indicated that their conduct was unconstitutional; indeed, the district judge agreed with the government's Fourth Amendment analysis, lending support to the agents' view that their conduct was lawful. SA18-29.

In sum, the government agents acted reasonably and with an objectively reasonable belief that the retention of the computer images from the 2003 search did not violate the Fourth Amendment.

2. The agents relied in good faith on the 2006 warrant, which was obtained after disclosure of the appropriate facts.

At a minimum, the government's reliance on the 2006 warrant fits squarely within the traditional *Leon* exception for conduct taken in reliance on a search warrant issued by a neutral and detached magistrate judge. The agents presented a warrant application to the magistrate judge and obtained a warrant. Even if this Court were to find that that warrant should not have issued, the agents reasonably relied on the issuance of that warrant to support their search.

Ganias argues that the 2006 warrant cannot "validate" an earlier unconstitutional seizure, relying principally on *United States v. Reilly*, 76 F.3d 1271 (2d Cir. 1996). This argument rests on a misreading of the law and the facts.

Underlying *Leon*'s good faith exception is the notion that the police should not be punished for a magistrate's error when the police reasonably believe that issuance of a warrant is based on a "valid application of the law to the known facts." *Reilly*, 76 F.3d at 1280. As part of the good faith

assessment, the police must not knowingly mislead the magistrate judge by omitting facts that would undermine probable cause. *Id.* If the police do mislead, it becomes the officers themselves who are responsible for the issuance of a defective warrant, rather than the magistrate judge. *Id.* at 1281. *See also United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992) (describing contexts where the good faith exception would not apply, including where the magistrate judge is knowingly misled).

In *Reilly*, this Court found that an officer had not acted in good faith in providing facts to the magistrate that were "almost calculated to mislead." *Id.* at 1280. The police had first visited the defendant's large property in 1990 and allegedly had detected a strong marijuana odor when walking around. *Id.* at 1274. A year later, they returned to the property, passing a number of personal structures (a vegetable garden, patio, and gazebo) before peering into the windows of a cottage and continuing to a wooded area where marijuana plants were growing. *Id.* Later that day, after their foray into the defendant's private property, the officers obtained a warrant and found more marijuana. *Id.*

This Court found that the officers did not act in good faith in securing the warrant because their affidavit did not mention the 1990 visit, failed to describe the layout of the property adequately (including the number of personal struc-

tures passed during their journey), and presented the fruits of the meandering 1991 intrusion as nearly the only probable cause for the search. *Id.* at 1280-81. Under these circumstances, the officers' actions were not "the kind of behavior to which the term good faith [could] be applied." *Id.* at 1281.

This case is a far cry from the facts of *Reilly*. The district court here praised the agents' conduct as "scrupulous[]." SA25. To be akin to *Reilly*, the government here would have had to (a) review, under "authority" of the 2003 warrant, the "Steve_ga.qbw" QuickBooks file and the accounting information it held for Ganias and his clients, (b) discover the incriminating information held therein, and (c) then seek a search warrant to bless its earlier review of the QuickBooks file, all without telling the magistrate that it had already peeked at the file. *See Reilly*, 76 F.3d at 1282. The agents did nothing of the sort here and thus the analogy is inapt.

Instead, the agents here gave the magistrate judge (the same judge who issued the 2003 warrant) the pertinent facts to allow him to evaluate whether there was probable cause to issue the 2006 warrant. The warrant application set out that the images to be searched were seized in November 2003 at Taxes International. JA461; JA463. It further noted that, pursuant to the 2003 search warrant "only files for American Boiler and IPM could be viewed," thereby ex-

plaining the intended scope of the 2003 warrant. JA464. The application demonstrated in full detail how the agent came to know that the "Steve_ga.qbw" file existed and why she believed it would contain evidence of the tax evasion that other records had evinced. JA464-67. Contrary to Ganias's assertion, it was plain from the application that the images had been held by the government between November 2003 and April 2006.

Because the warrant application sufficiently informed the magistrate judge of the facts pertinent to issuance of the 2006 warrant, *Leon*'s general rule that law enforcement agents may rely on a search warrant in conducting a search—even if the warrant is later deemed invalid—applies to the search here.

3. The costs of suppression outweigh its benefits.

Evidence should be suppressed only where the benefits of deterring the government's unlawful conduct appreciably outweigh the costs of suppressing the evidence, a "high obstacle" for those urging application of the exclusionary rule. *Herring*, 555 U.S. at 141. The serious cost of applying the rule is, "of course, letting guilty and possibly dangerous defendants go free—something that offends basic concepts of the criminal justice system." *Id.* (internal quotation marks omitted).

As the district court's factual findings make clear, there was no misconduct here to deter.[19] The agents acted reasonably, plodding "scrupulously" through shifting legal and technological landscapes that remain unresolved today, nearly twelve years after the initial search occurred. SA25. In the absence of guidance from the courts about the acceptable rules of computer searches, the agents did all that they possibly could to respect Ganias's Fourth Amendment rights. The facts here are far from the type of deliberate, reckless, or grossly negligent conduct at which the exclusionary rule's sharp arrow is aimed. *See Davis*, 131 S. Ct. at 2427.

The costs of suppression here, too, are high. *Davis* made clear that there is always a cost to the judicial system and to society at large when reliable, trustworthy evidence is suppressed at the expense of both the truth and justice for a criminal like Ganias. 131 S. Ct. at 2427. These costs are especially salient when the government has invested several years in an investigation that culminates in a lengthy trial, as was the case here. In light of the "serious and nefarious effects of money fraud crimes on society," *Ganias*, 755 F.3d at 142 (Hall, J., concurring and dis-

---

[19] Ganias concedes that the Court need not address whether wholesale suppression of records falling both within and outside the scope of a warrant is an appropriate remedy here. *See* Def. Br. at 54 n.18.

senting), these costs are no less significant when the criminal has committed tax evasion than when he has committed a controlled substance or violent offense. And in the context of tax cases, the costs of suppression—including the cost of "set[ting] the criminal loose in the community without punishment," *Davis*, 131 S. Ct. at 2427, also include the costs associated with reduced general deterrence. *See United States v. Park*, 758 F.3d 193, 201 (2d Cir. 2014) (per curiam) (recognizing that "general deterrence occupies an especially important role in criminal tax offenses, as criminal tax prosecutions are relatively rare").

In sum, the government acted both reasonably and in good faith throughout the course of this lengthy investigation. To hold otherwise would result in a miscarriage of justice.

Conclusion

For the foregoing reasons, the judgment of the district court should be affirmed.

Dated: August 28, 2015

Respectfully submitted,

DEIRDRE M. DALY
UNITED STATES ATTORNEY
DISTRICT OF CONNECTICUT

SANDRA S. GLOVER
SARALA V. NAGALA
ANASTASIA ENOS KING
JONATHAN N. FRANCIS
ASSISTANT U.S. ATTORNEYS

WENDY R. WALDRON
SENIOR COUNSEL
COMPUTER CRIME &
INTELLECTUAL PROPERTY
SECTION
UNITED STATES
DEPARTMENT OF JUSTICE

Federal Rule of Appellate Procedure 32(a)(7)(C) Certification

This is to certify that the foregoing brief complies with the 14,000 word limitation of Fed. R. App. P. 32(a)(7)(B), in that the brief is calculated by the word processing program to contain approximately 13,527 words, exclusive of the Table of Contents, Table of Authorities, Addendum, and this Certification.

SANDRA S. GLOVER
ASSISTANT U.S. ATTORNEY

Addendum

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.