No. _____

In the Supreme Court of the United States

STAVROS M. GANIAS,

Petitioner,

v.

UNITED STATES,

Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Second Circuit

PETITION FOR WRIT OF CERTIORARI

Daniel E. Wenner
John W. Cerreta
Day Pitney LLP
242 Trumbull Street
Hartford, CT 06103-1212
(860) 275-0100
dwenner@daypitney.com
jcerreta@daypitney.com

Stanley A. Twardy, Jr.
Counsel of Record
Day Pitney LLP
One Canterbury Green
201 Broad Street
Stamford, CT 06103-1212
(203) 977-7300
stwardy@daypitney.com

Counsel for Petitioner

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

QUESTION PRESENTED

Does the good-faith exception to the exclusionary rule apply when law-enforcement officials obtain a warrant based on a predicate unconstitutional search or seizure (as the First, Second, Fifth, Sixth, and Eighth Circuits hold), or does the good-faith exception have no application where a search warrant is issued based on a predicate Fourth Amendment violation (as the Ninth Circuit, Tenth Circuit, Eleventh Circuit, and several state high courts hold)?

TABLE OF CONTENTS

QUESTION PRESENTED i

TABLE OF AUTHORITIES v

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 2

JURISDICTION 2

CONSTITUTIONAL PROVISIONS INVOLVED . . 3

STATEMENT 3

1. The Army's seizure of Ganias' personal records 3

2. The government conducts its searches for files within the scope of the warrant 5

3. The IRS begins to investigate Ganias and eventually obtains a second warrant to search Ganias' personal financial records 6

4. The District Court denies Ganias' motion to suppress, and the government uses Ganias' over-seized personal financial records to obtain his conviction 8

5. The Second Circuit reverses the denial of Ganias' suppression motion 8

6. The *en banc* Second Circuit vacates the panel decision and affirms the conviction 9

REASONS FOR GRANTING THE PETITION . . . 12

I. The lower courts are in conflict on the application of the good-faith exception to predicate Fourth Amendment violations 12

A. In addition to the Second Circuit, four other federal courts of appeals apply the good-faith exception to warrants obtained based on predicate Fourth Amendment violations . . . 12

B. Other courts of appeals and several state courts of last resort have refused to extend the good-faith exception to predicate Fourth Amendment violations 14

C. The conflict is widely acknowledged and is ripe for this Court's review 17

II. This case provides a suitable vehicle for resolving the split 19

A. This case does not have vehicle problems of the sort that have prevented review of past petitions 19

B. The fact that the *en banc* majority assumed a Fourth Amendment violation facilitates and simplifies this Court's review 20

CONCLUSION 23

APPENDIX

Appendix A Opinion in the United States Court of Appeals for the Second Circuit (May 27, 2016) . . . . . App. 1

Appendix B Judgment in the United States Court of Appeals for the Second Circuit (May 27, 2016) . . . . . App. 92

Appendix C Opinion in the United States Court of Appeals for the Second Circuit (June 17, 2014) . . . . . App. 94

Appendix D Judgment in a Criminal Case in the United States District Court District of Connecticut (January 18, 2012) . . . . . App. 129

Appendix E Ruling on Motion to Suppress Evidence in the United States District Court District of Connecticut (June 24, 2011) . . . . . App. 138

TABLE OF AUTHORITIES

CASES

Adarand Constructors, Inc. v. Mineta,
534 U.S. 103 (2001) 22

Davis v. United States,
564 U.S. 229 (2011) 1

Herring v. United States,
555 U.S. 135 (2009) 20, 21

Illinois v. Krull,
480 U.S. 340 (1987) 1, 20, 21

Pearson v. Callahan,
555 U.S. 223 (2009) 21

People v. Machupa,
872 P.2d 114 (Cal. 1994) 15

State v. Carter,
630 N.E.2d 355 (Ohio 1994) 15

State v. De Witt,
910 P.2d 9 (Ariz. 1996) 15, 16

State v. Hicks,
146 Ariz. 533 (Ariz. Ct. App. 1985) 1, 16

State v. Johnson,
716 P.2d 1288 (Idaho 1986) 15

United States v. Cannon,
703 F.3d 407 (8th Cir. 2013) 14

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 22

United States v. Diehl,
276 F.3d 32 (1st Cir. 2002) 13

United States v. Jones,
564 U.S. 1036 (2011) 21

United States v. Leon,
468 U.S. 897 (1984) . . . . . *passim*

United States v. Massi,
761 F.3d 512 (5th Cir. 2014) 13

United States v. McClain,
444 F.3d 556 (6th Cir. 2005) 1, 13, 14, 17

United States v. McGough,
412 F.3d 1232 (11th Cir. 2005) 11, 15, 16

United States v. Reilly,
76 F.3d 1271 (2d Cir. 1996) 10, 11, 13, 14

United States v. Scales,
903 F.2d 765 (10th Cir. 1990) . . 11, 15, 16, 17, 19

United States v. Thomas,
757 F.2d 1359 (2d Cir. 1985) 10, 12, 13

United States v. Vasey,
834 F.2d 782 (9th Cir. 1987) 11, 15

United States v. Wanless,
882 F.2d 1459 (9th Cir. 1989) 1, 14, 15

Utah v. Strieff,
136 S. Ct. 2056 (2016) 20

CONSTITUTION AND STATUTES

U.S. Const. amend. IV . . . . . *passim*

28 U.S.C. § 1254(1) 2

OTHER AUTHORITIES

Bradley, *The 'Good Faith Exception' Cases: Reasonable Exercises in Futility*, 60 Ind. L.J. 287 (1985) 16

Cox, Note, *Does It Stay, or Does It Go?: Application of the Good-Faith Exception When the Warrant Relied Upon Is Fruit of the Poisonous T*ree, 72 Wash & Lee L. Rev. 1505 (2015) 2, 18

Halcom, Note, *Illegal Predicate Searches and the Good-Faith Exception*, 2007 U. Ill. L. Rev. 467 (2007) 18

IRS, 2014 Instructions for Schedule C, Profit or Loss from Business 6

Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on Camreta v. Greene and Davis v. United States*, 2010-2011 Cato Supreme Court Review 237 (2011) 22

Lipson, *The Good Faith Exception as Applied to Illegal Predicate Searches: A Free Pass to Institutional Ignorance?*, 60 Hastings L.J. 1147 (2009) 18

Massi v. United States, no. 14-740, Brief in Opposition (April 2015) 18, 19

PETITION FOR A WRIT OF CERTIORARI

The good-faith exception to the Fourth Amendment exclusionary rule rests on the principle that courts should not suppress evidence where doing so would "deter objectively reasonable law enforcement activity." *United States v. Leon*, 468 U.S. 897, 919 (1984). Exclusion of evidence is thus inappropriate where officials violate the Fourth Amendment while acting in "reasonable reliance" on a warrant later held invalid, *see id*. at 922, or on a subsequently invalidated statute, *see Illinois v. Krull*, 480 U.S. 340, 349–50 (1987), or on then-binding judicial precedent, *see Davis v. United States*, 564 U.S. 229, 249–50 (2011).

This case raises an important question concerning the scope of the good-faith exception, on which federal and state appellate courts have long been split: Does the good-faith exception apply to a search warrant obtained based on a predicate Fourth Amendment violation? *See, e.g., United States v. McClain*, 444 F.3d 556, 565 (6th Cir. 2005) (surveying the split). The Second Circuit, sitting *en banc*, held below that "a predicate constitutional violation" does *not* foreclose "good faith reliance on" a later issued warrant. Pet. App. 52. Other courts, by contrast, take the opposing view and hold that nothing in *Leon* permits law-enforcement officials to "launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate." *State v. Hicks*, 146 Ariz. 533, 535 (Ariz. Ct. App. 1985); *see, e.g., United States v. Wanless*, 882 F.2d 1459, 1466 (9th Cir. 1989) ("the good faith exception does not apply where a search warrant is issued on the basis of evidence obtained as the result of an illegal search").

Courts and commentators alike have noted the pressing need for this Court to resolve this entrenched split.[1] And this case provides an excellent vehicle in which to do so. For these reasons, and as explained below, petitioner Stavros Ganias respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Second Circuit in this case.

OPINIONS BELOW

The *en banc* decision of the court of appeals (Pet. App. 1–91) is published at 824 F.3d 199. The court of appeals' vacated panel decision (Pet. App. 94–128) is reported at 755 F.3d 125. The district court's decision denying the motion to suppress (Pet. App. 138–61) is not reported but is available at 2011 WL 2532396.

JURISDICTION

The judgment of the court of appeals was entered on May 27, 2016. Pet. App. 92–93. This Court has jurisdiction under 28 U.S.C. § 1254(1).

---

[1] *E.g.*, Cox, Note, *Does It Stay, or Does It Go?: Application of the Good-Faith Exception When the Warrant Relied Upon Is Fruit of the Poisonous T*ree, 72 Wash & Lee L. Rev. 1505, 1547–48 (2015) ("The issue of whether the good-faith exception saves evidence from exclusion when the warrant relied upon is based on an unconstitutional act has important practical effects," and "it is exceedingly important that the Supreme Court adopt a uniform standard").

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides:

> 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.

STATEMENT

This petition arises from Stavros Ganias' conviction in the District of Connecticut on two counts of evasion of his income taxes. Pet. App. 130. That conviction was the culmination of an IRS inquiry into Ganias' personal finances and tax liability. Pet. App. 99–100. But years before the IRS opened any investigation into Ganias, it was the U.S. Army's Criminal Investigation Command that seized his personal financial records—along with everything else on his computers—while executing a November 2003 warrant for the records of two clients of Ganias' accounting business. Pet. App. 97–98.

1. The Army's seizure of Ganias' personal records.

In August of 2003, Army special agents received a tip indicating that defense contractor Industrial Property Management, Inc. ("IPM") had committed various acts of theft and fraud, including billing the Army for work that IPM actually performed for an affiliated entity, American Boiler. Pet. App. 97.

Evidence of these crimes, the Army's sources stated, could be found at IPM and American Boiler's offices. *Id.* In addition, a source claimed that IPM and American Boiler's financial books were maintained by Mr. Ganias, an accountant doing business as "Taxes International." Pet. App. 4–5. Nothing in the record suggests that Ganias was in any way suspected of wrongdoing in connection IPM and American Boiler's alleged conduct. *Id*.

Based on the evidence that had been developed, Army investigators applied for and obtained three separate warrants to search the offices of IPM, the offices of American Boiler, and the offices of Ganias' accounting business. Pet. App. 140. The warrant for Ganias' accounting business, dated November 17, 2003, authorized seizure of "[a]ll books, records, documents, materials, computer hardware[,] . . . software, and computer associated data relating to the business, financial, and accounting operations of [IPM] and American Boiler." Pet. App. 97.

Two days later, Army officials executed the warrant at Ganias' office. In the affidavit supporting the warrant application, an Army special agent had explained that because identification of relevant data "can take weeks or months," on-site review of "electronic storage devices" for files within the scope of a warrant is often infeasible. Pet. App. 6 & n.4. Anticipating this difficulty, the computer specialists who came to Ganias' office on the day of the warrant's execution "chose to make mirror image" copies of every file on Ganias' three computers. Pet. App. 142.

By completing this mirror imaging, the Army seized vast quantities of information that was not responsive

to the November 2003 warrant. Pet. App. 3, 7–8. The mirror images captured not just the IPM and American Boiler data relevant to the government's investigation, but also Ganias' own personal financial records, records of his other accounting clients, and other personal information and files having nothing to do with the Army's investigation of IPM and American Boiler. Pet. App. 8.

2. The government conducts its searches for files within the scope of the warrant.

Army computer specialists then copied Ganias' data onto DVDs. Pet. App. 143. A delay of more than eight months followed before the Army Criminal Investigation Lab began its review of the electronic files for documents within the scope of the warrant. Pet. App. 98.

Meanwhile, Army investigators working on the case discovered evidence suggesting that an unregistered business had received regular payments from IPM, but failed to report the payments as income. *Id.* In May 2004, the Army decided to invite the Internal Revenue Service ("IRS") to join the investigation. *Id.* It gave the IRS copies of the imaged hard drives so that the IRS could conduct its own review and analysis of the seized electronic files. Pet. App. 98–99 The Army and the IRS then proceeded, in parallel, to search the imaged hard drives for the IPM and American Boiler files covered by the warrant. *Id*.

By December 2004—approximately 13 months after the seizure of every file on Ganias' computers—the Army and IRS investigators working on the case had extracted and isolated the IPM and American Boiler

data that appeared to them to be within the scope of the warrant. Pet. App. 99. At this point, the "investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records." *Id*. Yet notwithstanding this awareness, the investigators made no effort to purge or delete the non-responsive files in their possession that had nothing to do with IPM or American Boiler; instead, the agents decided to retain all of the files on Ganias' computers indefinitely. As one agent explained it: "We viewed the data as the government's property. Not Mr. Ganias' property." 2d Cir. Joint App. 145–46, ECF 151.

3. The IRS begins to investigate Ganias and eventually obtains a second warrant to search Ganias' personal financial records.

Ganias' private files thus remained with the agents working on the case as the investigation into IPM and American Boiler proceeded. Then, in July of 2005—more than 21 months after the over-seizure of Ganias' non-responsive personal files—the IRS' "investigation was expanded to include Ganias" and his personal tax liability. Pet. App. 149.

After reviewing Ganias' bank records and tax returns, IRS agents found a discrepancy between the deposits into Ganias' business accounts and the "gross receipts" reported on his Schedule C. 2d Cir. Joint App. 465–67, ECF 152.[2] The agents suspected that

---

[2] Schedule C is an attachment to Form 1040 used "to report income or loss from a business." IRS, 2014 Instructions for Schedule C, Profit or Loss from Business.

Ganias had underreported his income, but to confirm, they wanted to review Ganias' own personal financial records. *Id.* Fortunately for the government, it still had possession of the preserved mirror image of those personal financial files, as they existed in November 2003.

The lead IRS agent on the case knew that those personal financial records were beyond the scope of the November 2003 warrant, because records pertaining to the finances of "Ganias and Taxes International were not" included in the "items to be seized" listed in the November 2003 warrant. 2d Cir. Joint App. 336, 347–48. The agent therefore asked Ganias and his attorney for Ganias' consent to search the retained images of his personal financial records. Pet. App. 17. When the government did not hear back from Ganias on this request, the agents applied for a warrant to search the preserved images of Ganias' financial records. Pet. App. 17–18. In April of 2006—almost two-and-a-half years after the seizure of Ganias' personal files—the warrant issued, and the government proceeded to review the files. Pet. App. 18–19.[3]

---

[3] At no time, before or after the April 2006 warrant, did the government seek a warrant to search or seize Ganias' actual personal financial records, as they existed in 2006. Nor would such a warrant have yielded the same information as the search of the imaged records. Two days after the execution of the November 2003 warrant, Ganias reviewed his personal financial records and corrected errors in earlier journal entries. Pet. App. 9 & n.8.

4. The District Court denies Ganias' motion to suppress, and the government uses Ganias' over-seized personal financial records to obtain his conviction.

Prior to his trial, Ganias moved to suppress the evidence seized and retained from his computers outside the scope of the November 2003 warrant. The District Court held a suppression hearing, and denied the motion. Pet. App. 138–61. The case proceeded to trial.

At trial, the government used Ganias' personal financial records as key evidence on the government's claim that Ganias had willfully understated his income (by about $35,000 per year) in 2002 and 2003. The jury rendered verdicts of guilty on two counts of tax evasion in March of 2011, and the District Court sentenced Ganias to two years in prison. Pet. App. 130.

5. The Second Circuit reverses the denial of Ganias' suppression motion.

On appeal, the Second Circuit initially reversed the denial of Ganias' suppression motion and remanded the case for a new trial. Pet. App. 94–125. The panel first held—unanimously—that the government "violated Ganias' Fourth Amendment rights" when it seized his non-responsive personal files and retained them for two-and-a-half years, until "finally develop[ing] probable cause to search and seize them." Pet. App. 117–18.

The panel also determined that suppression of this unconstitutionally seized evidence was warranted. The two-and-a-half-year retention of Ganias' private files, even after files responsive to the warrant had been

identified, was not the product of any "objectively reasonable reliance" on precedent or on a warrant. Pet. App. 122–23. In addition, the agents' later efforts to "obtain[] the 2006 search warrant" also did nothing to "cure[]" or excuse the earlier unconstitutional seizure of "wrongfully retained files." Pet. App. 118–19. The panel therefore held that the substantial "benefits of deterr[ing]" the agents' "culpable" conduct outweighed the costs of suppression. Pet. App. 123–24.

Writing separately, Judge Hall agreed with the panel majority that retention of Ganias' "non-responsive documents . . . represent[ed] an unreasonable seizure," but he dissented from the Court's suppression holding. Pet. App. 126. Judge Hall saw no "need for deterrence" of the agents' conduct because they had not violated any clearly "established precedent" then in existence, and "there was little caselaw . . . at the time" of the agents' unlawful seizure suggesting "that the Government could not hold onto non-responsive material" indefinitely. Pet. App. 127.

6. The *en banc* Second Circuit vacates the panel decision and affirms the conviction.

On its own motion, the Second Circuit ordered an *en banc* rehearing of both the panel's Fourth Amendment merits holding and its application of the exclusionary rule. 2d Cir. ECF 102.[4] In deciding the case, however, the *en banc* majority elected to reach only the

[4] The government had petitioned only for panel rehearing, limited only to the exclusionary-rule issue. 2d Cir. ECF 90.

exclusionary-rule issue. Pet. App. 3–4.[5] The majority assumed that federal agents had unconstitutionally seized Ganias's personal financial records, but it nonetheless held that the "agents who . . . engaged in [this] predicate Fourth Amendment violation" could "rely on [the] subsequently issued warrant to establish [a] good faith" exception to the exclusionary rule. Pet. App. 49–53, citing *United States v. Thomas*, 757 F.2d 1359 (2d Cir. 1985), and *United States v. Reilly*, 76 F.3d 1271 (2d Cir. 1996).

Judge Chin dissented. He would have held, as the panel unanimously held, that the government "clearly violated Ganias's rights under the Fourth Amendment." Pet. App. 73. It was patently unconstitutional, in the dissent's view, for federal agents to "overseize[] Ganias's data in November 2003" and then retain non-responsive personal files indefinitely, "until . . . finally develop[ing] a justification to search them again" two-and-a-half years later. *Id*.

The dissent also would have suppressed the unconstitutionally seized evidence. The dissent acknowledged that Second Circuit precedent had, in limited circumstances, extended the good-faith exception to cases where law-enforcement officials "illegally obtain evidence" and "later obtain a warrant" based on the predicate Fourth Amendment violation. Pet. App. 87 & n.10. But as the dissent pointed out,

---

[5] The majority discussed the Fourth Amendment merits in *dictum*, while ultimately "offer[ing] no opinion on the existence of a Fourth Amendment violation." Pet. App. 21; *see also* Pet. App. 58 (Lohier, J., concurring).

this expansion of the good-faith exception had often been "criticized" by "conflicting case law" in other circuits. Pet. App. 87 & n.10, citing, among other cases, *United States v. McGough*, 412 F.3d 1232, 1240 (11th Cir. 2005), *United States v. Scales*, 903 F.2d 765, 768 (10th Cir. 1990), and *United States v. Vasey*, 834 F.2d 782, 789 (9th Cir. 1987). On first principles, the dissent rejected the notion that the good-faith exception transforms warrants into "Band-Aid[s] that the Government may" use to cover its predicate unconstitutional conduct. Pet. App. 86.

Moreover, even accepting the Second Circuit's questionable expansion of the good-faith exception, the dissent disagreed with the majority's application of the governing circuit precedent. Under the Second Circuit's standard, the good-faith exception applies to a warrant obtained based on a predicate Fourth Amendment violation if the agents lay out for the issuing magistrate all of "'the details of their dubious pre-warrant conduct,'" and if the agents do "not have any significant reason to believe" that their prior conduct "was unconstitutional." Pet. App. 87, citing *Reilly*, 76 F.3d at 1281–82. As the dissent saw it, the agents "did *not* present the magistrate judge all the details of their dubious" over-seizure of Ganias' records, and the agents also should have known that mass seizure and retention of Ganias' non-responsive personal files "was unconstitutional." Pet. App. 88.

The Second Circuit subsequently granted Ganias' unopposed motion to "stay . . . the mandate pending the filing and resolution of a petition for a writ of certiorari." 2d Cir. ECF 232. This petition followed.

REASONS FOR GRANTING THE PETITION

I. The lower courts are in conflict on the application of the good-faith exception to predicate Fourth Amendment violations.

The decision below further entrenches a deep split on an important question of constitutional criminal procedure: When law-enforcement officials engage in an unconstitutional search or seizure, does a later warrant obtained based on the predicate Fourth Amendment violation trigger application of the good-faith exception to the exclusionary rule?

A. In addition to the Second Circuit, four other federal courts of appeals apply the good-faith exception to warrants obtained based on predicate Fourth Amendment violations.

A total of five federal courts of appeals—the First, Second, Fifth, Sixth, and Eighth Circuits—have held that the good-faith exception does apply in cases where law-enforcement officials violate a suspect's Fourth Amendment rights, then obtain and execute a warrant based on that predicate violation.

1. The Second Circuit first extended the good-faith exception to unlawful predicate conduct in *United States v. Thomas*, 757 F.2d 1359 (2d Cir. 1985), a tersely worded opinion handed down just a few months after *Leon*. In *Thomas*, law-enforcement officials obtained a warrant based on an unconstitutional dog sniff. But notwithstanding that predicate constitutional violation, the Second Circuit concluded that the good-faith exception applied. For the *Thomas* court, it was enough that the agent had brought his

unconstitutionally obtained "positive 'alert' from the canine to a neutral and detached magistrate," who "determined that the canine sniff could form the basis for probable cause." *Id*. at 1368.

More than a decade later, in *United States v. Reilly*, 76 F.3d 1271 (2d Cir. 1996), the Second Circuit noted that in the intervening years a number of "courts ha[d] criticized *Thomas*." 76 F.3d at 1282–83. The *Reilly* court explained that it was "neither the time nor the place to reconsider" *Thomas*. *Id*. at 1283. But the court added that, in order for the good-faith exception to apply, the officers applying for a subsequent warrant based on a predicate constitutional violation must at least give the magistrate all "the details of [the] dubious pre-warrant conduct," and must show that they had "no significant reason to believe" their conduct was unconstitutional. *Id.* at 1281–82.

In the decision below, the Second Circuit distinguished *Reilly* and expressly reaffirmed the prior circuit precedent in *Thomas*. "[A]gents who have engaged in a predicate Fourth Amendment violation," the court concluded, may continue to rely on "a subsequently issued warrant to establish good faith." Pet. App. 49–51.

2. The decisions of the First, Fifth, Sixth, and Eighth Circuits are to the same effect. *See, e.g., United States v. Diehl*, 276 F.3d 32, 43–44 (1st Cir. 2002) (good-faith exception applied where prior entry into curtilage disclosed in warrant application); *United States v. Massi*, 761 F.3d 512, 528 (5th Cir. 2014) (good-faith exception applies notwithstanding predicate violation); *United States v. McClain*, 444 F.3d 556, 559

(6th Cir. 2005) (same); *United States v. Cannon*, 703 F.3d 407, 413 (8th Cir. 2013) (same).

These decisions generally hold that the good-faith exception applies notwithstanding a predicate Fourth Amendment violation, at least in certain circumstances. In accord with the Second Circuit's approach in *Reilly*, the cases generally require that, in order to reap the benefit of the good-faith exception, law enforcement must "fully disclose[] to a neutral and detached magistrate the circumstances surrounding" the unlawful predicate search or seizure. *McClain*, 444 F.3d at 566. And the cases also demand that law enforcement's "prewarrant conduct must have been close enough to the line of validity to make the officers' belief" in the legality of their behavior "objectively reasonable." *Cannon*, 703 F.3d at 413. If these requirements are met, then a "subsequent search warrant" obtained based on a predicate Fourth Amendment violation can trigger application of the good-faith exception. *See id.*

B. Other courts of appeals and several state courts of last resort have refused to extend the good-faith exception to predicate Fourth Amendment violations.

In conflict with the decisions mentioned above, other courts have held that the good-faith exception does *not* apply when law-enforcement officials obtain a warrant based on a predicate constitutional violation. In particular, the Ninth, Tenth, and Eleventh Circuits all hold that a subsequent warrant predicated on an earlier Fourth Amendment violation provides no basis for recognizing a good-faith exception. *See United States v. Wanless*, 882 F.2d 1459, 1466–67 (9th Cir.

1989); *United States v. Scales*, 903 F.2d 765, 767–68 (10th Cir. 1990); *United States v. McGough*, 412 F.3d 1232, 1239–1240 (11th Cir. 2005).

The decisions of several state courts of last resort are to the same effect. *State v. De Witt*, 910 P.2d 9, 15 (Ariz. 1996); *People v. Machupa*, 872 P.2d 114, 123–24 (Cal. 1994); *State v. Johnson*, 716 P.2d 1288, 1301 (Idaho 1986); *State v. Carter*, 630 N.E.2d 355, 364 (Ohio 1994).

As these courts have explained, the rationale for the good-faith exception simply does not apply in cases involving predicate Fourth Amendment violations. *Leon*'s good-faith exception is expressly based on the understanding that "the exclusionary rule is designed to deter police misconduct," not "to punish the errors of judges and magistrates." *Leon*, 468 U.S. at 916. Cases involving predicate Fourth Amendment violations, however, *do* involve "police misconduct," and do not involve *any* judicial error.

That is because the role of a judge or magistrate who is presented with a warrant application is a limited one. The "magistrate's role when presented with evidence to support a search warrant is to weigh [it] to determine whether it gives rise to probable cause." *United States v. Vasey*, 834 F.2d 782, 789 (9th Cir. 1987). The magistrate is not tasked with deciding the legality of each and every predicate act on which the probable cause showing is based. Indeed, the magistrate is "simply not in a position," in an *ex parte* proceeding, to home in on or "evaluate the legality" of a predicate search or seizure. *Id.*

As such, the issuance of a warrant in these circumstances is not an "endorse[ment] [of] past activity"; it is an "authoriz[ation] [of] future activity." *De Witt*, 910 P.2d at 15 (quoting Bradley, *The 'Good Faith Exception' Cases: Reasonable Exercises in Futility*, 60 Ind. L.J. 287, 302 (1985)). Suppression of evidence remains essential to deter the "officers' unlawful" conduct prior to the issuance of the warrant. *McGough*, 412 F.3d at 1240. And neither *Leon* nor any other of this Court's exclusionary-rule precedents suggests that law enforcement should be permitted to "launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate." *Hicks*, 146 Ariz. at 535.

The Tenth Circuit's decision in *United States v. Scales*, 903 F.2d 765, provides an illustrative example of the decisions on this side of the split. In *Scales*, DEA agents unconstitutionally seized a "suitcase and held it for more than twenty-four hours before obtaining a search warrant." *Id*. at 768. The Tenth Circuit concluded that "the search of the suitcase *after* the search warrant was issued [did not] prevent [the court] from evaluating the agents' behavior *prior* to that time." *Id*. The DEA agents had committed a predicate unconstitutional seizure "when they seized the luggage and held it for more than twenty-four hours," and nothing in *Leon* suggested that the good-faith exception permitted the agents to use a subsequent warrant "to ratify their actions" after the fact. *Id*.

The Second Circuit's decision below takes precisely the opposite position. The *en banc* majority assumed—as the panel unanimously held—that federal agents violated Ganias' Fourth Amendment rights

when they seized and retained his non-responsive personal financial records outside the November 2003 warrant's scope. Pet. App. 3, 48. But the majority nonetheless held that the "agents who . . . engaged in [this] predicate Fourth Amendment violation" *could* invoke a subsequent warrant, issued two-and-a-half years later, to ratify their conduct after the fact. Pet. App. 49–51; c*ontra Scales*, 903 F.2d at 768. The conflict in the lower courts' approach to this issue is direct and entrenched, and only this Court can resolve it.

C. The conflict is widely acknowledged and is ripe for this Court's review.

The conflict presented by this petition is widely recognized, deeply entrenched, and ripe for this Court's review.

For example, courts weighing in on whether to apply the good-faith exception to warrants obtained based on a predicate Fourth Amendment violation have often surveyed and noted the clear circuit conflict. *See, e.g., United States v. McClain*, 444 F.3d 556, 565 (6th Cir. 2005) ("The Ninth and Eleventh Circuits have answered that question in the negative. . . . On the other hand, the Second and Eighth Circuits have held that, at least under some circumstances, the *Leon* good faith exception can still apply when the warrant affidavit relies on evidence obtained in violation of the Fourth Amendment."); *see also* Pet. App. 87 & n.10 (Chin, J., dissenting) (discussing the "conflicting case law"). The split has now been percolating for many years, and it has shown no signs of abating or resolving itself without this Court's intervention.

Commentators, as well, have frequently noted the persistent conflict in the caselaw on this issue. *See, e.g.*, Lipson, *The Good Faith Exception as Applied to Illegal Predicate Searches: A Free Pass to Institutional Ignorance?*, 60 Hastings L.J. 1147, 1156–71 (2009) (surveying split). Some have presented it as a simple two-way split, while others sub-divide the conflicting caselaw into a three-way division between "(1) courts that apply the good faith exception, (2) courts that refuse to apply the good faith exception, and (3) courts that make application of the good faith exception contingent on whether officers informed the magistrate how they obtained the facts contained in the warrant application." Halcom, Note, *Illegal Predicate Searches and the Good-Faith Exception*, 2007 U. Ill. L. Rev. 467, 475–77 (2007) ("Lower court decisions regarding *Leon*'s application to illegal predicate searches fall into three categories."). However the dispute is framed, all appear to agree that "whether the good-faith exception saves evidence from exclusion when the warrant relied upon is based on an unconstitutional act has important practical effects," and "it is exceedingly important that the Supreme Court adopt a uniform standard." Cox, Note, *Does It Stay, or Does It Go?: Application of the Good-Faith Exception When the Warrant Relied Upon Is Fruit of the Poisonous Tree*, 72 Wash & Lee L. Rev. 1505, 1547–48 (2015).

Even the government has, in past submissions to this Court, acknowledged the existing conflict on this issue. *Massi v. United States*, no. 14-740, Brief in Opposition at 13–15 (April 2015) (surveying the split, but arguing that "this disagreement [was] not implicated" in *Massi*). The question whether the good-faith exception applies to warrants obtained based on

predicate Fourth Amendment violations is undoubtedly worthy of this Court's review.

II. This case provides a suitable vehicle for resolving the split.

A. This case does not have vehicle problems of the sort that have prevented review of past petitions.

This case, moreover, provides an excellent vehicle in which to resolve the conflict. As noted, the government has in the past successfully avoided this Court's review based on factual disputes over whether "the evidence used to obtain the search warrant" was in fact "the fruit" of the predicate Fourth Amendment violation. *Massi v. United States*, no. 14-740, Brief in Opposition at 15 (April 2015). This case has no such vehicle problems.

Here, the Second Circuit's analysis proceeded on the assumption that the government unconstitutionally seized certain evidence—Ganias' personal financial records—and then, two-and-half-years later, obtained a warrant to search the *very files* that it had unconstitutionally seized. As such, and unlike in *Massi*, this case does not raise complications regarding the applicability of a "poisonous-tree analysis." Massi Brief in Opposition at 16–17; *compare Scales*, 903 F.2d at 767–68 ("the search of the suitcase after the search warrant was issued does not prevent" suppression based on an earlier unlawful "seiz[ure] [of] the luggage").

Nor does this case raise any complications relating to the distinct exclusionary-rule issues that may arise in cases where "the link between the unconstitutional

conduct and the discovery of the evidence is too attenuated to justify suppression." *See, e.g., Utah v. Strieff*, 136 S. Ct. 2056 (2016). Here, the link is clear and direct: The government unconstitutionally seized and retained Ganias' personal files, kept them for two-and-a-half years outside the scope of the November 2003 warrant, and then obtained a subsequent warrant to search the very evidence that had been unconstitutionally seized. The case thus provides an ideal vehicle in which to decide a question that is undeniably worthy of this Court's review: Whether the good-faith exception applies to warrants obtained based on predicate Fourth Amendment violations.

B. The fact that the *en banc* majority assumed a Fourth Amendment violation facilitates and simplifies this Court's review.

1. That the *en banc* majority assumed—as the panel unanimously held—that the overseizure and retention of Ganias' personal files violated the Fourth Amendment, *see* Pet. App. 3–4, simplifies this Court's review. The Court can and should resolve the question presented just as the Second Circuit did: by assuming a constitutional violation.

Indeed, this Court's cases on the scope of the exclusionary rule regularly adopt this approach. Particularly when addressing the good-faith exception, it has been standard practice for this Court to assume, but not decide, the existence of a constitutional violation. *See Herring v. United States*, 555 U.S. 135, 139 (2009) (deciding the case on the "assumption that there was a Fourth Amendment violation"); *Illinois v. Krull*, 480 U.S. 340, 356 n.13 (1987) ("The question whether the Illinois statute in effect at the time of

McNally's search was, in fact, unconstitutional is not before us."). The Court can take precisely the same approach here. If it ultimately agrees with the Second Circuit's answer to the question presented, then it can simply affirm, as the Court did in *Herring* and *Krull*. If, on the other hand, the Court agrees with Mr. Ganias, then it can remand for a decision on the Fourth Amendment merits.

2. Of course, if the Court deems it preferable to address both the Fourth Amendment merits and the good-faith exception together, it can certainly add the substantive Fourth Amendment issue as an additional question presented.

In recent years, this Court has occasionally added questions presented in Fourth Amendment cases. *E.g.*, *Pearson v. Callahan*, 555 U.S. 223, 227 (2009) ("In granting certiorari, this Court directed the parties to address whether *Saucier* should be overruled in light of widespread criticism directed at it."); *United States v. Jones*, 564 U.S. 1036 (2011) ("In addition to the question presented by the petition, the parties are directed to brief and argue the following question: 'Whether the government violated respondent's Fourth Amendment rights by installing the GPS tracking device on his vehicle without a valid warrant and without his consent."). The Court can do the same here if it deems review of the Fourth Amendment merits desirable.[6]

---

[6] At least one scholar has suggested that, because opportunities to review substantive Fourth Amendment issues may be tapering off, this Court should affirmatively "take a more active role in law development by adding questions presented when it agrees to

There is, moreover, no doubt that the Fourth Amendment merits issue in this case is an exceptionally important question of national significance: namely, whether "the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer." Pet. App. 116. That question has garnered increased attention in recent years, and has now been the subject of *en banc* consideration in both the Second and Ninth Circuits. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171, 1175–76 (9th Cir. 2010) (en banc). In addition, if the Court elects to review the Fourth Amendment merits, it will not lack for careful lower court opinions addressing the issue. *Cf. Adarand Constructors, Inc. v. Mineta*, 534 U.S. 103, 110 (2001) (per curiam) (this Court sits as "a court of final review and not first view"). Quite the contrary, the Court will have the benefit of the panel's unanimous opinion holding that overseizure and indefinite retention of Ganias' personal financial information *did* violate his Fourth Amendment rights.[7]

Either way—whether the Court adds the merits question or follows its standard practice of assuming unconstitutionality—the Court should take this

---

review Fourth Amendment claims." Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on Camreta v. Greene and Davis v. United States*, 2010-2011 Cato Supreme Court Review 237, 259 (2011).

[7] The *en banc* majority also provided some *dictum* on the question while ultimately "offer[ing] no opinion on the existence of a Fourth Amendment violation." Pet. App. 21.

opportunity to grant review of an important exclusionary-rule issue that has long divided the circuits: Whether the good-faith exception applies to warrants obtained based on a predicate Fourth Amendment violation.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Daniel E. Wenner
John W. Cerreta
Day Pitney LLP
242 Trumbull Street
Hartford, CT 06103-1212
(860) 275-0100
dwenner@daypitney.com
jcerreta@daypitney.com

Stanley A. Twardy, Jr.
Counsel of Record
Day Pitney LLP
One Canterbury Green
201 Broad Street
Stamford, CT 06103-1212
(203) 977-7300
stwardy@daypitney.com

Counsel for Petitioner

APPENDIX

APPENDIX

TABLE OF CONTENTS

Appendix A Opinion in the United States Court of Appeals for the Second Circuit (May 27, 2016) . . . . . App. 1

Appendix B Judgment in the United States Court of Appeals for the Second Circuit (May 27, 2016) . . . . . App. 92

Appendix C Opinion in the United States Court of Appeals for the Second Circuit (June 17, 2014) . . . . . App. 94

Appendix D Judgment in a Criminal Case in the United States District Court District of Connecticut (January 18, 2012) . . . . . App. 129

Appendix E Ruling on Motion to Suppress Evidence in the United States District Court District of Connecticut (June 24, 2011) . . . . . App. 138

APPENDIX A

12-240-cr (en banc)
United States v. Ganias

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

No. 12-240-cr

[Filed May 27, 2016]

UNITED STATES OF AMERICA,

Appellee,

-v.-

STAVROS M. GANIAS,

Defendant-Appellant.

August Term 2015

(Argued: September 30, 2015
Decided: May 27, 2016)

Before: KATZMANN, *Chief Circuit Judge*, JACOBS, CABRANES, POOLER, RAGGI, WESLEY, HALL, LIVINGSTON, LYNCH, CHIN, LOHIER, CARNEY, and DRONEY, *Circuit Judges*.

LIVINGSTON and LYNCH, *JJ.*, filed the majority opinion in which KATZMANN, *C.J.*, JACOBS, CABRANES, RAGGI, WESLEY, HALL, CARNEY, and DRONEY, *JJ.*,

joined in full, and POOLER and LOHIER, *JJ*., joined in full as to Parts I and III and in part as to Part II.

LOHIER, *J.*, filed a concurring opinion in which POOLER, *J.*, joined.

CHIN, *J.*, filed a dissenting opinion.

Appeal from the judgment of the United States District Court for the District of Connecticut (Thompson, *J.*), convicting Defendant-Appellant Stavros Ganias of two counts of tax evasion, in violation of 26 U.S.C. § 7201. Ganias argues that the Government retained non-responsive data on mirrored hard drives acquired pursuant to a 2003 search warrant in violation of the Fourth Amendment, and that evidence acquired pursuant to a 2006 search of that data should thus have been suppressed. Because we find that the Government relied in good faith on the 2006 warrant, we need not and do not decide whether the Government violated the Fourth Amendment, and we affirm the judgment of the district court.

AFFIRMED.

SANDRA S. GLOVER (Sarala V. Nagala, Anastasia Enos King, Jonathan N. Francis, Assistant United States Attorneys; Wendy R. Waldron, Senior Counsel, U.S. Dep't of Justice, *on the brief*), *for* Deirdre M. Daly, United States Attorney for the District of Connecticut, *for Appellee United States of America*.

STANLEY A. TWARDY, JR., Day Pitney LLP, Stamford, CT (Daniel E. Wenner, John W. Cerreta, Day Pitney LLP, Hartford, CT,

on the brief), *for Defendant-Appellant Stavros Ganias*.

(Counsel for *amici curiae* are listed in Appendix A.)

DEBRA ANN LIVINGSTON and GERARD E. LYNCH, *Circuit Judges*:

Defendant-Appellant Stavros Ganias appeals from a judgment of the United States District Court for the District of Connecticut (Thompson, *J.*) convicting him, after a jury trial, of two counts of tax evasion in violation of 26 U.S.C. § 7201. He challenges his conviction on the ground that the Government violated his Fourth Amendment rights when, after lawfully copying three of his hard drives for off-site review pursuant to a 2003 search warrant, it retained these full forensic copies (or "mirrors"), which included data both responsive and non-responsive to the 2003 warrant, while its investigation continued, and ultimately searched the non-responsive data pursuant to a second warrant in 2006. Ganias contends that the Government had successfully sorted the data on the mirrors responsive to the 2003 warrant from the non-responsive data by January 2005, and that the retention of the mirrors thereafter (and, by extension, the 2006 search, which would not have been possible but for that retention) violated the Fourth Amendment. He argues that evidence obtained in executing the 2006 search warrant should therefore have been suppressed.

We conclude that the Government relied in good faith on the 2006 warrant, and that this reliance was objectively reasonable. Accordingly, we need not decide whether retention of the forensic mirrors violated the

Fourth Amendment, and we AFFIRM the judgment of the district court.

I

A. Background[1]

In August 2003, agents of the U.S. Army Criminal Investigation Division ("Army CID") received an anonymous tip that Industrial Property Management ("IPM"), a company providing security for and otherwise maintaining a government-owned property in Stratford, Connecticut, pursuant to an Army contract, had engaged in misconduct in connection with that work. In particular, the informant alleged that IPM, owned by James McCarthy, had billed the Army for work that IPM employees had done for one of McCarthy's other businesses, American Boiler, Inc. ("AB"), and for construction work performed for IPM's operations manager at his home residence. The informant told the agents, including Special Agent Michael Conner, that IPM and AB's financial books were maintained by Stavros Ganias, a former Internal Revenue Service ("IRS") agent, who conducted business as Taxes International. On the basis of the informant's information, as well as extensive additional corroboration, Agent Conner prepared an affidavit seeking three warrants to search the offices of IPM, AB, and Taxes International for evidence of criminal

[1] These facts are drawn from the district court decision denying Ganias's motion to suppress and from testimony at the suppression hearing and at Ganias's jury trial. With few exceptions noted herein, the facts in this case are not in dispute.

activity.[2] Nothing in the record suggests that Ganias himself was suspected of any crimes at that time.

In a warrant dated November 17, 2003, U.S. Magistrate Judge William I. Garfinkel authorized the search of Taxes International. The warrant authorized agents to seize, *inter alia*, "[a]ll books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and [AB]." J.A. 433. It further authorized seizure of "[a]ny of the items described [in the warrant] . . . which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including . . . fixed hard disks, or removable hard disk cartridges, software or memory in any form." *Id.* The warrant also specifically authorized a number of digital search protocols, though it did not state that *only* these protocols were permitted.[3] The warrant

---

[2] Specifically, Agent Conner sought evidence relating to violations of 18 U.S.C. § 287 (making false claims) and § 641 (stealing government property).

[3] The warrant specified as follows:

> The search procedure of the electronic data contained in computer operating software or memory devices may include the following techniques:
>
> (a) surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the 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;

authorized seizure of all hardware relevant to the alleged crimes.[4]

> (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.

J.A. 433-34.

[4] In his attached affidavit, Agent Conner offered three reasons why it was necessary for the agents to take entire hard drives off-site for subsequent search rather than search the hard drives on-site: First, he stated that computer searches had to be conducted by computer forensics experts, who "us[ed] . . . investigative techniques" to both "protect the integrity of the evidence . . . [and] detect hidden, disguised, erased, compressed, password protected, or encrypted files." J.A. 448-49. Because of "[t]he vast array" of software and hardware available, it would not always be possible "to know before a search which expert is qualified to analyze the [particular] system and its data." J.A. 450. Thus, the appropriate experts could not be expected, in all cases, to accompany agents to the relevant site to be searched. Second, Agent Conner affirmed that such searches often must occur in "a laboratory or other controlled environment" given the sensitivity of the digital storage media. J.A. 449-50. And third, he stated that "[t]he search process can take weeks or months, depending on the particulars of the hard drive to be searched." J.A. 449. The district court found, in denying Ganias's motion to suppress, that, as a result of technological limitations in 2003 and the complexities of searching digital data, "[a] full [on-site] search would have taken months to complete." *United States v. Ganias*, No. 3:08CR00224 (AWT), 2011 WL 2532396, at *2 (D. Conn. June 24, 2011).

On November 19, 2003, Army CID agents executed the search warrants. Because the warrants authorized the seizure of computer hardware and software, in addition to paper documents, Agent Conner sought the help, in executing the warrants, of agents from the Army CID's Computer Crimes Investigation Unit ("CCIU"), a unit with specialized expertise in digital forensics and imaging. At Ganias's office, the CCIU agents — and in particular Special Agent David Shaver — located three computers. Rather than take the physical hard drives, which would have significantly impaired Ganias's ability to conduct his business, Agent Shaver created mirror images: exact copies of all of the data stored thereon, down to the bit.[5] Ganias was present at his office during the creation of the mirrors, spoke with the agents, and was aware that mirrored copies of his three hard drives had been created and taken off-site.[6] There is no dispute that the forensic

---

[5] Hard drives are storage media comprising numerous bits — units of data that may be expressed as ones or zeros. Mirroring involves using a commercially available digital software (in the present case, though not always, EnCase) to obtain a perfect, forensic replica of the sequence of ones and zeros written onto the original hard drive. During the mirroring, EnCase acquires metadata about the mirroring process, writing an unalterable record of who creates the copy and when the copy is created. It also assigns the mirror a "hash value" — a unique code that can be used to verify whether, upon subsequent examination of the mirror at any later date, even a single one or zero has been altered from the original reproduction.

[6] Testifying at the suppression hearing, Agent Conner explained that the decision to take mirrors, rather than the hard drives themselves, reflected a desire to mitigate the burden on Ganias and his business. *See* J.A. 140-41. The district court credited this

mirrors taken from Ganias's office contained all of the computerized data maintained by Ganias's business, including not only material related to IPM or AB, but also Ganias's own personal financial records, and the records of "many other" accounting clients of Ganias: businesses of various sorts having no connection to the Government's criminal investigation.[7] J.A. 464, ¶ 14.

---

testimony, concluding that the agents "used a means less intrusive to the individual whose possessions were seized than other means they were authorized to use." *Ganias*, 2011 WL 2532396, at *8. The district court, further, explicitly found that the 2003 warrant authorized the Government to take these mirrors, *id.* at *10, a position Ganias has not challenged on appeal, and that runs directly counter to the dissent's seeming suggestions that the Government somehow acted improperly when it mirrored Ganias's hard drives or that this initial seizure went beyond the scope of the 2003 warrant, *see, e.g.*, Dissent at 3 (noting that "although the Government had a warrant for documents relating to only two of defendant-appellant Stavros Ganias's accounting clients, it seized *all* the data from three of his computers"); *id.* at 40 (stating that "the Government . . . entered Ganias's premises with a warrant to seize certain papers and indiscriminately seized — and *retained* — all papers instead").

[7] Ganias claimed before the district court that when he expressed some concern about the scope of the data being seized, an agent assured him that the agents were only looking for files related to AB and IPM, and that irrelevant files "would be purged once they completed their search" for such files. J.A. 428. The district court made no finding to this effect, however. It is undisputed, moreover, that Ganias became aware in February 2006 that the Government retained the mirrors and sought to search them in connection with Ganias's own tax reporting. At no time thereafter did Ganias seek return of the mirrors pursuant to Federal Rule of Criminal Procedure 41(g) or otherwise contact a case agent to seek their return or destruction.

The next day, Agent Shaver consolidated the eleven mirrored hard drives from all three searches (including the three from Ganias's office) onto a single external hard drive which he provided to Agent Conner. Agent Conner, in turn, provided this hard drive to the evidence custodian of the Army CID, who stored it at Fort Devens, Massachusetts. There the consolidated drive remained, unaltered and untouched, throughout the events relevant to this case. Around the same time, Agent Shaver created two additional copies of the mirrored drives on two sets of nineteen DVDs. After providing these DVD sets to Agent Conner, Agent Shaver then purged the external hard drives onto which he had originally written the mirrors. At this point, a week after the search, three complete copies of the mirrors of Ganias's hard drives existed: an untouched copy stowed away in an evidence locker and two copies available for forensic analysis.[8]

Though internal protocols required that specialized digital forensic analysts search the mirrored hard drives, the paper files were not subject to such limitations. Thus, shortly after the November 19 seizure, the Army CID agents began to analyze the non-digital files seized pursuant to the warrant. These files suggested that IPM had made payments to a third

---

[8] These copies were identical digital replicas of Ganias's hard drives as mirrored on November 19, 2003. Notably, the original hard drives in Ganias's computers had already been significantly altered since the Government mirrored them. Ganias explains in his brief before this Court that "[t]wo days after the execution of the November 2003 warrant, [he] reviewed his personal QuickBooks file and . . . . *corrected over 90 errors in earlier journal entries*." Appellant Br. at 15 n.7 (emphasis added).

company whose owner, according to the Connecticut Department of Labor, was a full-time employee of an insurance company who received no wages from any source other than that insurance company. This and other red flags spurred Agent Conner to contact the Criminal Investigation Division of the IRS, which subsequently joined the investigation.

In early February 2004, as he and his fellow agents continued to follow leads from the paper files, Agent Conner sent one of the two DVD sets containing the forensic mirrors to the Army Criminal Investigation Laboratory ("ACIL") in Forest Park, Georgia, accompanied by a copy of one of the three search warrants. In early June, the ACIL assigned Gregory Norman, a digital evidence examiner, to perform a forensic analysis. Around the same time, Special Agent Michelle Chowaniec, who replaced Agent Conner as the primary case agent for the Army CID in late March, provided the second set of DVDs to the IRS agent assigned to the case, Special Agent Paul Holowczyk. Agent Holowczyk in turn, passed it on, by way of intermediaries, to Special Agent Vita Paukstelis, a computer investigative specialist. By the end of June 2004, computer experts for the Army CID and the IRS — Norman and Agent Paukstelis, respectively — had received copies of the digital evidence (which, as the district court found, were "encoded so that only agents with forensic software not directly available to the case agents could view [them]," *Ganias*, 2011 WL 2532396, at *7), and forensic examination began.

Norman commenced his analysis in late June by loading the eleven mirrored drives into EnCase — the same software with which Agent Shaver initially

created the mirrors — so that he could search the data thereon. After looking at the search warrants, he created a number of keywords, with which he searched for potentially relevant data. Initially, the search returned far too many results for practicable review (more than 17,000 hits); thus, Norman requested new keywords from Agent Chowaniec. On the basis of these new keywords, he was able to narrow his search and ultimately identify several files he thought might be of interest to the investigation, all of which he put on a single CD.[9] Some of these files he was able personally to examine, to determine whether they were responsive to the warrant; a few (including the QuickBooks file labeled "Steve_ga.qbw," which was ultimately searched pursuant to the 2006 warrant, J.A. 467) Norman could not open without a specific software edition of QuickBooks to which he did not have immediate access. However, as these files (like the others) contained keywords that were taken from the narrower list and generated on the basis of the warrant, Norman included the QuickBooks files in the CD he ultimately sent to Agent Chowaniec along with a report.[10] On July 23, 2004, Chowaniec received this CD. Norman, in turn, returned the nineteen DVDs to Army CID's evidence custodian in Boston for safekeeping.

---

[9] The rest of the data remained on the DVDs, where agents would not be able to access it without specific forensic software. *See Ganias*, 2011 WL 2532396, at *7.

[10] Norman describes the storage device he sent to Chowaniec as a "DVD," J.A. 218; the district court described it as a "CD," *Ganias*, 2011 WL 2532396, at *4. The distinction is immaterial.

Norman's counterpart in the IRS, Agent Paukstelis — who, in addition to receiving the search warrant with her set of DVDs, also received a list of companies, addresses, and key individuals relating to the investigation, along with "a handwritten notation next to the name 'Taxes International' that stated '(return preparer) do not search,'" *Ganias*, 2011 WL 2532396, at *3 — conducted her analysis over a period of about four months. Because she worked for the IRS, she limited her search to the three mirrored drives from Taxes International. Though Agent Paukstelis used ILook, a different software program, to review the mirrored hard drives, she too could not open QuickBooks files without the relevant proprietary software. Still, though she could not open these files, she believed, based on the information to which she had access, that they were within the scope of the warrant; thus, in October 2004, she copied this data, in concert with other responsive data, onto a CD, three copies of which she sent to Agent Holowczyk and Special Agent Amy Hosney, also with the IRS. In light of the note she had received with her DVD set as well as the list of relevant entities, Agent Paukstelis avoided, to the degree she could, searching any files of Taxes International that did not appear to be directly relevant to that list. On November 30, 2004, Paukstelis also provided a "restoration" of the mirrors of the Taxes International hard drives to Special Agent George Francischelli, an IRS computer specialist assigned to the case.[11]

---

[11] A "restoration" is a software interface that enables a user (potentially a jury) to view data on a mirror as such data would have appeared to a person accessing the data on the original storage device at the time the mirror was created. *Ganias*, 2011 WL 2532396, at *4.

Agents Chowaniec and Conner, after receiving Norman's CD and report in late July, conducted initial reviews of the data. Like Norman and Agent Paukstelis, however, they could not open the QuickBooks files. At the same time, the agents were busy, in the words of Agent Chowaniec, "tracking down other leads[,] . . . [issuing] grand jury subpoenas, . . . doing interviews of subcontractors and identifying subcontractors from the papers that [the agents had] received from the search warrants." J.A. 294-95. In October, Agents Hosney and Chowaniec attempted, together, to review the QuickBooks files, but again lacked the relevant software to do so. Finally, in November 2004, Agent Chowaniec, having acquired the appropriate software, opened two IPM QuickBooks files on her office computer, and then in December, Agents Hosney and Chowaniec, using the restoration provided by Agent Paukstelis, looked at additional IPM QuickBooks files. Though they had the entirety of the mirrored data before them (the only time throughout the investigation that the case agents had direct access to a software interface permitting them to view essentially all of the data stored on the mirrors), they carefully limited their search: Agent Hosney testified that they "only looked at the QuickBooks files for Industrial Property Management and American Boiler . . . [b]ecause those were the only two companies named in the search warrant attachment." J.A. 340. They did, however, observe that other files existed — both on the CD Norman had provided and on the restoration — in particular, the files Agent Hosney ultimately searched in 2006.

Ganias contends that there is no dispute that by this point, the agents had finished "identifying and

segregating the files within the November 2003 warrant's scope." Appellant Reply Br. at 5. In actuality, the record is unclear as to whether the forensic examination of the mirrored computers pursuant to the initial search warrant had indeed concluded as a forward-looking matter, rather than from the perspective of hindsight.[12] The district court did not find any facts decisive to this question. It is, further, undisputed that the investigation into McCarthy, IPM, and AB was ongoing at this time, and that this investigation would culminate in an indictment of McCarthy in 2008 secured in large part through reliance on evidence responsive to the 2003 warrant and located on the mirrored copies of Ganias's hard drives. *See* Indictment, *United States v. McCarthy*, No. 3:08cr224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 1.

---

[12] At the suppression hearing, Agent Chowaniec testified, in response to the question whether "as of mid-December, [her] forensic analysis was completed": "That's correct, of the computers." J.A. 322. But when asked later, "[D]id you know [in December 2004] you wouldn't need to look at any information that had been provided by Greg Norman on that CD anymore in the course of this investigation," Agent Chowaniec responded, "No," and when further asked, "Did you know you wouldn't require further analysis by Greg Norman or any other examiner at the Army lab in Georgia after December of 2004," Agent Chowaniec again responded, "No." J.A. 324. Agent Conner similarly answered with uncertainty when asked a related question. *See* J.A. 145 ("I didn't know the entire universe of information that was contained within the DVDs that were sent to [Norman] for analysis. I knew only what he sent back to me saying this is what I found off your keyword search."). The dissent disputes our conclusion that the record was unclear on this point, arguing, through citation to Agent Chowaniec's testimony, that "the record . . . shows otherwise." Dissent at 19. The district court found no facts on this issue, and the record, as demonstrated above, is indeed unclear.

When asked why, at this time or any time later, Agent Conner did not return or destroy the data stored on the mirrors that did not appear directly to relate to the crimes alleged in the warrant, Agent Conner explained that "[the] investigation was still . . . open" and that, generally, items would be "released back to the owner" once an investigation was closed. J.A. 123. He further noted that the Army CID "would not routinely go into DVDs to delete data, as we're altering the original data that was seized." J.A. 122.[13]

Over the next year, the agents continued to investigate IPM and AB. Analysis of the paper files taken pursuant to the November 2003 search warrant

---

[13] Agent Conner's explanation for why the Government did not, as a matter of policy in this or other cases, delete mirrored drives or otherwise require segregation or deletion of non-responsive data, is not a model of clarity: in addition to citing concerns of evidentiary integrity and suggesting a policy of non-deletion or return prior to the end of an investigation, he noted that "you never know what data you may need in the future," J.A. 122, and at one point referred to the DVDs as "the government's property, not Mr. Ganias'[s] property," J.A. 146. The dissent seizes on this single sentence during Agent Conner's cross-examination as the smoking gun of the Government's bad faith, citing it on no fewer than four occasions. *See* Dissent at 3, 8, 33, 37. The district court, however, did not find facts explicating Agent Conner's testimony or placing it within the context of the explanations that he and other agents offered for retention of the mirrors. The court did note in its legal analysis that "[a] copy of the evidence was preserved in the form in which it was taken." *Ganias*, 2011 WL 2532396, at *8. Further, the Government on appeal provides numerous rationales — many echoing those articulated by Agent Conner *throughout* his testimony — for why retention of a forensic mirror may be necessary during the pendency of an investigation, none of which amounts to the argument that the mirror is simply "government[] property."

revealed potential errors in AB's tax returns that seemed to omit income reflected in checks deposited into IPM's account. Aware that Ganias had prepared these tax returns and deposited the majority of these checks, Agent Hosney came to suspect that Ganias was engaged in tax-related crimes.[14] She did not, however, return to the restoration or otherwise open any of Ganias's digital financial documents or files associated

---

[14] The dissent suggests that "[w]hat began nearly thirteen years ago as an investigation by the Army into two of Ganias's business clients *somehow* evolved into an unrelated investigation by the IRS into Ganias's personal affairs, largely because" the Government retained the mirrored copies of Ganias's hard drives. Dissent at 40 (emphasis added). In fact, Agent Hosney's affidavit in support of the 2006 warrant explains that the Government suspected Ganias of underreporting his income because of evidence that Ganias had assisted McCarthy in underreporting income from *McCarthy's* companies — evidence which led to an indictment of *both* McCarthy and Ganias for conspiracy to commit tax fraud. Further, when Agent Hosney developed this suspicion — which was hardly "unrelated" to the initial investigation — she did not turn to the mirrors, but instead engaged in old-fashioned investigatory work, "examin[ing Ganias's tax returns] more closely to determine if his own income was underreported." J.A. 465, ¶ 18. She then reviewed deposits in his bank account, cross-referenced bank records and tax returns, and finally presented this evidence in a proffer session to Ganias — all without once looking at any non-responsive information on the mirrors. Only after she had acquired independent probable cause — and only after extensive evidence suggested Ganias may have committed a crime — did Agent Hosney seek a second warrant to search the mirrors. It is, in short, no mystery how the investigation of McCarthy, IPM, and AB came to include Ganias, and, further, an inaccurate statement of the record to suggest that this "evolution" had anything to do with the retention of the mirrors.

with Taxes International.[15] Instead, Agent Hosney subpoenaed Ganias's bank records from 1999 to 2003 and accessed his income tax returns for the same period. On July 28, 2005, the IRS — believing Ganias to be involved both personally and as an accomplice or co-conspirator in tax evasion — officially expanded the investigation to include him.

On February 14, 2006, Ganias, accompanied by his lawyer, met in a proffer session with Agent Hosney and others involved in the investigation.[16] That day or shortly thereafter, Agent Hosney asked Ganias for consent to access his personal QuickBooks files and those of his business, Taxes International — data Agent Hosney knew to be present on the forensic mirrors but which she had not accessed. When, by April 24, 2006 (two and a half months later), Ganias had failed to respond (either by consenting, objecting, or filing a motion under Federal Rule of Criminal Procedure 41(g) for return of seized property), Agent

---

[15] Agent Hosney explained in her testimony: "[W]e couldn't look at that file because it wasn't — Steve Ganias and Taxes International were not listed on the original Attachment B, items to be seized." J.A. 348.

[16] According to Agent Hosney, in that proffer session Ganias claimed "that he failed to record income from his own business [to his QuickBook files] as a result of a computer flaw in the QuickBooks software . . . [but that,] . . . although he attempted to duplicate the software error, he was unable to do so." J.A. 467, ¶ 28. Agent Hosney contacted Intuit, Inc., which released QuickBooks, to determine whether such an error might have affected, generally, the pertinent version of the software, and was told that the company was aware of no such "widespread malfunction." J.A. 469, ¶ 35.

Hosney sought a search warrant to search the mirrored drives again.[17] In her search warrant affidavit, Agent Hosney pointed to bank records, income tax forms, and additional evidence to demonstrate that she had probable cause to believe that Ganias had violated 26 U.S.C. § 7201 (by committing tax evasion) and § 7206(1) (by making false declarations).[18] She further noted that the items to be searched were "mirror images of computers seized on November 19, 2003 from the offices of Taxes International," J.A. 461, ¶ 7; that information material to the initial investigation had been located on these mirrors and that, "[d]uring th[at] investigation," such information had been "analyzed in detail," J.A. 464, ¶ 15; that Ganias was not, at the time of the initial seizure, under investigation, J.A. 461, ¶ 3 ("On July 28, 2005, the Government's investigation was expanded to include an examination of whether Ganias, McCarthy's accountant and former IRS Revenue Agent, violated the federal tax laws."); and thus that, though Agent Hosney believed that the second mirrored drive, called TaxInt_2, was "the primary computer for Taxes International," J.A. 463, ¶ 13, she could not search Ganias's personal or business files as "[p]ursuant to the 2003 search warrant, only files for [AB] and IPM could be viewed," J.A. 464, ¶ 14. The magistrate judge issued the

---

[17] U.S. Magistrate Judge William I. Garfinkel, who had authorized the 2003 warrant, authorized this 2006 warrant as well. J.A. 430, 454.

[18] Ganias did not contest before the district court, and does not contest on appeal, that this evidence — none of which was acquired through search of non-responsive data on the mirrors — created sufficient probable cause for the 2006 warrant.

warrant, Agent Hosney searched the referenced data, and ultimately the Government indicted Ganias for tax evasion.

B. Procedural History

In February 2010, Ganias moved to suppress the evidence Agent Hosney acquired pursuant to the 2006 warrant. After a two-day hearing, the district court denied the motion on April 14, 2010, and issued a written decision on June 24, 2011. In that decision, the district court found, *inter alia*, that the forensic examination of the mirrored drives "was conducted within the limitations imposed by the [2003] warrant" and that "[a] copy of the evidence was preserved in the form in which it was taken." *Ganias*, 2011 WL 2532396, at *8. Judge Thompson observed that Ganias "never moved for destruction or return of the data, which could have led to the seized pertinent data being preserved by other means." *Id.* The district court concluded that the Government's retention of the mirrored drives — and thus its subsequent search of those drives pursuant to a warrant — did not violate the Fourth Amendment. Having found no Fourth Amendment violation, the district court did not reach the question of good faith. *Id.* at *9.

At trial, the Government introduced information in Ganias's QuickBooks files as evidence against him, in particular highlighting the fact that payments made to him by clients such as IPM were characterized as "owner's contributions," which prevented QuickBooks

from recognizing them as income.[19] On the basis of this and other evidence, the jury convicted Ganias of two counts of tax evasion, and the district court sentenced him to two terms of 24 months' incarceration, to be served concurrently.

Ganias appealed. On review of his conviction, a panel of this Court concluded, unanimously, that the Government had violated the Fourth Amendment; in a divided decision, the panel then ordered suppression of the evidence obtained in executing the 2006 warrant and vacated the jury verdict. We subsequently ordered this rehearing *en banc* in regards to, first, the existence of a Fourth Amendment violation and, second, the appropriateness of suppression.[20]

---

[19] Many of these entries existed *only* on the QuickBooks files that the Government had accessed on the mirrors, as a result of Ganias's amendments to the entries on his hard drives days after the execution of the 2003 warrant. At trial, Ganias testified that his characterization of the payments as "owner's contributions" was simply a good faith mistake, and not evidence of intent to commit tax evasion, a claim that the Government labeled implausible in light of Ganias's extensive experience as an IRS agent and accountant.

[20] Specifically, we asked the parties to brief the following two issues:

> (1) Whether the Fourth Amendment was violated when, pursuant to a warrant, the government seized and cloned three computer hard drives containing both responsive and non-responsive files, retained the cloned hard drives for some two-and-a-half years, and then searched the non-responsive files pursuant to a subsequently issued warrant; and
>
> (2) Considering all relevant factors, whether the

II

"On appeal from a district court's ruling on a motion to suppress evidence, 'we review legal conclusions de novo and findings of fact for clear error.'" *United States v. Bershchansky*, 788 F.3d 102, 108 (2d Cir. 2015) (quoting *United States v. Freeman*, 735 F.3d 92, 95 (2d Cir. 2013)). We may uphold the validity of a judgment "on any ground that finds support in the record." *Headley v. Tilghman*, 53 F.3d 472, 476 (2d Cir. 1995).

The district court concluded that the conduct of the agents in this case comported fully with the Fourth Amendment, and thus did not reach the question whether they also acted in good faith. Because we conclude that the agents acted in good faith, we need not decide whether a Fourth Amendment violation occurred. We thus affirm the district court on an alternate ground. Nevertheless, though we offer no opinion on the existence of a Fourth Amendment violation in this case, we make some observations bearing on the reasonableness of the agents' actions, both to illustrate the complexity of the questions in this significant Fourth Amendment context and to highlight the importance of careful consideration of the technological contours of digital search and seizure for future cases.

"The touchstone of the Fourth Amendment is reasonableness . . . ." *United States v. Miller*, 430 F.3d

---

> government agents in this case acted reasonably and in good faith such that the files obtained from the cloned hard drives should not be suppressed.

United States v. Ganias, 791 F.3d 290 (2d Cir. 2015) (mem.).

93, 97 (2d Cir. 2005) (alteration omitted) (quoting *United States v. Knights*, 534 U.S. 112, 118 (2001)). As relevant here, "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *United States v. Leon*, 468 U.S. 897, 922 (1984) (alteration omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 267 (1983) (White, J., concurring in judgment)). Nevertheless, both the scope of a seizure permitted by a warrant,[21] and the reasonableness of government

---

[21] Specifically, courts have long recognized that a prohibition on "general warrants" — warrants completely lacking in particularity — was a central impetus for the ratification of the Fourth Amendment. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (noting, in the context of evaluating the reasonableness of a warrantless search of a cell phone, that "[o]ur cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity" and that "opposition to such searches was in fact one of the driving forces behind the Revolution itself"); *Marshall v. Barlow's, Inc*., 436 U.S. 307, 311 (1978) (noting, in the context of evaluating the reasonableness of warrantless inspections of business premises, that "[t]he particular offensiveness" of general warrants "was acutely felt by the merchants and businessmen whose premises and products were inspected" under them); *Stanford v. Texas*, 379 U.S. 476, 486 (1965) ("[T]he Fourth . . . Amendment[] guarantee[s] . . . that no official . . . shall ransack [a person's] home and seize his books and papers under the unbridled authority of a general warrant . . . ."); *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) ("The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of "general warrants."'" (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980))).

We agree with the dissent that "the precedents are absolutely clear that general warrants are unconstitutional." Dissent at 30.

conduct in executing a valid warrant,[22] can present Fourth Amendment issues. Ganias thus argues that the Government violated the Fourth Amendment in this case, notwithstanding the two warrants that issued, by retaining complete forensic copies of his three hard drives during the pendency of its investigation.

According to Ganias, when law enforcement officers execute a warrant for a hard drive or forensic mirror

---

To the degree that the dissent would go further, however, and find it "absolutely clear" to a reasonable government agent in 2005 that the retention of a lawfully acquired mirror during the pendency of an investigation and the subsequent search of data on that mirror pursuant to a second warrant would implicate the ban on general warrants, we respectfully disagree.

[22] *See, e.g.*, *L.A. Cty. v. Rettele*, 550 U.S. 609, 614-16 (2007) (applying the reasonableness standard to evaluate whether police officers' manner of executing a valid warrant violated the Fourth Amendment); *Wilson v. Layne*, 526 U.S. 603, 611 (1999) ("[T]he Fourth Amendment does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion . . . ."); *Dalia v. United States*, 441 U.S. 238, 258 (1979) ("[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness."); *Terebesi v. Torreso*, 764 F.3d 217, 235 (2d Cir. 2014) ("[T]he method used to execute a search warrant . . . [is] as a matter of clearly established constitutional law, subject to Fourth Amendment protections . . . ."), *cert. denied sub nom. Torresso v. Terebesi*, 135 S. Ct. 1842 (2015) (mem.); *Lauro v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) ("[T]he Fourth Amendment's proscription of unreasonable searches and seizures 'not only . . . prevent[s] searches and seizures that would be unreasonable if conducted at all, but also . . . ensure[s] reasonableness in the manner and scope of searches and seizures that are carried out.'" (all but first alteration in original) (quoting *Ayeni v. Mottola*, 35 F.3d 680, 684 (2d Cir. 1994))).

that contains data that, as here, cannot feasibly be sorted into responsive and non-responsive categories on-site, "the Fourth Amendment demands, at the very least, that the officers expeditiously complete their off-site search and then promptly return (or destroy) files outside the warrant's scope."[23] Appellant Br. at 18. Arguing that a culling process took place here and that it had concluded by, at the latest, January 2005, Ganias faults the Government for retaining the

---

[23] On appeal, Ganias does not question the scope or validity of the 2003 warrant. The district court found that the 2003 warrant authorized the Government to mirror Ganias's hard drives for off-site review, *Ganias*, 2011 WL 2532396, at *10; that the warrant, though authorizing such seizure, was sufficiently particularized and not a "general warrant," *id.*; that, absent mirroring for off-site review, on-site review would have taken months, *id.* at *2; and that mirroring thus minimized any intrusion on Ganias's business, *id.* at *8; *cf.* Fed. R. Crim. P. 41(e)(2)(B) (which, as amended in 2009, permits a warrant to "authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," and notes that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant"); Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note to 2009 amendments (explaining that, because "[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location[, t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant"). Ganias does not contest these conclusions on appeal but contends, instead, that considerations *underlying* the prohibition on general warrants may require that, if the government lawfully mirrors an entire hard drive containing non-responsive as well as responsive information for off-site review, it may not then retain the mirror throughout the pendency of its investigation.

mirrored drives — including storing one forensic copy in an evidence locker for safekeeping.[24] It was this retention, he argues, that constituted the Fourth Amendment violation — a violation that, in turn, made the 2006 search of the data itself unconstitutional as, but for this retention, the search could never have occurred.

To support this argument, Ganias relies principally on *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), a Ninth Circuit case involving the search and seizure of physical records. In *Tamura* (unlike the present case, in which a warrant specifically authorized the agents to seize hard drives and to search them off-site) officers armed only with a warrant authorizing them to seize specific "records" instead seized numerous boxes of printouts, file drawers, and cancelled checks for off-site search and sorting. *Id.* at 594-95. After the officers had clearly sorted the responsive paper documents from the non-responsive ones, they refused — despite request — to return the non-responsive paper files. *Id.* at 596-97. The Ninth Circuit concluded that both the unauthorized seizure of voluminous material not specified in the warrant and the retention of the seized documents violated the Fourth Amendment.[25] *Id.* at 595, 597; *see also Andresen*

---

[24] As already noted, the district court made no finding as to when or whether forensic examination of the mirrors pursuant to the 2003 warrant was completed.

[25] The Ninth Circuit declined to reverse the defendant's conviction, as no improperly seized document was admitted at trial, and as blanket suppression was not warranted. *See Tamura*, 694 F.2d at 597.

v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[W]e observe that to the extent [seized] papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others. . . . In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . [R]esponsible officials [conducting such searches], including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."); *cf. United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) ("[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items . . . .").

Because we resolve this case on good faith grounds, we need not decide the relevance, if any, of *Tamura* (or, more broadly, the validity of Ganias's Fourth Amendment claim). We note, however, that there are reasons to doubt whether *Tamura* (to the extent we would indeed follow it) answers the questions before us. First, on its facts, *Tamura* is distinguishable from this case, insofar as the officers there seized for off-site review records that the warrant did not authorize them to seize,[26] and retained those records even after their

---

[26] The fact that the officers in *Tamura* lacked a warrant for the initial seizure was not incidental to the decision: the *Tamura* court explicitly found that it was the lack of a warrant that made the initial seizure — even if otherwise understandable in light of the voluminous material to be reviewed — a violation of the Fourth Amendment. *See* 694 F.2d at 596.

return was requested. Here, in contrast, the warrant authorized the seizure of the hard drives, not merely particular records, and Ganias did not request return or destruction of the mirrors (even after he was indisputably alerted to the Government's continued retention of them) by, for instance, filing a motion for such return pursuant to Federal Rule of Criminal Procedure 41(g). Second, and more broadly, even if the facts of *Tamura* were otherwise on point, Ganias's invocation of *Tamura*'s reasoning rests on an analogy between paper files intermingled in a file cabinet and digital data on a hard drive. Though we do not take any position on the ultimate disposition of the constitutional questions herein, we nevertheless pause to address the appropriateness of this analogy, which is often invoked (including by the dissent) and bears examination.

The central premise of Ganias's reliance on *Tamura* is that the search of a digital storage medium is analogous to the search of a file cabinet. The analogy has some force, particularly as seen from the perspective of the affected computer user. Computer users — or at least, average users (in contrast to, say, digital forensics experts) — typically experience computers as filing cabinets, as that is precisely how user interfaces are designed to be perceived by such users.[27] Given that the file cabinet analogy (at least

---

[27] *See* Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 8-14 (2015) (contrasting "operating systems . . . [which] hide the hardware resources behind abstractions to provide an environment that is more user-friendly," *id.* at 13, with machine language, assembly language, high-level

largely) thus captures an average person's subjective experience with a computer interface, the analogy may shed light on a user's subjective expectations of privacy regarding data maintained on a digital storage device. Because we experience digital files as discrete items, and because we navigate through a computer as through a virtual storage space, we may expect the law similarly to treat data on a storage device as comprised of distinct, severable files, even if, in fact, "[s]torage media do not naturally divide into parts." Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112, 131 (2011). In this case, for example, a person in Ganias's situation could well understand the "files" on his hard drives containing information relating to IPM and AB as separate from the "files" containing his personal financial information and that of other clients. Indeed, the very fact that the Government sought additional search authorization via the 2006 warrant when it established probable cause to search Ganias's personal files indicates that the Government too understood — and credited — this distinction.

---

languages, data structures, and algorithms); Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112, 117 (2011) (contrasting two perspectives on digital storage media — the "internal perspective," or how "the user experiences [such media,] as parcels of information, grouped into files, or even into smaller units such as spreadsheet rows" and the "external perspective," or how the actual computer functions, in which "files are not . . . 'things' at all," but "groupings of data . . . inseparably tied to the storage medium," created by the computer by manipulating "chunks of physical matter [such as regions on a hard drive] whose state is altered to record information").

That said, though it may have some relevance to our inquiry, the file cabinet analogy is only that — an analogy, and an imperfect one. *Cf.* James Boyle, *The Public Domain* 107 (2008) ("Analogies are only bad when they ignore the key difference between the two things being analyzed."). Though to a user a hard drive may seem like a file cabinet, a digital forensics expert reasonably perceives the hard drive simply as a coherent physical storage medium for digital data — data that is interspersed *throughout* the medium, which itself must be maintained and accessed with care, lest this data be altered or destroyed.[28] *See*

---

[28] *See* Eoghan Casey, *Digital Evidence and Computer Crime* 472, 474-96 (3d ed. 2011) (highlighting the fact that forensic examination of storage media can create tiny alterations, which necessitates care on the part of examiners in acquiring, searching, and preserving that data); *id.* at 477-78 (describing the importance of protecting digital storage media from "dirt, fluids, humidity, impact, excessive heat and cold, strong magnetic fields, and static electricity"); Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 95 (2014) ("Computer data is extremely volatile and easily deleted, and can be destroyed, either intentionally or accidentally, with a few mouse clicks."); Bill Nelson et al., *Guide to Computer Forensics and Investigations* 160 (5th ed. 2015) (emphasizing the importance of "maintain[ing] the integrity of digital evidence in the lab" by creating a read-only copy prior to analysis); Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 Jurimetrics J. 147, 153 (2010) ("[All electronically stored information is] prone to manipulation[;] . . . [such] alteration can occur intentionally or inadvertently."); Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* 17 (2012) [hereinafter ISO/IEC, *Guidelines*] (emphasizing the importance of careful storage and transport techniques and

Goldfoot, *supra*, at 114 (arguing digital storage media are physical objects like "drugs, blood, or clothing"); Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. Pitt. J. Tech. L. & Pol'y, art. 5, at 1, 30 (2007) ("[A] computer does not simply hold data, it is *composed* of data."). Even the most conventional "files" — word documents and spreadsheets such as those the Government searched in this case — are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact "fragmented" on a storage device, potentially across physical locations. Jekot, *supra*, at 13. "Because of the manner in which data is written to the hard drive, rarely will one file be stored intact in one place on a hard drive," *id*.; so-called "files" are stored in multiple locations and in multiple forms, *see* Goldfoot, *supra*, at 127-28.[29] And as a corollary to this fragmentation, the computer stores unseen information about any given "file" — not only metadata about when the file was created or who created it, *see* Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 94-95 (2014),

---

noting that "[s]poliation can result from magnetic degradation, electrical degradation, heat, high or low humidity exposure, as well as shock and vibration").

[29] *See* Goldfoot, *supra* ("Storage media do not naturally divide into parts," *id.* at 131; "it is difficult to agree . . . on where the subcontainers begin and end," *id.* at 113.); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 557 (2005) ("[V]irtual files are not robust concepts. Files are contingent creations assembled by operating systems and software."); *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 32 (2015) ("What does it mean to 'delete' data?").

but also prior versions or edits that may still exist "in the document or associated temporary files on [the] disk" — further interspersing the data corresponding to that "file" across the physical storage medium, Eoghan Casey, *Digital Evidence and Computer Crime* 507 (3d ed. 2011).

"Files," in short, are not as discrete as they may appear to a user. Their interspersion throughout a digital storage medium, moreover, may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data. To be clear, we do not suggest that it is impossible to do so in any particular or in every case; we emphasize only that in assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular case — features that simply do not exist in the context of paper files.

These features include an additional complication affecting the validity of the file cabinet analogy: namely, that a good deal of the information that a forensic examiner may seek on a digital storage device (again, because it is a coherent and complex forensic object and not a file cabinet) does not even remotely fit into the typical user's conception of a "file." *See* Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 39 (2015) ("Forensic software gives a forensic examiner access to electronically stored information (ESI) that is otherwise unavailable to a typical computer user.").

Forensic investigators may, *inter alia*, search for and discover evidence that a file was deleted as well as evidence sufficient to reconstruct a deleted file — evidence that can exist in so-called "unallocated" space on a hard drive. *See* Casey, *supra*, at 496; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542, 545 (2005); Fed. Judicial Ctr., *supra*, at 40 ("A host of information can lie in the interstices between the allocated spaces."). They may seek responsive metadata about a user's activities, or the manner in which information has been stored, to show such things as knowledge or intent, or to create timelines as to when information was created or accessed.[30] Forensic examiners will sometimes seek evidence on a storage medium that something *did not happen*: "If a defendant claims he is innocent because a computer virus committed the crime, the absence of a virus on his hard drive is 'dog that did not bark' negative evidence that disproves his story. . . . To prove something is not on a hard drive, it is necessary to look at every place on the drive where it might be found and confirm it is not there."[31] Goldfoot, *supra*, at 141; *see*

---

[30] *See Fharmacy Records v. Nassar*, 379 F. App'x 522, 525 (6th Cir. 2010) (describing testimony of a digital forensics expert in a copyright case that the number and physical location of a file on an Apple Macintosh — which saves files sequentially on its storage medium — demonstrated that the file had been back-dated).

[31] Indeed, in this very case, as already noted, *see supra* note 16, Ganias at one point claimed that a "software error" or "computer flaw" prevented him from recording certain income in his QuickBooks files. J.A. 467, ¶ 28. Data confirming the existence, or non-existence, of an error affecting the particular installation of a program on a given digital storage device could be, in a

also United States v. O'Keefe, 461 F.3d 1338, 1341 (11th Cir. 2006) ("[The government's expert] testified that the two viruses he found on [the defendant's] computer were not capable of 'downloading and uploading child pornography and sending out advertisements.'").[32]

---

hypothetical case, relevant to the probity of information otherwise located thereupon.

[32] We note that some of these inferences may be limited to — or at least of more relevance to — traditional magnetic disk drives, which have long been the primary digital storage technology. "Generally when data is deleted from a [traditional hard disk drive], the data is retained until new data is written onto the same location. If no new data is written over the deleted data, then the forensic investigator can recover the deleted data, albeit in fragments." Alastair Nisbet et al., *A Forensic Analysis and Comparison of Solid State Drive Data Retention with TRIM Enabled File Systems*, Proceedings of the 11th Australian Digital Forensics Conference 103 (2013). In contrast, the technology used in solid state drives "requires a cell to be completely erased or zeroed-out before a further write can be committed," *id.* at 104, and in part because such erasure can be time consuming, solid state drives incorporate protocols which "zero-delete data locations . . . as a matter of course," thereby "reduc[ing] the data that can be retrieved from the drive by [a] forensic investigator," *id.* at 103. *See also* Graeme B. Bell & Richard Boddington, *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?*, 5 J. Digital Forensics, Sec. & L., no. 3, 2010, at 1, 12 (stating that, in connection with such storage devices, "evidence indicating 'no data' does not authoritatively prove that data did not exist at the time of capture"). That is not to say that studies indicate that deleted information is *never* recoverable from any model of solid state drive. *See, e.g.*, Christopher King & Timothy Vidas, *Empirical Analysis of Solid State Disk Data Retention When Used with Contemporary Operating Systems*, 8 Digital Investigation 111, 113 (2011) (citing a study suggesting that data deleted from a particular solid state drive was recoverable in certain contexts); Gabriele Bonetti et al., *A Comprehensive Black-*

Finally, because of the complexity of the data thereon and the manner in which it is stored, the nature of digital storage presents potential challenges to parties seeking to preserve digital evidence, authenticate it at trial, and establish its integrity for a fact-finder — challenges that materially differ from those in the paper file context. First, the extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium. Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial. Graves, *supra*, at 95-96 ("[The investigator] must be able to prove that the information presented came from where he or she claims and was not altered in any way during examination, and that there was no opportunity for it to have been replaced or altered in the interim."); *see also* Casey, *supra*, at 480 ("Even after copying data from a computer or piece of storage media, digital investigators generally retain the original evidential item in a secure location for future reference.").[33] The

---

Box Methodology for Testing the Forensic Characteristics of Solid-State Drives, Proceedings of the 29th Annual Computer Security Applications Conference 277 (2013) (observing that, though several tested solid state drives contained no recoverable deleted data, one model contained "high[ly] recoverab[le]" quantities of such data). The point is simply that there may be material differences among different varieties of storage media that, in turn, make certain factors cited herein more or less relevant to a given inquiry.

[33] We do not suggest that authentication of evidence from computerized records is impossible absent retention of an entire hard drive or mirror. Authentication is governed by Federal Rule

preservation of data, moreover, is not simply a concern for law enforcement. Retention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved. *See, e.g.*, *United States v. Kimoto*, 588 F.3d 464, 480 (7th Cir. 2009) (quoting the defendant's motion as stating: "Upon beginning their work, [digital analysis experts] advised [the defendant's] Counsel that the discovery provided to the defense did not appear to be a complete forensic copy, and that such was necessary to verify the data as accurate and unaltered.").[34] Defendants may

---

of Evidence 901, which requires only that "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). As we have stated, "[t]his requirement is satisfied 'if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.'" *United States v. Pluta*, 176 F.3d 43, 49 (2d Cir. 1999) (citation omitted) (quoting *United States v. Ruggiero*, 928 F.2d 1289, 1303 (2d Cir. 1991)). "[T]he burden of authentication does not require the proponent of the evidence to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood." *Id.* (alteration omitted) (quoting *United States. v. Holmquist*, 36 F.3d 154, 168 (1st Cir. 1994)). The weight of digital evidence admitted at trial, however, may be undermined by challenges to its integrity — challenges which proper preservation might have otherwise avoided.

[34] Where, as in this case, a mirror containing responsive data has been lawfully seized from a third-party custodian, this concern cannot be avoided simply by returning the original medium to the

also require access to a forensic copy to conduct an independent analysis of precisely what the government's forensic expert did — potentially altering evidence in a manner material to the case — or to locate exculpatory evidence that the government missed.[35]

Notwithstanding any other distinctions between this case and *Tamura*, then, the Government plausibly argues that, because digital storage media constitute coherent forensic objects with contours more complex than — and materially distinct from — file cabinets

---

party from whom it was seized. A third-party custodian may need to utilize a hard drive in ways that will alter the data, and will likely have no incentive to retain a mirrored copy of drives as they once existed but that are of no further use to the custodian.

[35] *See Kimoto*, 588 F.3d at 480-81 ("[The defendant] argued that the failure to provide him with a complete forensic copy of all digital files impaired his ability to prepare a defense. . . . [The defendant] submitted that he should not be punished 'because the Government failed to properly preserve or maintain a digital forensic copy of the data.'"); Casey, *supra*, at 510-11 (discussing a case study in which, due to forensic investigators' own mistakes, discovery of digital evidence confirming a murder suspect's alibi was greatly delayed); *see also id.* at 508-510 (detailing the importance of experts reporting their processes); Fed. Judicial Ctr., *supra*, at 41 ("The forensic examiner . . . generate[s] reports, detailing the protocols and processes that he or she followed . . . . The forensic reports must provide enough data to allow an independent third-party examiner to recreate the exact environment that yielded the report's findings and observations."); Darren R. Hayes, *A Practical Guide to Computer Forensics Investigations* 116 (2015) ("[B]ecause forensics is a science, the process by which the evidence was acquired must be repeatable, with the same results."); ISO/IEC, *Guidelines*, *supra*, at 7 (emphasizing the importance of repeatability and reproducibility).

containing interspersed paper documents, a digital storage medium or its forensic copy may need to be retained, during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained. To be clear, we do not decide the ultimate merit of this argument as applied to the circumstances of this case.[36]

---

[36] That said, it is important to correct a misunderstanding in the dissent's analysis, as it pertains to these factors and their application here. The dissent suggests that the Government can have had no interest in retention, as "[t]he agents could not have been keeping non-responsive files [in order to authenticate and defend the probity of responsive files] for the purpose of proceeding against Ganias, as [in December 2004] they did not yet suspect [him] of criminal wrongdoing." Dissent at 22. This argument misunderstands the Government's position: the Government was not retaining the mirrors in late 2004 and 2005 in the hopes of proceeding against Ganias; it was retaining the mirrors as part of its ongoing investigation of James McCarthy and his two companies, AB and IPM — an investigation that would culminate in an indictment of McCarthy in 2008 secured through extensive reliance on responsive data recovered from the mirrored copies of Ganias's hard drives. The dissent's focus on Ganias, the owner of the hard drives the Government mirrored, and not McCarthy, a third-party defendant, thus permits the dissent to dismiss out-of-hand Government interests that, properly viewed, are significant — whether or not ultimately dispositive. *See* Dissent at 24 ("As a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image."); *id.* at 25-26 (dismissing the Government's *Brady* concern by noting that "[t]he Government is essentially arguing that it must hold on to the materials so that it can give them back to the defendant," a

Nor do we gainsay the privacy concerns implicated when the government retains a hard drive or forensic mirror containing personal information irrelevant to the ongoing investigation, even if such information is never viewed. We discuss the aptness and limitations of Ganias's analogy and the Government's response simply to highlight the complexity of the relevant questions for future cases and to underscore the importance, in answering such questions, of engaging with the technological specifics.[37]

---

concern that the dissent argues "can be obviated simply by returning the non-responsive files to the defendant in the first place"). Perhaps in some situations, in which the owner of computerized data seized pursuant to a search warrant is the expected defendant in a criminal proceeding, problems of authentication or probity could be handled by stipulations, and *Brady* issues might be mooted by the return of the data to the defendant — though we express no view on those questions. As this case illustrates, however, when the owner of hard drives mirrored by the government is a third party who is not the expected target of the investigation, the government's interests in retention take on an additional layer of complexity. A stipulation with Ganias about the authenticity or probity of data extracted from his computers would not have affected the ability of the original targets of the investigation to raise challenges to authenticity or probity. Nor would returning the mirrors to Ganias — who at that point, absent a stipulation to the contrary, could presumably have destroyed or altered them, intentionally or accidentally — have protected the interests of those anticipated defendants in conducting their own forensic examination of the data in search of exculpatory evidence or to replicate and criticize the Government's inspection procedures.

[37] Of course, engaging with the specifics requires acknowledging and emphasizing that technologies rapidly evolve, and that the specifics change. *See* John Sammons, *The Basics of Digital Forensics* 170 (2012) (commenting that digital forensics faces the

In emphasizing such specifics, we reiterate that we do not mean to thereby minimize or ignore the privacy

---

"blinding speed of technology [and] new game-changing technologies such as cloud computing and solid state hard drives . . . just to name a few"). In discussing the technological specifics of computer hard drives, we have primarily addressed a particular form of electronic storage that has become conventional. *See supra* note 32. Newer forms of emerging storage technology, or future developments, may work differently and thus present different challenges. *See, e.g.*, Bell & Boddington, *supra*, at 3, 6, 14 (observing that "the peculiarity of 'deleted, but not forgotten' data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology" and that increasingly popular solid state drives can "modify themselves very substantially without receiving instructions to do so from a computer," and thus predicting that "recovery of deleted files and old metadata will become extremely difficult, if not impossible" as solid state storage devices utilizing a particular deletion protocol called "TRIM" become more prevalent); King & Vidas, *supra*, at 111 ("We show that on a TRIM-enabled [solid state drive], using an Operating System (OS) that supports TRIM, . . . in most cases no data can be recovered."); *id.* at 113 ("[M]ost [solid state drive] manufacturers have a TRIM-enabled drive model currently on the market."). *But see* Bonetti et al., *supra*, at 270-71, 278 (making clear that solid state drives, which differ considerably among models and vendors, may yield differing levels of deleted-file recoverability, depending upon their utilization of TRIM and other deletion protocols, erasing patterns, compression, and wear leveling protocols). Solid state drives, of course, are just one example. *Cf.* Bell & Boddington, *supra*, at 3 ("It is . . . in the nature of computing that we perceive regular paradigm shifts in the ways that we store and process information."). The important point is that considerations discussed in this opinion may well become obsolete at some future point, the challenges facing forensic examiners and affected parties may change, and courts dealing with these problems will need to become conversant with the particular forms of technology involved in a given case and the evidentiary challenges presented by those forms.

concerns implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant. The seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. Indeed, another weakness of the file cabinet analogy is that no file cabinet has the capacity to contain as much information as the typical computer hard drive. In 2005, Professor Orin Kerr noted that the typical personal computer hard drive had a storage capacity of about eighty gigabytes, which he estimated could hold text files equivalent to the "information contained in the books on one floor of a typical academic library." Kerr, *Searches and Seizures in a Digital World*, *supra*, at 542. By 2011, computers were being sold with one terabyte of capacity — about twelve times the size of Professor Kerr's library floor. Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1, 6 (2011). The *New York Times* recently reported that commercially available storage devices can hold "16 petabytes of data, roughly equal to 16 billion thick books." Quentin Hardy, *As a Data Deluge Grows, Companies Rethink Storage*, N.Y. Times, Mar. 15, 2016, at B3.

Moreover, quantitative measures fail to capture the significance of the data kept by many individuals on their computers. Tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, banking and shopping information — all may be kept in the same device, interspersed among the evidentiary material

that justifies the seizure or search. *Cf. Riley v. California*, 134 S. Ct. 2473, 2489-90 (2014) (explaining that even microcomputers, such as cellphones, have "immense storage capacity" that may contain "every piece of mail [people] have received for the past several months, every picture they have taken, or every book or article they have read," which can allow the "sum of an individual's private life [to] be reconstructed"); *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."). While physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material, the reasonableness of seizure and subsequent retention by the government of such vast quantities of irrelevant private material was rarely if ever presented in cases prior to the age of digital storage, and has never before been considered justified, or even practicable, in such cases. Even as we recognize that search and seizure of digital media is, in some ways, distinct from what has come before, we must remain mindful of the privacy interests that necessarily inform our analysis.[38]

---

[38] The dissent extensively addresses these privacy interests. As this opinion makes clear, we do not disagree with the proposition that the seizure and retention of computer hard drives or mirrored copies of those drives implicate such concerns and raise significant Fourth Amendment questions. We do not agree, however, for reasons we have also discussed at length, with the dissent's dismissal of the countervailing government concerns. However these issues are ultimately resolved, we believe that the Government's arguments are, at a minimum, sufficiently forceful

We note, however, that parties with an interest in retained storage media are not without recourse. As noted above, Ganias never sought the return of any seized material, either by negotiating with the Government or by motion to the court. Though negotiated stipulations regarding the admissibility or integrity of evidence may not always suffice to satisfy reasonable interests of the government in retention during the pendency of an investigation,[39] such stipulations may make return feasible in a proper case, and can be explored.

A person from whom property is seized by law enforcement may move for its return under Federal Rule of Criminal Procedure 41(g).[40] Rule 41(g) permits

---

that it is unwise to try to reach definitive conclusions about the constitutional issues in a case that can be decided on other grounds.

[39] For instance, as we have previously noted, where, as here, the owner of the records is not (at least at the time of the seizure) the target of the investigation, a stipulation from that party may not serve the government's need to establish the authenticity or integrity of evidence it may seek to use, and access to the records by that party will not necessarily satisfy the need of potential future defendants to test the processes used by the government to extract or accurately characterize data culled from a hard drive. In some cases, however, negotiated solutions may be practicable.

[40] Rule 41(g) provides as follows:

> **Motion to Return Property.** A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it

a defendant or any "person aggrieved" by either an unlawful or *lawful* deprivation of property, *see United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc) (per curiam), to move for its return, Fed. R. Crim. P. 41(g). Evaluating such a motion, a district court "must receive evidence on any factual issue necessary to decide the motion," and, in the event that the motion is granted, may "impose reasonable conditions to protect access to the property and its use in later proceedings." *Id.* Since we resolve this case on other grounds, we need not address whether Ganias's failure to make such a motion forfeited any Fourth Amendment objection he might otherwise have had to the Government's retention of the mirrors. But we agree with the district court that, as a pragmatic matter, such a motion "would have given a court the opportunity to consider 'whether the government's interest could be served by an alternative to retaining the property,' and perhaps to order the [mirrors] returned to Ganias, all while enabling the court to 'impose reasonable conditions to protect access to the property and its use in later proceedings.'" *Ganias*, 2011 WL 2532396, at *8 (citation omitted) (first quoting *In re Smith*, 888 F.2d 167, 168 (D.C. Cir. 1989) (per curiam); then quoting Fed. R. Crim. P. 41(g)).

Rule 41(g) thus provides a potential mechanism, in at least some contexts, for dealing with the question of retention at a time when the government may be

---

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.

expected to have greater information about the data it seeks and the best process through which to search and present that data in court. It is worth observing, then, that Rule 41(g) constitutes a statutory solution (as opposed to a purely judicially constructed one) to at least one facet of the retention problem.[41] Statutory approaches, of course, do not relieve courts from their obligation to interpret the Constitution; nevertheless, such approaches have, historically, provided one mechanism for safeguarding privacy interests while, at the same time, addressing the needs of law enforcement in the face of technological change. Indeed, when Congress addressed wiretapping in the Omnibus Crime Control and Safe Streets Act of 1968, the Senate Judiciary Committee issued a report reflecting precisely this ambition — to provide a framework through which law enforcement might comport with the demands of the Constitution and meet important law enforcement interests. *See* S. Rep. No. 90-1097, at

---

[41] The advisory committee notes to the 2009 amendments to Federal Rule of Criminal Procedure 41(e)(2)(B) contemplate that Rule 41(g) may indeed constitute such a solution. Regarding specifically the seizure of electronic storage media or the search of electronically stored information, the advisory committee notes observe that though the rule does not create

> a presumptive national or uniform time period within which . . . off-site copying or review of . . . electronically stored information would take place, . . . [i]t was not the intent of the amendment to leave the property owner without . . . a remedy[:] . . . Rule 41(g) . . . provides a process for the "person aggrieved" to seek an order from the court for a return of the property, including storage media or electronically stored information, under reasonable circumstances.

66-76 (1968) (describing the construction of the then-Omnibus Crime Control and Safe Streets of Act of 1967, which laid out comprehensive rules for when and how law enforcement could intercept wire and oral communications through electronic surveillance, as a Congressional attempt to respond to and synthesize, first, technological change, *id.* at 67, second, ineffective or unclear state statutory regimes, *id.* at 69, third, evolving Supreme Court precedent, *id.* at 74-75, and fourth, law enforcement concerns, *id.* at 70); *see also id.* at 66 ("Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."). The Act did not seek to supplant the role of the courts, nor could it have done so, but it did demonstrate the intuitive proposition that Congress can and should be a partner in the process of fleshing out the contours of law-enforcement policy in a shifting technological landscape. In acknowledging the role of Rule 41(g), then, we seek also to suggest that search and seizure of electronic media may, no less than wiretapping, merit not only judicial review but also legislative analysis; courts need not act alone.

As we have said, we need not resolve the ultimate question whether the Government's retention of forensic copies of Ganias's hard drives during the pendency of its investigation violated the Fourth Amendment. We conclude, moreover, that we should not decide this question on the present record, which does not permit a full assessment of the complex and rapidly evolving technological issues, and the significant privacy concerns, relevant to its

consideration.[42] Having noted Ganias's argument, we

---

[42] The dissent faults us for our caution in this regard, suggesting that "the prevailing scholarly consensus has been that the [original *Ganias*] panel largely got it right." Dissent at 5 n.5. With respect, the dissent mischaracterizes the scholarly response. As an initial matter, the dissent cites Professor Kerr as having concluded that the panel "largely got it right." *Id.* In fact, Kerr's analysis of the original panel opinion is generally critical, not complimentary. *See* Kerr, *Executing Warrants for Digital Evidence*, *supra*, at 32 (critiquing the panel for going too far and thus offering a "particularly strong version" of Kerr's approach). Assessing the original panel's analysis, Kerr first concludes that, given the technological contours of electronic media, an affirmative obligation to delete could be "difficult to implement," just as it could be difficult to ascertain at what point in the process such a "duty [would be] triggered." *Id.* Second, Kerr concludes that — to the degree that restrictions should be placed upon what the government may do with non-responsive data that must, for pragmatic reasons, be retained — a restriction preventing the government from viewing data pursuant to a search warrant acquired with independent probable cause is unnecessary "to restore the basic limits of search warrants in a world of digital evidence." *Id.* at 33.

Apart from this citation to Kerr and to two student notes (which reach differing conclusions about the merits of the panel opinion), the articles the dissent cites (as is evident from the carefully worded parentheticals the dissent itself provides) are not evaluations of the original panel opinion, but instead provide largely descriptive accounts of the opinion and its relation to other case law in the context of making other points. The signed article that comes the closest to providing a normative critique of the panel's opinion concludes that "*perhaps* the panel's answer is broadly the right answer," but rejects the panel's — and the dissent's — reasoning. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. Pa. J. Const. L. 933, 948 (2016) (emphasis added); *see id.* at 947 (concluding that, because "in 2003 and in 2006 the government obtained a warrant demonstrating particularized

do not decide its merits. We instead turn to the question of good faith.

III

The Government argues that, because it acted in good faith throughout the pendency of this case, any potential violation of the Fourth Amendment does not justify the extraordinary remedy of suppression. *See Davis v. United States*, 564 U.S. 229, 237 (2011) (noting the "heavy toll" exacted by suppression, which "requires courts to ignore reliable, trustworthy evidence," and characterizing suppression as a "bitter pill," to be taken "only as a 'last resort'" (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006))); *accord United States v. Clark*, 638 F.3d 89, 99 (2d Cir. 2011). In particular, the Government urges that its "reliance on the 2006 warrant," which it obtained after disclosing to the magistrate judge all relevant facts regarding its retention of the mirrored files, "fits squarely within the traditional *Leon* exception for conduct taken in reliance on a search warrant issued by a neutral and detached

---

suspicion towards Ganias's data, and in each instance agents thereafter only looked for the responsive data," it was inapt for the original panel to conclude that the Government's position would transform a warrant for electronic data into a "general warrant"). We do not opine on these issues here, but we see no scholarly consensus on the complicated questions implicated in this case that would suggest caution is ill-advised in a matter where these questions need not be answered to reach a resolution. Caution, although not always satisfying, is sometimes the most appropriate approach.

magistrate judge."[43] Government Br. at 59; *see Leon*, 468 U.S. at 922. For the following reasons, we agree.

In *Leon*, the Supreme Court determined that the exclusion of evidence is inappropriate when the government acts "in objectively reasonable reliance" on a search warrant, even when the warrant is subsequently invalidated. 468 U.S. at 922; *see also Clark*, 638 F.3d at 100 ("[I]n *Leon*, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within its protection."). Such reliance, however, must be *objectively reasonable*. *See Leon*, 468 U.S. at 922-23 ("[I]t is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." (footnote omitted)). Thus, to assert good faith reliance successfully, officers must, *inter alia*, disclose all potentially adverse information to the issuing judge. *See United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.) ("The good faith exception to the exclusionary rule does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge . . . ."), *aff'd and amended*, 91 F.3d 331 (2d Cir. 1996) (per curiam); *see also United States v. Thomas*, 757 F.2d 1359, 1368

---

[43] The Government also contends: (1) that it relied in good faith on the 2003 warrant in retaining the mirrors; and (2) that its behavior was in no way culpable, rendering exclusion inappropriate, *see* Government Br. at 51; *see also Herring v. United States*, 555 U.S. 135, 144 (2009) ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."); *accord Davis*, 546 U.S. at 237. Given our conclusion that the Government relied in good faith on the 2006 warrant, we need not address these additional arguments.

(2d Cir. 1985) (finding good faith reliance on a warrant, under *Leon*, where officers, first, committed a constitutional violation they did not reasonably know, at the time, was unconstitutional — a warrantless canine sniff — and second, in relying on evidence from this sniff in a warrant application, fully revealed the fact of the canine sniff to a magistrate judge), *cert. denied by Fisher v. United States*, 474 U.S. 819 (1985) *and Rice v. United States*, 479 U.S. 818 (1986).

Ganias argues that reliance on the 2006 warrant is misplaced for two reasons. First, he urges that the alleged constitutional violation here (unlawful retention of the mirrored drives) had "long since" ripened into a violation by April 2006, when the second warrant was obtained, Appellant Br. at 55-56, and attests that "[n]othing [in *Leon*] suggests that the police, *after* they engage in misconduct, can then 'launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate,'" *id.* at 56 (quoting *State v. Hicks*, 707 P.2d 331, 333 (Ariz. Ct. App. 1985)). Second, Ganias argues that, even if "a subsequent warrant can ever appropriately purge the taint of an earlier violation, the agent must, at the very least, 'provide all potentially adverse information' regarding the earlier illegality 'to the issuing [magistrate] judge,'" a requirement that he argues was not satisfied here. *Id.* at 58 (quoting *Reilly*, 76 F.3d at 1280). Ganias's arguments are unavailing.

First, Ganias relies on this Court's decision in *Reilly* to argue categorically that agents who have engaged in a predicate Fourth Amendment violation may not rely on a subsequently issued warrant to establish good faith. *Reilly*, however, stands for no such thing. In

Reilly, officers unlawfully intruded on the defendant's curtilage, discovering about twenty marijuana plants, before they departed and obtained a search warrant based on a "bare-bones" description of their intrusion and resulting observations which this Court found "almost calculated to mislead." *Reilly*, 76 F.3d at 1280; *see also id.* ("[The affidavit] simply . . . stated that [the officers] walked along Reilly's property until they found an area where marijuana plants were grown. It did not describe this area to the Judge[,] . . . [and it] gave no description of the cottage, pond, gazebo, or other characteristics of the area. . . . [The omitted information] was crucial. Without it, the issuing judge could not possibly make a valid assessment of the legality of the warrant that he was asked to issue."). We rejected the government's argument that the officers were entitled to rely on the warrant, noting that the officers had "undert[aken] a search that caused them to invade what they could not fail to have known was potentially . . . curtilage," and that they thereafter "failed to provide [the magistrate issuing the warrant] with an account of what they did," so that the magistrate was unable to ascertain whether the evidence on which the officers relied in seeking the warrant was "itself obtained illegally and in bad faith." *Id.* at 1281. In such circumstances, *Leon* did not — and does not — permit good faith reliance on a warrant. *See Leon*, 468 U.S. at 923 (observing that an officer's reliance on a warrant is not *objectively reasonable* if he "misled [the magistrate with] information in an affidavit that [he] knew was false or would have known was false except for his reckless disregard of the truth").

The present case, however, is akin not to *Reilly*, but to this Court's decision in *Thomas*, which the *Reilly* panel carefully distinguished, while reaffirming. *See Reilly*, 76 F.3d at 1281-82. In *Thomas*, an agent, acting without a warrant, used a dog trained to detect narcotics to conduct a "canine sniff" at a dwelling. 757 F.2d at 1367. The agent presented evidence acquired as a result of the sniff to a "neutral and detached magistrate" who, on the basis of this and other evidence, determined that the officer had probable cause to conduct a subsequent search of the dwelling in question. *Id.* at 1368. The defendant moved to suppress the evidence found in executing the search warrant, arguing that the antecedent canine sniff constituted a warrantless, unconstitutional search and that the evidence acquired from that sniff was dispositive to the magistrate judge's finding of probable cause. *See id.* at 1366. This Court agreed on both counts: first deciding, as a matter of first impression in our Circuit, that the canine sniff at issue constituted a search, *id.* at 1367, and second determining that, absent the evidence acquired from this search, the warrant was not supported by probable cause, *id.* at 1368. The *Thomas* panel nevertheless concluded that suppression was inappropriate because the agent's reliance on the warrant was objectively reasonable: "The . . . agent brought his evidence, including [a factual description of the canine sniff], to a neutral and detached magistrate. That magistrate determined that probable cause to search existed, and issued a search warrant. There is nothing more the officer could have or should have done under these circumstances to be sure his search would be legal." *Id.*

Reilly carefully distinguished *Thomas*, and in a manner that makes apparent that it is *Thomas* that is dispositive here. First, the *Reilly* panel noted that *Thomas* was unlike *Reilly*, in that the agent in *Thomas* disclosed all crucial facts for the legal determination in question to the magistrate judge. *Reilly*, 76 F.3d at 1281. Then, the *Reilly* panel articulated another difference: while in *Reilly*, "the officers undertook a search that caused them to invade what they could not fail to have known was potentially Reilly's curtilage," in *Thomas*, the agent "did not have any significant reason to believe that what he had done [conducting the canine sniff] was unconstitutional." *Id.*; *see also id.* ("[U]ntil *Thomas* was decided, no court in this Circuit had held that canine sniffs violated the Fourth Amendment."). Thus, the predicate act in *Reilly* tainted the subsequent search warrant, whereas the predicate act in *Thomas* did not. The distinction did not turn on whether the violation found was *predicate*, or prior to, the subsequent search warrant on which the officers eventually relied, but on whether the officers' reliance on the warrant was reasonable.

Contrary to Ganias's argument, then, it is not the case that good faith reliance on a warrant is never possible in circumstances in which a predicate constitutional violation has occurred. The agents in *Thomas* committed such a violation, but they had no "significant reason to believe" that their predicate act was indeed unconstitutional, *Reilly*, 76 F.3d at 1281, and the issuing magistrate was apprised of the relevant conduct, so that the magistrate was able to determine whether any predicate illegality precluded issuance of the warrant. In such circumstances, invoking the good faith doctrine does not "launder [the

agents'] prior unconstitutional behavior by presenting the fruits of it to a magistrate," as Ganias suggests. Appellant Br. at 56 (quoting *Hicks*, 707 P.2d at 333). In such cases, the good faith doctrine simply reaffirms *Leon*'s basic lesson: that suppression is inappropriate where reliance on a warrant was "objectively reasonable." *Leon*, 468 U.S. at 922.[44]

Such is the case here. First, Agent Hosney provided sufficient information in her affidavit to apprise the magistrate judge of the pertinent facts regarding the retention of the mirrored copies of Ganias's hard drives — the alleged constitutional violation on which he relies. Agent Hosney explained that the mirror images in question had been "seized on November 19, 2003 from the offices of Taxes International," J.A. 461, ¶ 7; that information material to the initial investigation of a third party had been located on the mirrors and "analyzed in detail," J.A. 464, ¶ 15; that Ganias was not, at the time of the original seizure, under

---

[44] Insofar as Ganias argues that *Thomas*'s and *Reilly*'s holdings are limited to when the alleged predicate violation is a *search* that taints the warrant, but do not extend to circumstances in which the alleged predicate violation is a seizure or unlawful retention, we discern no justification for this distinction. But for the canine search in *Thomas* — the predicate violation — there would have been no subsequent warrant pursuant to which the government searched the dwelling and on whose legality it relied in conducting that search. But for the retention in this case — the alleged predicate violation — there could have been no subsequent search warrant pursuant to which the Government searched the relevant evidence and on whose legality the Government relied in conducting that search. To credit Ganias's distinction would be to replace the underlying directive that reliance on a warrant be "objectively reasonable," *Leon*, 468 U.S. at 922, with an arbitrary formalism.

investigation, J.A. 461, ¶ 3; that, "[p]ursuant to [that initial warrant]," Agent Hosney could not search Ganias's personal or business files as the warrant authorized search only of "files for [AB] and IPM," J.A. 464, ¶ 14; and that Ganias's personal data — which Agent Hosney was not authorized to search — was *on those mirrored drives*, J.A. 467, ¶ 27, and thus, *a fortiori*, had been there for the past two and a half years. The magistrate judge was thus informed of the fact that mirrors containing data non-responsive to the 2003 warrant had been retained for several years past the initial execution of that warrant and, to the degree it was necessary, that data responsive to the 2003 warrant had been analyzed in detail. The magistrate therefore had sufficient information on which to determine whether such retention precluded issuance of the 2006 warrant. *Cf. Thomas*, 757 F.2d at 1368 ("The magistrate, whose duty it is to interpret the law, determined that the canine sniff could form the basis for probable cause . . . .").

Ganias disagrees, arguing, in particular, that, though Agent Hosney alerted the magistrate that the mirrors had been retained for several years; that data responsive to the original warrant had been both located and extensively analyzed; and that those of Ganias's QuickBooks files that Agent Hosney wanted to search were non-responsive to the original warrant, the Hosney affidavit did not go far enough in that it failed to disclose that the agents "had been retaining the non-responsive records for a full 16 months *after* the files within the November 2003 warrant's scope had been identified." Appellant Br. at 60. As an initial matter, the Government *did* alert the magistrate that it had located responsive data on the mirrors *and*

conducted extensive analysis of that responsive material, and it is not clear what else the Government should have said: the district court did not determine — nor does the record show — that by January 2005, as Ganias contends, the Government had determined, as a forward-looking matter, that it had performed all forensic searches of data responsive to the 2003 warrant that might prove necessary over the course of its investigation. *Compare* J.A. 322 (Q: "So it's fair to say that as of mid-December [2004], your forensic analysis was completed at that time?" Agent Chowaniec: That's correct, of the computers."), *with* J.A. 324 (Q: "Did you know you wouldn't require further analysis by Greg Norman or any other examiner at the Army lab in Georgia after December of 2004?" Agent Chowaniec: "No."); *see supra* note 12. Nor would it be reasonable to expect additional detail in the affidavit on this point, even assuming Ganias's contention to be correct that the Government had both finished its segregation *and* provided insufficient facts to alert the magistrate judge to that reality, given the dearth of precedent suggesting its relevance. *Cf. Clark*, 638 F.3d at 105 ("[W]here the need for specificity in a warrant or warrant affidavit on a particular point was not yet settled or was otherwise ambiguous, we have declined to find that a well-trained officer could not reasonably rely on a warrant issued in the absence of such specificity."); *cf. Reilly*, 76 F.3d at 1280 (noting that the affidavit in that case, in clear contrast to the affidavit in this one, was "almost calculated to mislead").

Second, here, as in *Thomas*, it is also clear that the agents, as the panel put it in *Reilly*, "did not have any significant reason to believe that what [they] had done

was unconstitutional," *Reilly*, 76 F.3d at 1281 — that their retention of the mirrored hard drives, while the investigation was ongoing, was anything but routine. At the time of the retention, no court in this Circuit had held that retention of a mirrored hard drive during the pendency of an investigation could violate the Fourth Amendment, much less that such retention would do so in the circumstances presented here. *See id.* (noting that suppression was inappropriate in *Thomas* in part because no relevant precedent established that canine sniffs of a dwelling "violated the Fourth Amendment").[45] Moreover, as noted above, the 2003 warrant authorized the lawful seizure not merely of particular records or data, but of the hard drives themselves, or in the alternative the creation of mirror images of the drives to be removed from the premises for later forensic evaluation, and set no greater limit on the Government's retention of those materials than on any other evidence whose seizure it authorized.

---

[45] The closest decision Ganias can locate is *United States v. Tamura*, 694 F.2d at 594-95, an out-of-circuit case that concerned intermingled paper files, the removal of which was unauthorized and the return of which had been vigorously sought by the affected parties. Whatever relevance that case may have by analogy, it is not sufficient to alert a reasonable agent to the existence of a serious Fourth Amendment problem: for to suggest that a holding applicable to retaining *intermingled paper files* specifically demanded to be returned clearly resolves a question about retention of a *physical digital storage medium* (the return of which had been neither suggested nor requested) would be "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 134 S. Ct. at 2488.

Finally, the record here is clear that the agents acted reasonably throughout the investigation. They sought authorization in 2003 to seize the hard drives and search them off-site; they minimized the disruption to Ganias's business by taking full forensic mirrors; they searched the mirrors only to the extent authorized by, first, the 2003 warrant, and then the warrant issued in 2006; they were never alerted that Ganias sought the return of the mirrors; and they alerted the magistrate judge to these pertinent facts in applying for the second warrant. In short, the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganias's tax evasion. This case fits squarely within *Leon* so that, assuming, *arguendo*, that a Fourth Amendment violation occurred, suppression was not warranted.

* * *

We conclude that the Government relied in good faith on the 2006 search warrant and thus AFFIRM the judgment of the district court. Given this determination, we do not reach the specific Fourth Amendment question posed to us today.

LOHIER, Circuit Judge, joined by POOLER, Circuit Judge, concurring:

I concur fully in Part I of the majority opinion, which accurately recites the facts, and Part III, which affirms based on the narrow ground that the Government relied in good faith on the 2006 search warrant obtained in this case. It bears emphasizing that Part III contains the only holding in the majority opinion. I also concur insofar as the majority opinion clarifies that under appropriate circumstances it may be helpful for litigants to use the mechanism provided by Rule 41(g) of the Federal Rules of Criminal Procedure when faced with the Government's retention of electronic data.

CHIN, *Circuit Judge*, dissenting:

I respectfully dissent.

Over two hundred fifty years ago, agents of the King of England, with warrant in hand, entered the home of John Entick. They rummaged through boxes and trunks, cabinets and bureaus. They were looking for evidence of known instances of seditious libel, but they took "all the papers and books without exception." *Entick v. Carrington*, 19 How. St. Tr. 1029, 1064 (C.P. 1765). In holding that Entick's rights were violated, the court explained:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.

Id. at 1066.

Entick was not lost on the Framers. As the Supreme Court has noted, "its propositions were in the minds of those who framed the fourth amendment to the constitution, and were considered as sufficiently explanatory of what was meant by unreasonable

searches and seizures." *Boyd v. United States*, 116 U.S. 616, 626-27 (1886). And enshrined in the Fourth Amendment is the foundational principle that the Government cannot come into one's home looking for some papers and, without suspicion of broader criminal wrongdoing, indiscriminately take all papers instead.

In this case, the Government argues that when those papers are inside a computer, the result is different. It argues that when computers are involved, it is free to overseize files for its convenience, including files outside the scope of a warrant, and retain them until it has found a reason for their use. In essence, the Government contends that it is entitled to greater latitude in the computer age. I disagree. If anything, the protections of the Fourth Amendment are even more important in the context of modern technology, for the Government has a far greater ability to intrude into a person's private affairs.[1]

---

[1] *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs . . . ."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

Here, although the Government had a warrant for documents relating to only two of defendant-appellant Stavros Ganias's accounting clients, it seized *all* the data from three of his computers, including wholly unrelated personal files and files of other clients. The Government did so solely as a mater of convenience, and not because it suspected Ganias or any of his other clients of wrongdoing. The Government was able to extract the responsive files some thirteen months later. But instead of returning the non-responsive files, the investigators retained them, because, as one agent testified, they "viewed the data as the government's property, not Mr. Ganias's property." J. App. 146.[2] Some sixteen months later, almost two and a half years after the files were first seized, the Government found an unrelated reason to prosecute Ganias -- his personal tax -- evasion and it sought judicial authorization to reexamine the data that was still in its possession. The Government contends that this conduct did not violate the Fourth Amendment, and that, even if it did, suppression was not warranted because its agents acted in good faith.

I disagree. I would hold, as the panel held unanimously, that the Government violated Ganias's Fourth Amendment rights when it retained Ganias's non-responsive files for nearly two-and-a-half years and then reexamined the files for evidence of additional crimes. *United States v. Ganias*, 755 F.3d 125, 133-40

---

[2] Throughout this dissent I refer as a matter of convenience to data on Ganias's hard drive as "files" or "documents." Of course, computers contain a variety of types of data, including data that we do not utilize as discrete "files" or "documents" (*e.g.*, metadata, the operating system, the BIOS).

(2d Cir. 2014). I would also hold, as two members of the panel did, that the Government's actions are not excused by the good faith exception. *Id.* at 140-41. *But see id.* at 141 (Hall, *J.*, dissenting in part).[3] Accordingly, I dissent.

I.

I consider first whether Ganias's Fourth Amendment rights were violated. The majority addresses the question at length, with some twenty-five pages of scholarly discussion about the Fourth Amendment in the digital age, but it reaches no conclusion. *E.g.*, Maj. Op. at 3, 22, 27, 38, 45, 47-48. Although we reheard the case *en banc* (at our own request and not at the request of any party), and despite the benefit of additional briefing and oral argument from the parties as well as eight *amicus* briefs,[4] the Court declines to rule on the question,

---

[3] The third member of the panel was the Honorable Jane A. Restani of the United States Court of International Trade, who sat by designation. Judge Restani was not eligible to participate in the *en banc* proceedings. *See* 28 U.S.C. § 46(c).

[4] All eight *amici* urged that we find a Fourth Amendment violation. Brief for *Amicus Curiae* Center for Constitutional Rights as *Amicus Curiae* in Support of Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597942; Brief for *Amici Curiae* Center for Democracy & Technology, ACLU, et al. in Support of Defendant-Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597943; Brief of *Amici Curiae* Electronic Privacy Information Center in Support of Appellant and Urging Affirmance, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4610149; Brief on Rehearing *En Banc* for *Amici Curiae* Federal Public Defenders Within the Second Circuit in Support of Appellant Stavros M. Ganias, No. 12-240-cr (July 29, 2015), 2015 WL 4597956; Brief of

"offer[ing] no opinion on the existence of a Fourth Amendment violation in this case." *Id.* at 22. I would reach the question, and I would hold, as did the panel, that the Fourth Amendment was indeed violated.[5]

Google Inc. as Amicus Curiae Supporting Defendant-Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597960; *Amicus Curiae* Brief of the National Ass'n of Criminal Defense Lawyers in Support of Defendant-Appellant and Urging Reversal , *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597959; Brief for *Amicus Curiae* New York Council of Defense Lawyers in Support of Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597958; Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Defendant- Appellant Stavros M. Ganias, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597961.

[5] I note also that the prevailing scholarly consensus has been that the panel largely got it right with its Fourth Amendment approach. *E.g.*, Stephen E. Henderson, *Fourth Amendment Time Machines (and What They May Say About Police Body Cameras)*, 18 U. Pa. J. Const. L. 933, 947 (2016) ("I agree, though I differ from the panel's reasoning."); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 30-33 (2015) (concluding that "[t]he basic approach mirrors the ongoing seizure approach recommended in this Article" and that "*Ganias* properly focuses on the reasonableness of the ongoing seizure of the nonresponsive files," while labeling the panel opinion as "a particularly strong version" that "courts could adopt"); *see also* Recent Case, *Second Circuit Creates A Potential "Right to Deletion" of Imaged Hard Drives.* -- United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014)*, 128 Harv. L. Rev. 743, 747-50 (2014) (concluding that "[t]he *Ganias* court's opinion properly held that Ganias's Fourth Amendment rights were violated, and it rightly recognized the importance of the particularity requirement in the context of electronic evidence," but arguing that the panel could have "issued a narrower opinion"). *But see* Note, *Digital Duplications and the Fourth Amendment*, 129 Harv. L. Rev. 1046, 1059-64 (2016) (arguing the retention at issue should have been considered as a "search" and

A.

The facts are largely undisputed. Ganias was providing tax and accounting services to individuals and small businesses, including Industrial Property Management, Inc. ("IPM") and American Boiler. In November 2003, the Army, as part of an investigation of those two entities, subpoenaed from Ganias:

> All books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and American Boiler . . . .

J. App. 433. Two Army computer specialists and another Army investigator came to Ganias's office, and

---

not a "seizure"). Others have likewise commented that the panel opinion fits with current Supreme Court jurisprudence, including, in particular, *Riley v. California*, 134 S. Ct. 1473. *E.g.*, Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 112-13 (2014) ("The rule adopted in *Ganias* is consistent with the scope of privacy interests in digital data outlined in *Riley*, and other courts will be more likely to adopt the rule in light of the Supreme Court's decision."); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117, 238-41 (2015) (commenting that, like the panel opinion, *Riley* "similarly supports a Fourth Amendment use restriction on lawfully obtained information" and concluding that "[e]ven though the government might have legally obtained the information at the front end, it could not search the information for evidence of criminal activity absent a warrant, supported by probable cause"); Paul Ohm, *The Life of* Riley *(*v. California*)*, 48 Tex. Tech L. Rev. 133, 138-39 (2015) (anticipating that future courts could find *Ganias* supportable under *Riley*).

they saw three computers. They made identical copies of the hard drives of those computers to take with them -- that is, they cloned the hard drives by making exact replicas ("mirror images") on blank hard drives. In the course of doing so, they took data and files *not* "relating to the business, financial and accounting operations of [IPM] and American Boiler." *Id.* In fact, they took from those hard drives *all* of Ganias's data, including files relating to his personal affairs.

Back in their offices, the Army investigators copied the data taken from Ganias's computers onto "two sets of 19 DVDs," one of which was "maintained as evidence" while the other was kept as a "working copy." Special App. 11. It took the Army Criminal Investigation Division some seven months to begin reviewing the files, but before it began doing so, it invited the Internal Revenue Service (the "IRS") to join the investigation. The Army and the IRS thereafter proceeded separately, reviewing the mirror images for files responsive to the warrant.

By December 2004, approximately thirteen months after the seizure, some four months of which was spent locating a copy of the off-the-shelf consumer software known as QuickBooks, Army and IRS investigators were able to isolate and extract the files covered by the warrant, that is, the files relating to IPM and American Boiler. The investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records. Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.

The investigators did not, however, purge or delete or return the non-responsive files. To the contrary, they retained the files because they "viewed the data as the government's property, not Mr. Ganias's property." J. App. 146.[6] Their view was that while items seized from an owner will be returned after an investigation closes, all of the electronic data here was evidence that was to be protected and preserved. As one agent testified, "[W]e would not routinely go into DVDs to delete data, as we're altering the original data that was seized. And you never know what data you may need in the future. . . . I don't normally go into electronic data and start deleting evidence off of DVDs stored in my evidence room." *Id.* at 122.

In late 2004, IRS investigators discovered accounting irregularities regarding transactions between IPM and American Boiler in the documents taken from Ganias's office. After subpoenaing and reviewing the relevant bank records in 2005, they began to suspect that Ganias was not properly reporting American Boiler's income. Accordingly, on July 28, 2005, some twenty months after the seizure of his computer files, the Government officially expanded its investigation to include possible tax violations by Ganias. Further investigation in 2005 and early 2006 indicated that Ganias had been improperly reporting income for both his clients, leading the Government to

---

[6] The majority suggests that I "seize[] on this single sentence . . . as the smoking gun of the Government's bad faith." Maj. Op. at 16 n.13. The testimony is what it is: a statement under oath by a law enforcement officer explaining the Government's actions. Moreover, as discussed below, there is more than just this single sentence to show the lack of good faith. *See infra* Part II.B.

suspect that he also might have been underreporting his own income.

At that point, the IRS case agent wanted to review Ganias's personal financial records, and she knew, from her review of the seized computer records, that they were among the files in the DVD copies of Ganias's hard drives. The case agent was aware, however, that Ganias's personal financial records were beyond the scope of the November 2003 warrant, and consequently she did not believe that she could review the non-responsive files, even though they were already in the Government's possession.

In February 2006, the Government asked Ganias and his counsel for permission to access certain of his personal files that were contained in the materials seized in November 2003. Ganias did not respond, and thus, on April 24, 2006, the Government obtained another warrant to search the preserved mirror images of Ganias's personal financial records taken in 2003. At that point, the mirror images had been in the Government's possession for almost two-and-a-half years.

B.

"[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). In adopting the Fourth Amendment, the Framers were principally concerned about "indiscriminate searches and seizures" conducted "under the authority of 'general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)). General warrants were ones "not grounded

upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013). The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin*, 720 F.3d at 445-46.

The latter requirement, in particular, "makes general searches . . . impossible" because it "prevents the seizure of one thing under a warrant describing another." *Id.* at 446 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant. *See Horton v. California*, 496 U.S. 128, 140 (1990); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982). Certain exceptions have been made in those "comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site." *Tamura*, 694 F.2d at 595-96. These circumstances might occur, for example, where potentially relevant documents are interspersed through a large number of boxes or file cabinets. *See id.* at 595. But in those cases, the off-site review had to be monitored by a neutral magistrate and non-responsive documents were to be returned after the relevant items were identified. *Id.* at 596-97.

In the computer age, off-site review has become much more common. The ability of computers to store

massive volumes of information presents logistical problems in the execution of search warrants, and files on a computer hard drive are often "so intermingled that they cannot feasibly be sorted on site." *Id.* at 595. Forensic analysis of electronic data may take weeks or months to complete, and it would be impractical for agents to occupy an individual's home or office, or retain an individual's computer, for such extended periods of time. It is now also unnecessary. Today, advancements in technology enable the Government to create a mirror image of an individual's hard drive, which can be searched as if it were the actual hard drive but without otherwise interfering with the individual's use of his home, office, computer, or files. Indeed, the Federal Rules of Criminal Procedure now provide that a warrant for computer data presumptively "authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B).

But these practical necessities must still be balanced against our possessory and privacy interests, which have become more susceptible to deprivation in the computer age. A computer does not consist simply of "papers," but now contains the quantity of information found in a person's residence or greater. *See Riley v. California*, 134 S. Ct. 2473, 2489 (2014); *Galpin*, 720 F.3d at 446. Virtually the entirety of a person's life may be captured as data: family photographs, correspondence, medical history, intimate details about how a person spends each passing moment of each day. GPS-enabled devices reveal our whereabouts. A person's internet search history may disclose her mental deliberations, whether or not those thoughts were favored by the Government, the public

at large, or even that person's own family. Smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 134 S. Ct. at 2489; *see also* Michael D. Shear, David E. Sanger & Katie Benner, *In the Apple Case, a Debate Over Data Hits Home*, N.Y. Times (Mar. 13, 2016) ("It is a minicomputer stuffed with every detail of a person's life: photos of children, credit card purchases, texts with spouses (and nonspouses), and records of physical movements."). From a mere data storage device, a forensic analyst could reconstruct a "considerable chunk of a person's life." Kerr, *supra* note 1, at 569. All of this information is captured when the Government, in executing a search warrant, makes a mirror image of a hard drive.

We know only general descriptions of what was in Ganias's three hard drives -- "personal and financial information," including information on other tax and accounting clients (*e.g.*, social security numbers) that was private to them -- but the Fourth Amendment requires us to consider broadly the ramifications of computer seizures. J. App. 428. If Ganias were a doctor, his computer might have contained the entire medical history of hundreds of individuals. If Ganias were a teacher, his computer could have contained educational information on dozens of students and communications with their families. If Ganias were not an individual but a corporation like Apple, Dropbox, Google, or Microsoft that stores individuals 'information in the "cloud," the Government would have captured an untold vastness of information on millions of individuals. *See* Jim Kerstetter, *Microsoft Goes on Offensive Against Justice Department*, N.Y. Times (Apr.

15, 2016) ("When customer information is stored in a giant data center run by companies like Google, Apple and Microsoft, investigators can go straight to the information they need, even getting a judge to order the company to keep quiet about it."); *see also* Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 743 (2016) ("Twenty years ago, a kidnapper might have confessed to a crime by writing in his diary. . . . Today the same admission is just as likely to be stored online. . . .").

To safeguard individuals' possessory and privacy interests, when the Government seeks to review mirror images off-site, we are careful to subject the Government's conduct to the rule of reasonableness. *See, e.g.*, *United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)). The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's notes to 2009 amendments. The committee noted that several variables -- storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload -- influence the duration of a forensic analysis and counsel against a "one size fits all" time period. *Id.* In combination, these factors might justify an off-site review lasting for a significant period of time. They do not, however, provide an "independent

basis" for retaining any electronic data "other than [those] specified in the warrant." *United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1171 (9th Cir. 2010) (*en banc*) (*per curiam*).

Hence, for these practical considerations, the Government may, consistent with the Fourth Amendment, overseize electronically stored data when executing a warrant. But overseizure is exactly what it sounds like. It is a seizure that *exceeds* or *goes beyond* what is otherwise authorized by the Fourth Amendment. It is an overseizure of evidence that may be reasonable, in light of the practical considerations.

But once the Government is able to extract the responsive documents, its right to the overseizure of evidence comes to an end. This obvious principle has long been adhered to in the context of physical documents, such as when the Government seizes entire file cabinets for off-site review. *See Tamura*, 694 F.2d at 596-97 ("We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper."); *see also Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("[T]o the extent such papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily . . . ."). By logical extension, at least in a situation where responsive computer files can be extracted without harming other government interests, this principle would apply with equal force. *See CDT*, 621 F.3d at 1175-76 (using "file cabinets" as a starting analogy for analyzing digital privacy issues). Once responsive files are segregated or extracted, the retention of non-responsive documents is no longer

reasonable, and the Government is obliged, in my view, to return or dispose of the non-responsive files within a reasonable period of time. *See CDT*, 621 F.3d at 1179 (Kozinski, *J.*, concurring) ("Once the data has been segregated . . . any remaining copies should be destroyed or . . . returned . . . ."). At that point, the Government's overseizure of files and continued retention of non-responsive documents becomes the equivalent of an unlawful general warrant. *See CDT*, 621 F.3d at 1176 (majority opinion) (noting "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *cf. United States v. Jones*, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, *J.*, concurring) (warning that "Government can store . . . records and efficiently mine them for information years into the future").

In the circumstances here, the Government violated Ganias's right against unreasonable searches and seizures. The Government overseized Ganias's data in November 2003, taking both responsive and non-responsive documents. By December 2004, the responsive documents had been segregated and extracted. Yet, instead of returning or deleting the non-responsive files, the Government retained them for another year and a half, until it finally developed a justification to search them again for unrelated reasons. Without some independent basis for retaining the non-responsive documents in the interim, however, in my view the Government clearly violated Ganias's rights under the Fourth Amendment.

The majority comments that it is "unclear" whether the Government had segregated the files relating to

IPM and American Boiler from non-responsive files by December 2004. Maj. Op. at 15-16 & n.12. But the record shows that by October 2004, the Government had placed files thought to be responsive onto a CD. Referring to this event at rehearing *en banc*, the Government stated:

> There does come a point where we often identify a subset of documents that are responsive, *and you could even call it segregating*. In this case, they put them onto a separate disc as working copies and sent [them] to the case agents.

Oral Arg. 32:12-43 (emphasis added). And as an agent then testified, "as of mid-December, [the] forensic analysis was completed." J. App. 322. In other words, the responsive files were segregated.

The majority posits that perhaps the agents did not consider the forensic analysis as to IPM and American Boiler completed "as a forward-looking matter" as of December 2004. Maj. Op. at 15, 58. The record, however, shows otherwise, and, at a minimum, it is clear that the segregation of the files was essentially complete at that point. Moreover, this factual distinction is both speculative and irrelevant. The Fourth Amendment should not be held in abeyance on the off-chance that later developments might cause agents to want to reexamine documents preliminarily determined to be non-responsive. Indeed, the Fourth Amendment recognizes that some degree of perfection must be sacrificed to safeguard liberties. By barring the Government from simply taking *everything* through the use of a general warrant, the Fourth Amendment contemplates that investigators may miss *something*. With computers, another search term can always be

concocted and data can always be further crunched. But the fact that another iota of evidence might be uncovered at some point down the road does not defeat the rights protected by the Fourth Amendment. *Cf. Riley*, 134 S. Ct. at 2491 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

C.

I next turn to the Government's arguments as to why the Fourth Amendment was not violated. The Government offers several "legitimate governmental interests" that it contends permit it to hold onto data long after it has been seized, sorted, and segregated, even though the data includes irrelevant, personal information. *See* Gov't Br. 29. During the *en banc* process, the Government suggested that these interests permit it to retain data for the duration of the prosecution. *See id.* at 17, 29; Oral Arg. 27:38-57.[7]

At the outset, in evaluating the legitimacy of these reasons in relation to this case, I note what is *not* implicated here. This is not a case where the defendant's non-responsive files had independent evidentiary value -- for instance, in a prosecution where the charge was that evidence had been destroyed, *e.g.*, 18 U.S.C. § 1519, it would be relevant

---

[7] In contrast, before the original panel, the Government argued: "Where the warrant does not specify a time period in which the review must be conducted -- like the November 2003 warrant -- this Court has allowed the government to retain computer material indefinitely and 'without temporal limitation.'" First Gov't Br. 30 (quoting *United States v. Anson*, 304 F. App'x 1, 3 (2d Cir. 2008)).

that certain documents were *not* on the hard drive.[8] This is also not a case where the manner in which a responsive file was stored could be used to prove knowledge or intent, as might be the situation in a child pornography prosecution. And this is not a case where the physical hard drive itself is of evidentiary value -- the fact that Ganias's files were actually found inside a computer did not make his guilt more or less probable. Finally, this is not a case where the Government seized Ganias's hard drive to proceed against him. Instead, the Government retained Ganias's hard drive for some two-and-a-half years without suspecting him of criminal wrongdoing, and the agency that ultimately suspected him of illicit tax activity (the IRS) was not even involved at the outset.

The Government argues that it has the right to retain non-responsive files so that, at trial, *responsive* files will be more easily authenticated or of greater evidentiary weight. Once again, the Government's argument obscures the issues in *this* case. The agents could not have been keeping non-responsive files for the purpose of proceeding against Ganias, as they did not yet suspect Ganias of criminal wrongdoing.

---

[8] The majority twice relatedly suggests that the entire mirror image might be relevant here because Ganias made allusion to a "computer flaw" or "software error" in QuickBooks that did not allow him to properly split deposited checks. *See* Maj. Op. at 18 n.16, 34 n.31. The issue surely could be resolved by retaining only the responsive files and a copy of the pertinent version of QuickBooks. Moreover, even assuming there is some speculative value to retaining entire mirror images to prove the non-existence of a glitch, it would hardly be reasonable to rule that these practical frustrations of everyday technology provide the Government license to keep everything.

Further, even if the authentication concern is genuine, "[t]he bar for authentication of evidence is not particularly high." *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007). Indeed, as long as *a* reasonable juror *could* find that evidence was authentic we permit that evidence to be introduced. *Id.*; *see* Fed. R. Evid. 901(a). Meeting this minimal burden is not difficult -- all the Government need do is to introduce as a trial witness one of its agents who handled the data. *See Tamura*, 694 F.2d at 597.

The Government presses the point by arguing that by keeping the hard drives, it could *more easily* preserve the chain of custody and authenticate by "calculat[ing] . . . a 'hash value' for the original and th[e] [mirror] image." Gov't Br. 30. A "hash value" is an alphanumeric marker (*e.g.*, "ABC123") for data that stays the same *if and only if* the data is not altered. Thus, if a hard drive and its mirror image have the same hash value, the files in the mirror image are exact replicas; whereas if the Government purges data from the mirror image, then hash values would not match. Hash values thus make authentication easy. *See* Fed. R. Evid. 901(b)(4).

The hashing argument, however, is not persuasive. First, the Government would have to call an expert just to explain to a jury what a hash value was, as it did here. *See* Fed. R. Evid. 702(a); Trial Tr. 128-30. This is no less burdensome than simply having an agent testify as to the chain of custody. Second, as the Government acknowledged at rehearing *en banc*, it can hash individual files that it has segregated. *See* Oral Arg. 31:08-30. This practice is not a hypothetical possibility: the Government has done so before, *see,*

e.g., *United States v. Hock Chee Koo*, 770 F. Supp. 2d 1115, 1123 (D. Or. 2011), and the Government did so in this very case for Ganias's QuickBooks files, *see* Trial Tr. 147-54. *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 40-41 (2005) ("Many digital analysis tools can be configured to calculate separate hash values of each individual file . . . ."). The Government's ability to authenticate individual files by hashing them undercuts its assertion that it must retain non responsive files to authenticate responsive ones. Hashing appears to make it easier for the Government to comply with the Fourth Amendment, not harder.

Next, the Government contends that it has an interest in retaining computer evidence in its "original form" to preserve "the integrity and usefulness of computer evidence during a criminal prosecution." Gov't Br. 32. This contention is unpersuasive. The Government can always preserve a copy of the *responsive* files to protect against degradation -- indeed, the Government points to no reason why a hard drive with all of Ganias's files would be less prone to degradation than a hard drive with some of his files. Moreover, even assuming there is some slight prosecutorial advantage gained by being able to show juries what a computer interface looked like in its "original form," this benefit surely does not justify a violation of basic Fourth Amendment rights.

In a similar vein, the Government argues that retention of mirror images "preserves the evidentiary value of computer evidence itself" and might "refute claims . . . of data tampering." Gov't Br. 31-34. As a

practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image.[9] More generally, the Government can argue in every case that overseized evidence will have some bearing on the "evidentiary value" of other, properly seized evidence at trial. When the Government makes authorized seizures of folders of financial information from a file cabinet, it could argue that it is entitled to seize the entire cabinet to demonstrate to a jury that folders were preserved in their original form. Or the Government might like to seize nearby, carefully organized folders of medical information to rebut a claim of incompleteness by showing how meticulous the defendant was. Or the Government might seek to seize a folder of children's report cards to show that the defendant normally kept information from a certain time period. Permitting the Government to keep non-responsive files merely to strengthen the evidentiary value of responsive files would eviscerate the Fourth Amendment.

Remarkably, the Government also argues that it should be allowed to hold on to overseized data for the *defendant's* benefit -- so that it can comply with its discovery obligations and duty to disclose exculpatory materials under *Brady*. *See generally Brady v. Maryland*, 373 U.S. 83 (1963). The Government is essentially arguing that it must hold on to the materials so that it can give them back to the

---

[9] Though the record is silent as to this point, the Government told the Court at rehearing *en banc* that it gave Ganias a copy of the forensic mirror image so that he could conduct his own analysis. *See* Oral Arg. 30:28-31:05.

defendant. Of course, this is not a genuine concern -- the problem can be obviated simply by returning the non-responsive files to the defendant in the first place.

The Government further argues that it should be permitted to retain forensic mirror images so that it may search the images for material responsive to a warrant "as the case evolves." Gov't Br. 35. At base, this is a blanket assertion that the Government can seize first and investigate later. *See CDT*, 579 F.3d at 998 (criticizing approach as: "Let's take everything back to the lab, have a good look around and see what we might stumble upon."). This is the equivalent of a general warrant, and the Fourth Amendment simply does not permit it.

Finally, the Government suggests that the availability of Federal Rule of Criminal Procedure 41(g) weighs in favor of the reasonableness of its actions. Rule 41(g) provides that a person aggrieved by an unlawful seizure "may move for the property's return." This rule, however, cannot shift the Government's burden under the Fourth Amendment onto the defendant. Pointing fingers at Ganias does not help the Government meet its *own* obligation to be reasonable.

The Government's arguments thus fail. In my view, Ganias's Fourth Amendment rights were violated when the Government unreasonably continued to hold on to his non-responsive files long after the responsive files had been extracted to reexamine when it subsequently saw need to do so.

II.

Instead of ruling on the question of whether the Government's actions violated the Fourth Amendment, the majority relies on the good faith exception to the exclusionary rule, and concludes that suppression was not warranted because the Government relied in good faith on the 2006 warrant and that this reliance was objectively reasonable. *See* Maj. Op. at 3.

A.

Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. *United States v. Julius*, 610 F.3d 60, 66 (2d Cir. 2010). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009).

To balance these interests, we have adopted the "good faith" exception, in certain circumstances, as a carve-out to the exclusionary rule. S*ee Davis v. United States*, 564 U.S. 229, 237-39 (2011). When a warrant is present, an agent's objectively reasonable good faith reliance on and abidance by the warrant generally makes exclusion an inappropriate remedy. *See United States v. Leon*, 468 U.S. 897, 922 (1984). Likewise, government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate precedent." *Davis*, 564 U.S. at 232. When agents act in good faith, the exclusionary rule will usually not apply. *See United States v. Aguiar*,

737 F.3d 251, 259 (2d Cir. 2013). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance." *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)).

Furthermore, evidence will be suppressed only where the benefits of deterring the Government's unlawful actions appreciably outweigh the costs of suppressing the evidence -- "a high obstacle for those urging . . . application" of the rule. *Herring*, 555 U.S. at 141 (quoting *Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998)); *see Davis*, 564 U.S. at 232. "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). "The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free -- something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908).

B.

The Government contends that it relied in good faith both on the 2003 warrant and the 2006 warrant. The majority, without supporting its holding with the 2003 warrant, concludes that the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganias's tax evasion, and that suppression therefore was not warranted. *See* Majority Op. at 44-55. I disagree, and would hold that neither warrant provided a good faith basis for retaining the non-

responsive files long after the responsive files had been extracted.

(1)

I first turn to the 2003 warrant. The Government's retention of Ganias's non-responsive files pursuant to the 2003 warrant was hardly lawful or in good faith. The Government, in keeping the entirety of the mirror images, kept substantial amounts of "computer associated data" that did not "relat[e] to the business, financial and accounting operations of [IPM] and American Boiler." J. App. 433. This sort of retention following a "widespread seizure" was not explicitly authorized by the 2003 warrant, *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (quoting *United States v. Matias*, 836 F.2d 744, 748 (2d Cir. 1988)), and, as discussed, amounted to a general search. Likewise, the Government points to no binding appellate precedent that allows it to retain files outside the scope of a warrant when the responsive files can be feasibly extracted. Instead the Fourth Amendment baseline is that the Government may not take and then *keep* papers without a warrant "particularly describing . . . the persons or things to be seized." U.S. Const. amend. IV.

The Government argues nonetheless that the agents had an objectively reasonable good faith belief that their post warrant conduct was lawful, because no precedent held that they could *not* do what they did. The argument fails, in my view, for the precedents are absolutely clear that general warrants are unconstitutional and that government agents authorized to come into one's home to seize papers for a limited purpose may not indiscriminately seize and

retain all papers instead. Any agent who professes to have the ability to do so merely because computers are involved is not acting in good faith.

Moreover, the Government's formulation of "the 'good faith' exception w[ould] swallow the exclusionary rule." *Davis*, 564 U.S. at 258 (Breyer, *J.*, dissenting). The Government is essentially arguing that the absence of binding appellate precedent addressing the overseizure and retention of computer files excuses the agents' actions. But it has always been the case that agents must rely on *something* for their reliance to be objective. That is, officers must "learn 'what is required of them'. . . and . . . conform their conduct to these rules." *Davis*, 564 U.S. at 241 (majority opinion) (quoting *Hudson v. Michigan*, 547 U.S. 586, 599 (2006)); *see also id.* at 250 (Sotomayor, *J.*, concurring) ("[W]hen police decide to conduct a search or seizure in the absence of case law (or other authority) specifically sanctioning such action, exclusion of the evidence obtained may deter Fourth Amendment violations . . . ."). Here, the basic principles were well settled and provided ample guidance. And even if the warrant and our precedent were unclear as to what was allowed, the answer was not for agents to venture alone into uncharted constitutional territory. *See United States v. Johnson*, 457 U.S. 537, 561 (1982) ("[I]n close cases, law enforcement officials would have little incentive to err on the side of constitutional behavior."). Rather, the answer was for the agents to seek out a magistrate to authorize the *continued retention* of Ganias's non-responsive files. *See CDT*, 621 F.3d at 1179 (Kozinski, *J.*, concurring). Once the responsive files were extracted, the Government could have asked to keep non-responsive files for use during a prosecution or for

the purpose of trial and allowed a magistrate to balance the Government's need against Ganias's Fourth Amendment interests. *See Leon*, 468 U.S. at 916 (noting we would not "punish the errors of judges and magistrates"). The Government did not do that, but instead retained the non-responsive files for another year and a half before seeking judicial guidance.

More troublingly, the agents here knew what they were supposed to do -- their actions were "deliberate." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). The agents *knew* they were supposed to return or delete overseized data. When asked whether he was "to return those items or destroy those items that don't pertain to your lawful authority to seize those particular items" after a "reasonable period" of off-site review, the testifying agent answered, "Yes, sir." J. App. 145-46; *see also id.* at 428 (Ganias corroborating that the agent "assured me that those materials and files not authorized under the warrant and not belonging to American Boiler and IPM would be purged once they completed their search"). Instead of following this protocol, that agent testified that the investigators "viewed the data as the government's property, not Mr. Ganias' property." *Id.* at 146; *see also id.* at 122 ("And you never know what data you may need in the future."). In other words, the agents "knew that limits of the warrant w[ere] not be[ing] honored." *United States v. Foster*, 100 F.3d 846, 852 (10th Cir. 1996). This knowledge of the need to return or delete non-responsive files compels a conclusion that the agents did not rely in good faith on the 2003 warrant or any appellate precedent (binding or non-binding) and that the deterrence value of suppression here is substantial.

(2)

I next turn to the 2006 warrant. On April 24, 2006, the Government sought a warrant -- seeking to search "Images of three (3) hard drives seized on November 19, 2003 from the offices of Steve M. Ganias" -- to investigate him personally. J. App. 455. A magistrate judge issued the warrant, and the Government searched the mirror images.

For the purpose of deterring Fourth Amendment violations, the relevant inquiry is whether the agents acted in good faith when they committed the violation. *See Leon*, 468 U.S. at 916 ("[T]he exclusionary rule is designed to deter police misconduct . . . ."). The agents here could not have relied in good faith on the 2006 warrant because it was issued almost two-and-a-half years after the files were first overseized, and some sixteen months after the responsive files had been extracted. That is, the agents did not rely on the 2006 warrant to retain non-responsive files because that warrant came into being only *after* the Fourth Amendment violation occurred. An agent can only rely on something that exists "at the time of the search." *Aguiar*, 737 F.3d at 259; *see Davis*, 131 S. Ct. at 2418 (asking if search was in "objectively reasonable reliance on binding judicial precedent" as of "the time of the search").

In other words, the later 2006 warrant could not cure the prior illegal retention of Ganias's data when agents did not rely on it to retain that data. A warrant is not a Band-Aid that the Government may seek when it realizes its Fourth Amendment violation has been discovered. *See* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 1.3(f) (5th ed.

2015) ("When the magistrate issued the warrant, he did not endorse past activity; he only authorized future activity."). As we have previously held, "Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996).

The Government and the majority rely on a line of cases that includes *United States v. Reilly*, 76 F.3d 1271, and its predecessor, *United States v. Thomas*, 757 F.2d 1359 (2d Cir. 1985). In *Reilly*, we affirmed the *Thomas* principle that illegally obtained evidence need not be excluded where the agents later obtained a warrant by providing a magistrate "the details of their dubious pre-warrant conduct" and where "'there was nothing more the officer could have or should have done under the[] circumstances to be sure his search would be legal.'" *Reilly*, 76 F.3d at 1282 (alterations omitted) (quoting *Thomas*, 757 F.2d at 1368). We required, however, that the officer "did not have any significant reason to believe that what he had done was unconstitutional." *Id.* at 1281.[10]

---

[10] As an initial observation, the *Thomas* principle is not free from doubt. *Reilly* acknowledged that *Thomas* is difficult to square with the holdings of many of our sister circuits without attempting to reconcile conflicting case law. *See id.* at 1282 ("Other courts have criticized *Thomas* . . . ."); *e.g.*, *United States v. McGough*, 412 F.3d 1232, 1240 (11th Cir. 2005); *United States v. O'Neal*, 17 F.3d 239, 243 (8th Cir. 1994); *United States v. Scales*, 903 F.2d 765, 768 (10th Cir. 1990); *United States v. Vasey*, 834 F.2d 782, 789 (9th Cir. 1987). Indeed, the language that exclusion may be avoided when the Government "did not have any significant reason to believe that what [it] had done was unconstitutional," *Reilly*, 76 F.3d at 1282, may one day prove to be too lax.

In this case, the agents did *not* present to the magistrate judge all of "the details of their dubious pre-warrant conduct." *Id.* at 1282. Though the majority points out that the agents disclosed to the magistrate judge in 2006 that the mirror images were seized in November 2003, that Ganias was not then under investigation, and that the mirror images included files outside the scope of the original warrant, this information was not sufficient on its own to permit the magistrate judge to evaluate whether the relevant constitutional violation occurred. *See* Maj. Op. at 56-57. The agents did not disclose that they had segregated responsive files from non-responsive files and extracted the responsive files and that for some time they did not have other, anticipated uses for the non-responsive files. Without this information relating to whether the Government still had a legitimate use for the mirror image during the retention, it simply would not have been feasible for a magistrate judge to consider the legitimacy of the continued retention of the mirror image. *See United States v. Vasey*, 834 F.2d 782, 789 (9th Cir. 1987) ("Typically, warrant applications are requested and authorized under severe time constraints.").

Likewise, unlike in *Thomas*, there was more that the Government could have done prior to 2006 to ensure that its conduct was legal. *See Thomas*, 757 F.2d at 1368. As noted above, it could have gone to a magistrate judge much earlier for permission to retain the non-responsive computer files.

Finally, the Government *did* have significant reason to believe that its conduct was unconstitutional. As noted, an agent testified that he knew he was supposed

to "return those items or destroy those items that d[idn't] pertain to [his] lawful authority to seize those particular items." J. App. 145-46. And any reasonable law enforcement agent would have understood that it was unreasonable to "view[] [private property] as the government's property" or to treat the 2003 warrant as a general warrant. *Id.* at 146. Furthermore, the language of the 2003 warrant clearly set parameters for what was lawful: only data "relating to" IPM and American Boiler could be kept. *Id.* at 433.

At bottom, in holding that the Government acted with objectively reasonable reliance on the 2006 warrant, the majority condones creative uses of government power to interfere with individuals' possessory interests and to invade their privacy. Without specifically opining on whether the Government can retain overseized, non-responsive files, the majority has crafted a formula for the Government to do just that. The Government only needs to: obtain a warrant to seize computer data, overseize by claiming files are intermingled (they always will be), keep overseized data until the however distant future, and then (when probable cause one day develops) ask for another warrant to search what it has kept. The rule that we have fashioned does nothing to deter the Government from continually retaining papers that are, though initially properly seized, not responsive to or particularly described in a warrant. Instead of deterring future violations, we have effectively endorsed them.

The Government bears the burden of proving "the objective reasonableness of the officers' good faith reliance." *Voustianiouk*, 685 F.3d at 215 (quoting

George, 975 F.2d at 77). It has not met that burden here. To the contrary, the agents exhibited a deliberate or reckless or grossly negligent disregard for Ganias's rights, *see Davis*, 564 U.S. at 238, and, in my view, the benefits of deterring the Government's unlawful actions here appreciably outweigh the costs of suppression, *see Herring*, 555 U.S. at 141; *see also Davis*, 564 U.S. at 232; *Pa. Bd. of Prob. & Parole*, 524 U.S. at 364-65.

III.

In the discussion of lofty constitutional principles, we sometimes forget the impact that our rulings and proceedings may have on individuals and their families. Here, there has been a cloud hanging over Ganias's head for nearly thirteen years, impacting every aspect of his life and the lives of those around him. The cloud is still there now.

The wheels of justice have spun ever so slowly in this case. The Government seized Ganias's files in November 2003, nearly thirteen years ago. He was indicted, in 2008, some eight years ago. He waited two-and-a-half years for a trial, and after he was found guilty, he waited roughly another ten months to be sentenced. He appealed his conviction, but it took another year for his appeal to be heard, and then another year for the appeal to be decided.

The panel issued its decision on June 17, 2014. The panel held that the Government violated Ganias's Fourth Amendment rights and rejected its reliance on the good faith exception. On August 15, 2014, the Government filed a petition for rehearing, seeking panel rehearing only, not rehearing *en banc*, and

seeking rehearing only with respect to the good faith exception. In other words, the Government did not seek rehearing on whether the Fourth Amendment was violated, and it did not seek rehearing *en banc* on either issue.

Yet, on June 29, 2015, more than a year after the panel decision, more than a year after Ganias thought he had won a substantial victory, this Court, on its own initiative, elected to rehear the case *en banc* -- with respect to *both* issues. The Court did so ostensibly to provide guidance in a novel and difficult area of law. But, after a year-long *en banc* process, no guidance has come forth. The Court took on an issue at Ganias's expense and then quickly retreated, relying instead on an issue that was not worthy of *en banc* review.

Ganias's non-responsive files are in the Government's custody still. What began nearly thirteen years ago as an investigation by the Army into two of Ganias's business clients somehow evolved into an unrelated investigation by the IRS into Ganias's personal affairs, largely because the Government did precisely what the Fourth Amendment forbids: it entered Ganias's premises with a warrant to seize certain papers and indiscriminately seized -- and *retained* -- all papers instead.

I respectfully dissent.

APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

Docket No. 12-240

[Filed May 27, 2016]

United States of America,	)
	)
Appellee,	)
	)
v.	)
	)
James L. McCarthy,	)
AKA James McCarthy,	)
	)
Defendant,	)
	)
Stavros M. Ganias,	)
	)
Defendant - Appellant.	)
	)

JUDGMENT

At a Stated Term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 27th day of May, two thousand and sixteen.

Before: Robert A. Katzmann
Chief Judge,
Dennis Jacobs,
José A. Cabranes,
Rosemary S. Pooler,
Reena Raggi,
Richard C. Wesley,
Peter W. Hall,
Debra Ann Livingston,
Gerard E. Lynch,
Denny Chin,
Raymond J. Lohier, Jr.,
Susan L. Carney,
Christopher F. Droney,
Circuit Judges,

The appeal in the above captioned case from a judgment of the United States District Court for the District of Connecticut was argued on the district court's record and the parties' briefs. Upon consideration thereof,

IT IS HEREBY ORDERED, ADJUDGED and DECREED that the judgment of the district court is AFFIRMED.

For The Court:

Catherine O'Hagan Wolfe,
Clerk of Court

APPENDIX C

12-240-cr
United States v. Ganias

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Docket No. 12-240-cr

[Filed June 17, 2014]

UNITED STATES OF AMERICA,	)
	)
Appellee,	)
	)
v.	)
	)
STAVROS M. GANIAS,	)
	)
Defendant-Appellant.	)
	)

August Term 2015

(Argued: April 11, 2013
Decided: June 17, 2014)

Before:

HALL and CHIN, *Circuit Judges*,
and RESTANI, *Judge*.[*]

[*] The Honorable Jane A. Restani, of the United States Court of International Trade, sitting by designation.

Appeal from a judgment of the United States District Court for the District of Connecticut convicting defendant-appellant, following a jury trial, of tax evasion. Defendant-appellant appeals on the grounds that: (1) the district court (Thompson, *J.*) erred in denying his motion to suppress his personal computer records, which had been retained by the Government for more than two-and-a-half years after it copied his computer hard drives pursuant to a search warrant calling for the seizure of his clients' business records; and (2) the district court (Burns, *J.*) abused its discretion in failing to order a new trial where a juror posted comments about the trial on his Facebook page and became Facebook friends with another juror during the trial. We find no abuse of discretion as to the second issue, but we conclude, however, that defendant-appellant's Fourth Amendment rights were violated by the unauthorized retention of his personal files. Accordingly, we vacate the judgment and remand for further proceedings.

VACATED and REMANDED.

Judge Hall concurs in part and dissents in part in a separate opinion.

SARALA V. NAGALA, Assistant United States Attorney (Anastasia E. King *and* Sandra S. Glover, Assistant United States Attorneys, *on the brief*), *for* David B. Fein, United States Attorney for the District of Connecticut, New Haven, Connecticut, *for Appellee*.

STANLEY A. TWARDY, JR. (Daniel E. Wenner, *on the brief*), Day Pitney LLP, Stamford, Connecticut, *for Defendant-Appellant*.

CHIN, *Circuit Judge*:

In this case, defendant-appellant Stavros M. Ganias appeals from a judgment convicting him, following a jury trial, of tax evasion. He challenges the conviction on the grounds that his Fourth Amendment rights were violated when the Government copied three of his computer hard drives pursuant to a search warrant and then retained files beyond the scope of the warrant for more than two-and-a-half years. He also contends that his right to a fair trial was violated when, during the trial, a juror posted comments about the case on his Facebook page and "friended" another juror. We reject the second argument but hold that the Government's retention of the computer records was unreasonable. Accordingly, we vacate the conviction and remand for further proceedings.

STATEMENT OF THE CASE

A. *The Facts*[1]

In the 1980s, after working for the Internal Revenue Service ("IRS") for some fourteen years, Ganias started his own accounting business in Wallingford, Connecticut. He provided tax and accounting services to individuals and small businesses. In 1998, he began

---

[1] The facts relevant to the issues on appeal are largely undisputed and are drawn from the testimony at the hearing on Ganias's motion to suppress, the decision of the district court (Thompson, *J.*) denying the suppression motion, and the transcript of the trial.

providing services to James McCarthy and two of McCarthy's businesses, American Boiler and Industrial Property Management ("IPM"). IPM had been hired by the Army to provide maintenance and security at a vacant Army facility in Stratford, Connecticut.

In August 2003, the Criminal Investigative Command of the Army received a tip from a confidential source that individuals affiliated with IPM were engaging in improper conduct, including stealing copper wire and other items from the Army facility and billing the Army for work that IPM employees performed for American Boiler. The source alleged that evidence of the wrongdoing could be found at the offices of American Boiler and IPM, as well as at the offices of "Steve Gainis [sic]," who "perform[ed] accounting work for IPM and American Boiler."[2]

Based on this information, the Army commenced an investigation. Army investigators obtained several search warrants, including one to search the offices of Ganias's accounting business. The warrant, issued by the United States District Court for the District of Connecticut and dated November 17, 2003, authorized the seizure from Ganias's offices of:

> All books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and American Boiler . . . .

---

[2] The record reflects that Ganias, whose first name is Stavros, was often referred to as "Steve."

The warrant was executed two days later. Army computer specialists accompanied investigators to Ganias's offices and helped gather the electronic evidence. The agents did not seize Ganias's computers; instead, the computer specialists made identical copies, or forensic mirror images, of the hard drives of all three of Ganias's computers. As a consequence, the investigators copied every file on all three computers -- including files beyond the scope of the warrant, such as files containing Ganias's personal financial records. Ganias was present as the investigators collected the evidence, and he expressed concern about the scope of the seizure. In response, one agent "assured" Ganias that the Army was only looking for files "related to American Boiler and IPM." Everything else, the agent explained, "would be purged once they completed their search" for relevant files.

Back in their offices, the Army computer specialist copied the data taken from Ganias's computers (as well as data obtained from the searches of the offices of IPM and American Boiler) onto "two sets of 19 DVDs," which were "maintained as evidence." Some eight months later, the Army Criminal Investigation Lab finally began to review the files.

In the meantime, while reviewing the paper documents retrieved from Ganias's offices, the Army discovered suspicious payments made by IPM to an unregistered business, which was allegedly owned by an individual who had not reported any income from that business. Based on this evidence, in May 2004, the Army invited the IRS to "join the investigation" of IPM and American Boiler and gave copies of the imaged hard drives to the IRS so that it could conduct its own

review and analysis. The Army and the IRS proceeded, separately, to search the imaged hard drives for files that appeared to be within the scope of the warrant and to extract them for further review.

By December 2004, some thirteen months after the seizure, the Army and IRS investigators had isolated and extracted the computer files that were relevant to IPM and American Boiler and thus covered by the search warrant. The investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records. Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.

They did not, however, purge or delete the non-responsive files. To the contrary, the investigators retained the files because they "viewed the data as the government's property, not Mr. Ganias's property." Their view was that while items seized from an owner will be returned after an investigation closes, all of the electronic data here were evidence that were to be protected and preserved. As one agent testified, "[W]e would not routinely go into DVDs to delete data, as we're altering the original data that was seized. And you never know what data you may need in the future. . . . I don't normally go into electronic data and start deleting evidence off of DVDs stored in my evidence room." The computer specialists were never asked to delete (or even to try to delete) those files that did not relate to IPM or American Boiler.

In late 2004, IRS investigators discovered accounting irregularities regarding transactions between IPM and American Boiler in the paper

documents taken from Ganias's office. After subpoenaing and reviewing the relevant bank records in 2005, they began to suspect that Ganias was not properly reporting American Boiler's income. Accordingly, on July 28, 2005, some twenty months after the seizure of his computer files, the Government officially expanded its investigation to include possible tax violations by Ganias. Further investigation in 2005 and early 2006 indicated that Ganias had been improperly reporting income for both of his clients, leading the Government to suspect that he also might have been underreporting his own income.

At that point, the IRS case agent wanted to review Ganias's personal financial records and she knew, from her review of the seized computer records, that they were among the files in the DVDs copied from Ganias's hard drives. The case agent was aware, however, that Ganias's personal financial records were beyond the scope of the November 2003 warrant, and consequently she did not believe that she could review the non-responsive files, even though they were already in the Government's possession.

In February 2006, the Government asked Ganias and his counsel for permission to access certain of his personal files that were contained in the materials seized in November 2003. Ganias did not respond, and thus, on April 24, 2006, the Government obtained another warrant to search the preserved images of Ganias's personal financial records taken in 2003. At that point, the images had been in the Government's possession for almost two-and-a-half years. Because Ganias had altered the original files shortly after the Army executed the 2003 warrant, the evidence

obtained in 2006 would not have existed but for the Government's retention of those images.

B. *Procedural History*

1. *The Indictment*

In October 2008, a grand jury indicted Ganias and McCarthy for conspiracy and tax evasion. The grand jury returned a superseding indictment in December 2009, containing certain counts relating to McCarthy's taxes and two counts relating to Ganias's personal taxes. The latter two counts were asserted only against Ganias. The case was assigned to Chief Judge Alvin W. Thompson.

2. *The Motion to Suppress*

In February 2010, Ganias moved to suppress the computer files that are the subject of this appeal. In April 2010, the district court (Thompson, *J.*) held a two-day hearing and, on April 14, 2010, it denied the motion, with an indication that a written decision would follow. On June 24, 2011, the district court filed its written decision explaining the denial of Ganias's motion to suppress. *See United States v. Ganias*, No. 3:08 Cr. 224, 2011 WL 2532396 (D. Conn. June 24, 2011).

3. *The Trial*

In April 2010, the case was transferred to Judge Ellen Bree Burns for trial. In May 2010, the district court severed the two counts against Ganias for tax

evasion with respect to his personal taxes from the other charges.[3]

Trial commenced on March 8, 2011, with jury selection, and testimony was scheduled to begin on March 10, 2011. At 9:34 p.m. on March 9, the evening before the start of the evidence, one of the jurors, Juror X, posted a comment on his Facebook page: "Jury duty 2morrow. I may get 2 hang someone...can't wait."

Juror X's posting prompted responses from some of his online "friends," including: "gettem while the're young !!!...lol" and "let's not be to hasty. Torcher first, then hang! Lol." During the trial, Juror X continued to post comments about his jury service, including:

March 10 at 3:34 pm:

> Shit just told this case could last 2 weeks..Jury duty sucks!

March 15 at 1:41 pm:

> Your honor I object! This is way too boring.. somebody get me outta here.

March 17 at 2:07 pm:

> Guiness for lunch break. Jury duty ok today.

During the second week of trial, Juror X became Facebook friends with another one of the jurors.

On April 1, 2011, the jury convicted Ganias on both counts. Later that evening, at 9:49 pm, Juror X posted

---

[3] All the other counts were later dismissed.

another comment on his Facebook page: "GUILTY:)." He later elaborated:

> I spent the whole month of March in court. I do believe justice prevailed! It was no cake walk getting to the end! I am glad it is over and I have a new experience under my belt!

4. *The Motion for a New Trial*

On August 17, 2011, Ganias moved for a new trial based on alleged juror misconduct. On August 30, 2011, the district court (Burns, *J.*) held an evidentiary hearing and took testimony from Juror X. The district court denied the motion (as well as a request for the further taking of evidence) in a decision filed on October 5, 2011. *See United States v. Ganias*, No. 3:08 Cr. 224, 2011 WL 4738684 (D. Conn. Oct. 5, 2011).

At the post-trial evidentiary hearing, Juror X explained that he posted the comment on his Facebook page about "hang[ing] someone" as "a joke, all friend stuff," and that he was "[j]ust joking, joking around." At first he could not recall whether he had any conversations with the other juror, with whom he became Facebook friends during the trial, outside the court. He later clarified, however, that he did not have any conversations with the other juror during the course of the trial, prior to deliberations, about the subject matter of the case. He also testified that he in fact considered the case fairly and impartially. The district court accepted Juror X's testimony, found that he was credible, and concluded that he had participated in the deliberations impartially and in good faith.

5. *Sentencing*

On January 5, 2012, the district court (Burns, *J.*) sentenced Ganias principally to twenty-four months' imprisonment. This appeal followed. Ganias was released pending appeal.

DISCUSSION

Ganias raises two issues on appeal: first, he contends that his Fourth Amendment rights were violated when the Government seized his personal computer records and then retained them for more than two-and-a-half years; and, second, he contends that he was entitled to a new trial because of the jury's improper use of social media.

As to the Fourth Amendment issue, we review the district court's findings of fact for clear error, viewing the evidence in the light most favorable to the Government, and its conclusions of law *de novo*. *United States v. Ramos*, 685 F.3d 120, 128 (2d Cir.), *cert. denied*, 133 S. Ct. 567 (2012). As to the issue of the district court's denial of Ganias's motion for a new trial for alleged juror misconduct, we review for abuse of discretion. *United States v. Farhane*, 634 F.3d 127, 168 (2d Cir.), *cert. denied*, 132 S. Ct. 833 (2011).

Although we vacate Ganias's conviction on the Fourth Amendment grounds, we address his juror misconduct claim because the increasing popularity of social media warrants consideration of this question. We address the juror misconduct question first, as it presents less difficult legal issues, and we then turn to the Fourth Amendment question.

A. *Juror's Improper Use of Social Media*

1. *Applicable Law*

Defendants have the right to a trial "by an impartial jury." U.S. Const. amend. VI. That right is not violated, however, merely because a juror places himself in a "potentially compromising situation." *United States v. Aiello*, 771 F.2d 621, 629 (2d Cir. 1985), *abrogated on other grounds by Rutledge v. United States*, 517 U.S. 292 (1996); *see also Smith v. Phillips*, 455 U.S. 209, 217 (1982) ("[I]t is virtually impossible to shield jurors from every contact or influence that might theoretically affect their vote."). A new trial will be granted only if "the juror's ability to perform her duty impartially has been adversely affected," *Aiello*, 771 F.2d at 629, and the defendant has been "substantially prejudiced" as a result, *United States v. Fumo*, 655 F.3d 288, 305 (3d Cir. 2011). Although courts are understandably reluctant to invade the sanctity of the jury's deliberations, the trial judge should inquire into a juror's partiality where there are reasonable grounds to believe the defendant may have been prejudiced. *United States v. Schwarz*, 283 F.3d 76, 97 (2d Cir. 2002); *United States v. Sun Myung Moon*, 718 F.2d 1210, 1234 (2d Cir. 1983). That inquiry should end, however, as soon as it becomes apparent that those reasonable grounds no longer exist. *See Sun Myung Moon*, 718 F.2d at 1234.

B. *Application*

A juror who "friends" his fellow jurors on Facebook, or who posts comments about the trial on Facebook, may, in certain circumstances, threaten a defendant's

Sixth Amendment right to an impartial jury.[4] Those circumstances, however, are not present here. The district court inquired into the matter and credited Juror X's testimony that he deliberated impartially and in good faith. The district judge's credibility determination was not clearly erroneous, and thus she did not abuse her discretion in denying the motion for a new trial.

This case demonstrates, however, that vigilance on the part of trial judges is warranted to address the risks associated with jurors' use of social media. The Third Circuit has endorsed the use of jury instructions like those proposed by the Judicial Conference Committee on Court Administration and Case Management. *See Fumo*, 655 F.3d at 304-05. We do so as well.

The Committee proposes that, before trial, the district judge give an instruction that includes the following:

> I know that many of you use cell phones, Blackberries, the internet and other tools of technology. You also must not talk to anyone

---

[4] *See, e.g.*, *Fumo*, 655 F.3d at 331 (Nygaard, J., concurring) ("The availability of the Internet and the abiding presence of social networking now dwarf the previously held concern that a juror may be exposed to a newspaper article or television program."); *United States v. Juror Number One*, 866 F. Supp. 2d 442, 451 (E.D. Pa. 2011) ("[T]he extensive use of social networking sites, such as Twitter and Facebook, have exponentially increased the risk of prejudicial communication amongst jurors and opportunities to exercise persuasion and influence upon jurors."). *See generally* Amy. J. St. Eve & Michael A. Zuckerman, *Ensuring an Impartial Jury in the Age of Social Media*, 11 Duke L. & Tech. Rev. 1 (2012).

> about this case or use these tools to communicate electronically with anyone about the case. This includes your family and friends. You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, through any internet chat room, or by way of any other social networking websites, including Facebook, My Space, LinkedIn, and YouTube.[5]

The Committee also recommends giving a similar instruction at the close of the case:

> During your deliberations, you must not communicate with or provide any information to anyone by any means about this case. You may not use any electronic device or media, such as a telephone, cell phone, smart phone, iPhone, Blackberry or computer; the internet, or any internet service, or any text or instant messaging service; or any internet chat room, blog, or website, such as Facebook, My Space, LinkedIn, YouTube or Twitter, to communicate to anyone any information about this case or to conduct any research about this case until I accept your verdict.[6]

---

[5] Judicial Conference Comm. on Court Admin. & Case Mgmt., Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate about a Case (December 2009), *available at* www.uscourts.gov/uscourts/News/2010/docs/DIR10-018-Attachment.pdf.

[6] *Id.*

Here, while the district court gave an appropriate instruction at the start of the jury's deliberations, it does not appear that it did so earlier. As demonstrated by this case, instructions at the beginning of deliberations may not be enough. We think it would be wise for trial judges to give the Committee's proposed instructions both at the start of trial and as deliberations begin, and to issue similar reminders throughout the trial before dismissing the jury each day. While situations like the one in this case will not always require a new trial, it is the better practice for trial judges to be proactive in warning jurors about the risks attending their use of social media.

B. *The Seizure and Retention of Ganias's Computer Records*

1. *Applicable Law*

The Fourth Amendment protects the rights of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV; *see, e.g.*, *United States v. Ramirez*, 523 U.S. 65, 71 (1998). A search occurs when the Government acquires information by either "physically intruding on persons, houses, papers, or effects," or otherwise invading an area in which the individual has a reasonable expectation of privacy. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (internal quotation mark omitted); *see also Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). A seizure occurs when the Government interferes in some meaningful way with the individual's possession of property. *United States v. Jones*, 132 S. Ct. 945, 951 n.5 (2012). Subject to limited

exceptions,[7] a search or seizure conducted without a warrant is presumptively unreasonable. *See Kyllo v. United States*, 533 U.S. 27, 31 (2001).

We must construe the Fourth Amendment "in [] light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens." *Kyllo,* 533 U.S. at 40. Applying 18th Century notions about searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the "computer age" against Fourth Amendment frameworks crafted long before this technology existed.[8] As we do so, we must keep in mind that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Missouri v. McNeely*,

---

[7] In this case, the Government has conceded that it needed a warrant to search the non-responsive computer files in its possession and has not argued that any exceptions apply.

[8] *See generally United States v. Jones*, 132 S. Ct. 945 (2012) (considering whether placing GPS tracking unit on vehicle constitutes search); *Kyllo*, 533 U.S. at 27 (determining whether use of thermal imaging constitutes search); *United States v. Aguiar*, 737 F.3d 251 (2d Cir. 2013) (determining whether warrantless placement of GPS tracking unit on vehicle fell within good-faith exception to exclusionary rule); *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) (analyzing whether warrant to search computer satisfies particularity requirement); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005); James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809 (2011); Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 Fordham Urb. L.J. 977 (2009).

133 S. Ct. 1552, 1569 (2013) (Roberts, C.J., concurring in part and dissenting in part) (internal quotation marks omitted). Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools.

"The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)) (internal quotation marks omitted). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013). The British Crown had long used these questionable instruments to enter a political opponent's home and seize all his books and papers, hoping to find among them evidence of criminal activity. *See Stanford v. Texas*, 379 U.S. 476, 482-83 (1965). The Framers abhorred this practice, believing that "papers are often the dearest property a man can have" and that permitting the Government to "sweep away all papers whatsoever," without any legal justification, "would destroy all the comforts of society." *Entick v. Carrington*, 95 Eng. Rep. 807, 817-18 (C.P. 1765).[9]

---

[9] The Supreme Court has explained that *Entick* was "undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate

The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin*, 720 F.3d at 445. The latter requirement, in particular, "makes general searches . . . impossible" because it "prevents the seizure of one thing under a warrant describing another." *Id.* at 446 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)) (internal quotation marks omitted). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant. *See Horton v. California*, 496 U.S. 128, 140 (1990); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982). Certain exceptions have been made in those "comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site." *Tamura*, 694 F.2d at 595-96. But in those cases, the off-site review had to be monitored by a neutral magistrate and non-responsive documents were to be returned after the relevant items were identified. *Id.* at 596-97.

These Fourth Amendment protections apply to modern computer files. Like 18th Century "papers," computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater

---

expression of constitutional law with regard to search and seizure." *Jones*, 132 S. Ct. at 949 (internal quotation marks omitted).

protection is warranted. *See, e.g.*, *Galpin*, 720 F.3d at 446 ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs . . . ."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

Not surprisingly, the ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants. It is "comparatively" commonplace for files on a computer hard drive to be "so intermingled that they cannot feasibly be sorted on site." *Tamura*, 694 F.2d at 595. As evidenced by this case, forensic analysis of electronic data may take months to complete. It would be impractical for agents to occupy an individual's home or office, or seize an individual's computer, for such long periods of time. It is now also unnecessary. Today, advancements in technology enable the Government to create a mirror image of an individual's hard drive, which can be searched as if it were the actual hard drive but without interfering with the individual's use of his home, computer, or files.

In light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for off-site review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be. Indeed, the 2009 amendments to the Federal Rules of Criminal Procedure, which added Rule 41(e)(2)(B), clearly contemplated off-site review of computer hard drives in certain circumstances.[10] Although Rule 41(e)(2)(B) was not in effect in 2003, when the warrant was executed with respect to Ganias's computers, case law both before and after the rule's adoption has recognized that off-site review of seized electronic files may be necessary and reasonable. *See, e.g.*, *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. Hill*, 459 F.3d 966, 976-77 (9th Cir. 2006); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

The off-site review of these mirror images, however, is still subject to the rule of reasonableness. *See, e.g.*,

---

[10] Rule 41(e)(2)(B) provides:

> **Warrant Seeking Electronically Stored Information.** A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B).

Ramirez, 523 U.S. at 71 ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)). The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's notes to the 2009 Amendments. The committee noted that several variables -- storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload -- influence the duration of a forensic analysis and counsel against a "one size fits all" time period. *Id.* In combination, these factors might justify an off-site review lasting for a significant period of time. They do not, however, provide an "independent basis" for retaining any electronic data "other than [those] specified in the warrant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (en banc).

Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. *United States v. Julius*, 610 F.3d 60, 66 (2d Cir. 2010). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). Suppression is required "only when

[agents] (1) . . . effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal quotation marks and citations omitted).

The Government effects a "widespread seizure of items" beyond the scope of the warrant when the Government' s search "resemble[s] a general search." *Id.* at 140-41. Government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate precedent." *Davis v. United States*, 131 S. Ct. 2419, 2423-24 (2011). When Government agents act on "good-faith reliance [o]n the law at the time of the search," the exclusionary rule will not apply. *United States v. Aguiar*, 737 F.3d 251, 259 (2d Cir. 2013). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance." *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012) (internal quotation marks omitted).

Furthermore, evidence will be suppressed only where the benefits of deterring the Government's unlawful actions appreciably outweigh the costs of suppressing the evidence -- "a high obstacle for those urging . . . application" of the rule. *Herring*, 555 U.S. at 141; *see Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998) (citing *United States v. Payner*, 447 U.S. 727, 734 (1980)). "The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free -- something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *United States v. Leon*, 468 U.S. 897, 908 (1984)).

2. *Analysis*

This case presents a host of challenging issues, but we need not address them all. The parties agree that the personal financial records at issue in this appeal were not covered by the 2003 warrant, and that they had been segregated from the responsive files by December 2004, before the Government began to suspect that Ganias was personally involved in any criminal activity. Furthermore, on appeal, Ganias does not directly challenge the Government's practice of making mirror images of computer hard drives when searching for electronic data, but rather challenges the reasonableness of its off-site review. Accordingly, we need not address whether: (1) the description of the computer files to be seized in the 2003 warrant was stated with sufficient particularity, *see, e.g.*, *Galpin*, 720 F.3d at 449-50; (2) the 2003 warrant authorized the Government to make a mirror image of the entire hard drive so it could search for relevant files off-site; or (3) the resulting off-site sorting process was unreasonably long.

Instead, we consider a more limited question: whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. We hold that it does not.

If the 2003 warrant authorized the Government to retain all the data on Ganias's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general warrant. The Government's retention of copies of Ganias's personal computer

records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled the Government to possess indefinitely personal records of Ganias that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganias's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment. *See United States v. Place*, 462 U.S. 696, 708 (1983) (detaining a traveler's luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure); *see also Soldal v. Cook Cnty.*, 506 U.S. 56, 62-64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched and the owner's privacy was never violated); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.").

We conclude that the unauthorized seizure and retention of these documents was unreasonable. The Government had no warrant authorizing the seizure of Ganias's personal records in 2003. By December 2004, these documents had been separated from those relevant to the investigation of American Boiler and IPM. Nevertheless, the Government continued to retain them for another year-and-a-half until it finally developed probable cause to search and seize them in 2006. Without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias's Fourth Amendment rights by

retaining the files for a prolonged period of time and then using them in a future criminal investigation.

The Government offers several arguments to justify its actions, but none provides any legal authorization for its continued and prolonged possession of the non-responsive files. First, it argues that it must be allowed to make the mirror image copies as a matter of practical necessity and, according to the Government's investigators, those mirror images were "the government's property." As explained above, practical considerations may well justify a reasonable accommodation in the manner of executing a search warrant, such as making mirror images of hard drives and permitting off-site review, but these considerations do not justify the indefinite retention of non-responsive documents. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1171. Without a warrant authorizing seizure of Ganias's personal financial records, the copies of those documents could not become *ipso facto* "the government's property" without running afoul of the Fourth Amendment.

Second, the Government asserts that by obtaining the 2006 search warrant, it cured any defect in its search of the wrongfully retained files. But this argument "reduces the Fourth Amendment to a form of words." *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920). In *Silverthorne*, the Government, "without a shadow of authority[,] went to the office of [the defendants'] company and made a clean sweep of all the books, papers and documents found there." *Id.* at 390. The originals were eventually returned because they were unlawfully seized, but the prosecutor had made "[p]hotographs and copies of material papers"

and used these to indict the defendants and obtain a subpoena for the original documents. *Id.* at 391. Justice Holmes succinctly summarized the Government's argument supporting the constitutionality of its actions as follows:

> [A]lthough of course its seizure was an outrage which the Government now regrets, it may study the papers before it returns them, copy them, and then may use the knowledge that it has gained to call upon the owners in a more regular form to produce them; that the protection of the Constitution covers the physical possession but not any advantages that the Government can gain over the object of its pursuit by doing the forbidden act.

Id. Unsurprisingly, the Supreme Court rejected that argument: "The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all" unless some exception applies.[11] *Id.* at 392. The same rationale

---

[11] The Supreme Court has abrogated *Silverthorne*'s broad proposition that wrongfully acquired evidence may "not be used at all." *See United States v. Havens*, 446 U.S. 620, 624-25 (1980) (noting that this evidence may be used for purposes of impeachment); *see also Murray v. United States*, 487 U.S. 533, 537 (1988) (explaining that the "independent source" doctrine allows the admission of "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality"); *Nix v. Williams*, 467 U.S. 431, 444 (1984) (explaining that "inevitable discovery" doctrine permits the admission of unlawfully obtained evidence if "th[at] information ultimately or inevitably

applies here. If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant.

Third, the Government argues that it must be permitted to search the mirror images in its possession because the evidence no longer existed on Ganias's computers. But the ends, however, do not justify the means. The loss of the personal records is irrelevant in this case because the Government concedes that it never considered performing a new search of Ganias's computers and did not know that the files no longer existed when it searched the mirror images in its possession. And even if it were relevant, the Fourth Amendment clearly embodies a judgment that some evidence of criminal activity may be lost for the sake of protecting property and privacy rights. *See, e.g.*, *United States v. Calandra*, 414 U.S. 338, 361 (1974) ("The judges who developed the exclusionary rule were well aware that it embodied a judgment that it is better for some guilty persons to go free than for the [Government] to behave in forbidden fashion.").

Fourth, the Government contends that returning or destroying the non-responsive files is "entirely impractical" because doing so would compromise the

---

would have been discovered by lawful means"). The Government does not rely on any of these exceptions here. Indeed, it concedes that if it "had not preserved that data from the November 2003 seizure, it would have been lost forever." Appellee's Br. at 33. We do not hold that the Government has waived its right to use the evidence in question for impeachment purposes.

remaining data that was responsive to the warrant, making it impossible to authenticate or use it in a criminal prosecution. Appellee Br. at 34. We are not convinced that there is no other way to preserve the evidentiary chain of custody. But even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose.

Finally, the Government argues that Ganias's failure to bring a motion for the return of property, pursuant to Federal Rule of Criminal Procedure 41(g), precludes him from seeking suppression now. Although the district court accepted this argument, we find no authority for concluding that a Rule 41(g) motion is a prerequisite to a motion to suppress. *See* Fed. R. Crim. P. 41(g) ("A person aggrieved . . . *may* move for the property's return." (emphasis added)); Fed. R. Crim. P. 41(h) ("A defendant *may* move to suppress evidence . . . ." (emphasis added)). Imposing such a prerequisite makes little sense in this context, where Ganias still had the original computer files and did not need the Government's copies to be returned to him. Moreover, we fail to see what purpose a Rule 41(g) motion would have served, given the Government's position that non-responsive files in its possession could not feasibly have been returned or purged anyway.

Because the Government has demonstrated no legal basis for retaining the non-responsive documents, its retention and subsequent search of those documents were unconstitutional. The Fourth Amendment was intended to prevent the Government from entering individuals' homes and indiscriminately seizing all

their papers in the hopes of discovering evidence about previously unknown crimes. *See Entick*, 95 Eng. Rep. at 817-18; *see also Jones*, 132 S. Ct. at 949. Yet this is exactly what the Government claims it may do when it executes a warrant calling for the seizure of particular electronic data relevant to a different crime. Perhaps the "wholesale removal" of intermingled computer records is permissible where off-site sorting is necessary and reasonable, *Tamura*, 694 F.2d at 595-97, but this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations. *See Comprehensive Drug Testing,* 621 F.3d at 1171.

We turn now to the application of the exclusionary rule. As discussed above, suppression is required when (1) there is a widespread seizure of items not covered by the warrant and (2) agents do not act in good faith. *United States v. Shi Yan Liu*, 239 F.3d 138, 141 (2d Cir. 2000). There must also be a weighing of (3) the benefits of deterrence against (4) the costs of suppression. *Herring v. United States*, 555 U.S. 135, 141 (2009).

First, as we set forth above, the Government effected a widespread seizure of files beyond the scope of the warrant -- conduct that resembled an impermissible general search. *Shi Yan Liu*, 239 F.3d at 141. For almost two-and-a-half years, the Government retained records that were beyond the scope of the 2003 warrant, in violation of Ganias's Fourth Amendment rights.

Second, the agents here did not act in good faith. Government agents act in good faith when they conduct

searches in objectively reasonable reliance on binding appellate precedent. *Davis v. United States*, 131 S. Ct. 2419, 2423-24 (2011). It is the Government's burden -- not Ganias's -- to demonstrate the objective reasonableness of the officers' good faith reliance. *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012). We are not persuaded that the agents in this case reasonably concluded that the 2003 warrant authorized their search of Ganias's personal records and their retention for more than two years. The agents acknowledged, at least initially, that the Government was obliged to "purge[]" the non-responsive data after they completed their search for relevant files. The record also makes clear that Government investigators "viewed the data as the government's property" and intentionally retained Ganias's records for future use. This clearly was not reasonable, and the agents could not have had a good-faith basis to believe the law permitted them to keep the non-responsive files indefinitely.

Third, the benefits of deterrence in this case are great. With the Government's use of forensic mirror images becoming increasingly common, deterring its unconstitutional handling of non-responsive data has grown in importance. The substantial deterrence value in this case is clear when compared to *Davis*, 131 S. Ct. at 2419. In *Davis*, there was no deterrence value because the police officers conducted their search in compliance with appellate precedent at the time. While Davis's appeal was pending in the Eleventh Circuit, the Supreme Court overruled that precedent. There was no cause to deter unlawful Government conduct because the conduct was lawful when it occurred. That is not the situation here. In this case, the Government's

handling of Ganias's personal records violated precedent at the time of the search, and relevant Fourth Amendment law has not fundamentally changed since.

Finally, the costs of suppression are minimal here. This is not a case where a dangerous defendant is being set free. *See Herring v. United States*, 555 U.S. 135, 144 (2009) ("The principal cost of applying the [exclusionary] rule is, of course, letting [a] guilty and possibly dangerous defendant[] go free."). Even assuming Ganias committed tax evasion -- a serious matter -- this case does not involve drugs, guns, or contraband. Nor is this a case where police officers happened upon guns or drugs or other evidence they otherwise could not have found. Rather, early on, the evidence here was readily obtainable by subpoena or search warrant. Moreover, when guns or drugs are suppressed, that evidence is usually irreplaceable. The records here, however, conceivably are available elsewhere as hard copies or can be reconstructed from other records. As made clear by the Government's behavior, the costs of suppression that the Government has asserted are outweighed by the benefits of deterring future misconduct.

Accordingly, we reverse the denial of the motion to suppress and vacate the judgment of conviction.

CONCLUSION

We conclude that the Government violated Ganias's Fourth Amendment rights by seizing and indefinitely retaining non-responsive computer records, and then searching them when it later developed probable cause. Accordingly, Ganias's personal records, seized in the

execution of the November 2003 warrant and retained for two-and-a-half years, should have been suppressed. For the reasons stated above, we REVERSE the district court's denial of the motion to suppress, VACATE the judgment of conviction, and REMAND for further proceedings not inconsistent with this opinion.

PETER W. HALL, Circuit Judge, concurring in part and dissenting in part:

While I concur with my two colleagues that holding onto non -responsive documents for an extended period of time without some independent basis for retention represents an unreasonable seizure for purposes of the Fourth Amendment, I respectfully dissent from that portion of the opinion which holds that in this case the evidence should be suppressed.

The exclusionary rule is a deterrent sanction created by the Supreme Court to bar[ ] the prosecution from introducing evidence obtained by way of a Fourth Amendment violation. *Davis v. United States*, 564 U.S. 1---, 131 S.Ct. 2419, 2423 (2011). The Supreme Court has cautioned, however, that "exclusion [should be] 'our last resort, not our first impulse.'" *Herring v. United States*, 555 U.S. 135, 140 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). This is so because the rule is "'not a personal constitutional right,' nor is it designed to 'redress the injury' occasioned by an unconstitutional search[,] . . . [its] sole purpose . . . is to deter future Fourth Amendment violations." *Davis*, 131 S.Ct. at 2426 (citations omitted). The rule specifically deters "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id*. In general, "searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule . . . . [as] the harsh sanction of

exclusion 'should not be applied to deter objectively reasonable law enforcement activity.'" *Davis*, 131 S.Ct. at 2423-24, 2429 (citation omitted).

In this case, I cannot agree with the majority's determination that the Government acted in bad faith. The documents were seized pursuant to a warrant and the non-responsive documents were culled and segregated. While testimony reveals that the Government mistakenly considered the mirror images it created of the non-responsive documents as its own property, there was little caselaw either at the time of the search or in the following years to indicate that the Government could not hold onto the non-responsive material in the way it did. Where caselaw existed, the Government complied with the guidelines for the seizure and offsite search of large amounts of documents. *See United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) (noting that "[i]n the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site," the Government may seize items outside the scope of the warrant under certain conditions). What is more, the Government scrupulously avoided reviewing files that it was not entitled to review before obtaining the 2006 search warrant.

With respect to the balancing between deterrence and the cost of suppression, because the Government's actions did not violate established precedent at the time of the search, I do not perceive a need for deterrence. "[A]ll that exclusion would deter in this case is conscientious police work." *Davis*, 131 S.Ct. at 2429. Additionally, as Ganias himself stated, the evidence to be suppressed in this case would not have

existed but for the Government's retention of the non-responsive materials. The evidence to be suppressed is thus, contrary to the majority's conclusion, of the same irreplaceable nature as guns or drugs. Moreover, in light of the serious and nefarious effects of money fraud crimes on society, *see, e.g.*, *United States v. Madoff*, No. 09 Crim. 213(DC), 2009 WL 3347945 (S.D.N.Y. Oct. 13, 2009), I am loathe to conclude that guns, drugs and/or contraband are the only indicia of a dangerous defendant. Accordingly, while I agree that the Government violated the defendant's Fourth Amendment rights to be free from an unreasonable seizure because it held for a prolonged period of time mirror images of computer generated records that were not responsive to the 2003 search warrant without returning them (or destroying them), I see no reason to suppress the evidence derived therefrom under the circumstances presented.

APPENDIX D

AO245b (USDC-CT Rev. 9/07)

UNITED STATES DISTRICT COURT
District of Connecticut

CASE NO. 3:08cr224-2
USM NO: 17707-014

[Filed January 18, 2012]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
STAVROS M. GANIAS	)
a/k/a STEVE GANIAS	)
	)

JUDGMENT IN A CRIMINAL CASE

Anastasia King / Calvin Kurimai
Assistant United States Attorneys

ROBERT LACOBELLE
Defendant's Attorney

THE DEFENDANT: was found guilty by jury verdict as to Count 4 and Count 5 of the Superseding Indictment

Accordingly the defendant is adjudicated guilty of the following offenses:

Title & Section	Nature of Offense	Offense Concluded	Count(s)
26 USC 7201	Attempt to evade or defeat tax; tax evasion	January 1, 2003	4s
26 USC 7201	Attempt to evade or defeat tax; tax evasion	January 1, 2003	5s

The following sentence is imposed pursuant to the Sentencing Reform Act of 1984.

IMPRISONMENT
The defendant is hereby committed to the custody of the United States Bureau of Prisons to be **imprisoned for a total of 24 months** on count 4s and 24 months on count 5s of the superseding indictment which shall run concurrently.

SUPERVISED RELEASE
Upon release from imprisonment, the defendant shall be placed on **supervised release for a total term of 36 months**. The Mandatory and Standard Conditions of Supervised Release as attached, are imposed. In addition, the following Special Conditions are imposed:

1. The defendant shall not incur new credit card charges or open additional lines of credit without the United States Probation Office's (USPO) permission until criminal defendants' obligation is paid.

2. The defendant shall provide the USPO with access to requested financial information.
3. The defendant shall not possess a firearm or dangerous weapon of any kind.

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments as follows:

Special Assessment:	$200.00	Received on January 6, 2012 by the Clerk's Office
Restitution:	$69,842.00	To be paid at the rate of $500.00 per month. Payment should be made to the Clerk's Office which will then be forwarded to the following address: IRS Attn: MPU Stop 151 Restitution P.O. Box 47-421 Doraville, GA 30362

It is further ordered that the defendant will notify the United States Attorney for this district within 30 days of any change of name, residence or mailing address until all fines, restitution, costs and special assessments imposed by this judgment, are paid.

Counts 1,4, and 5 of the Indictment and Counts 1 and 3 of the Superseding Indictment are dismissed on motion of the United States.

JUDICIAL RECOMMENDATION(S) TO THE BUREAU OF PRISONS

The Court recommends that the Defendant be incarcerated at FCI Camp Cannan located in PA.

The Defendant Shall Surrender to the Institution Designated by the Bureau of Prisons on February 8th at 10:00am

January 5, 2012
Date of Imposition of Sentence

/s/
Ellen Bree Burns
Senior United States District Judge
Date: 1/17/12

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____ a _____ , with a certified copy of this judgment.

_____
Joseph P. Faughnan
United States Marshal

By _____
Deputy Marshal

CERTIFIED AS A TRUE COPY
ON THIS DATE _____
ROBERTA D. TABORA, Clerk
BY: _____
Deputy Clerk

CONDITIONS OF SUPERVISED RELEASE

In addition to the Standard Conditions listed below, the following indicated (■) Mandatory Conditions are imposed:

MANDATORY CONDITIONS

■ (1) The defendant shall not commit another federal, state or local offense;

■ (2) The defendant shall not unlawfully possess a controlled substance;

□ (3) The defendant who is convicted for a domestic violence crime as defined in 18 U.S.C. section 3561(b) for the first time shall attend a public, private, or private non-profit offender rehabilitation program that has been approved by the court, in consultation with a State Coalition Against Domestic Violence or other appropriate experts, if an approved program is available within a 50-mile radius of the legal residence of the defendant;

□ (4) The defendant shall refrain from any unlawful use of a controlled substance and submit to one drug test within 15 days of release on supervised release and at least two periodic drug tests thereafter for use of a controlled substance;

□ (5) If a fine is imposed and has not been paid upon release to supervised release, the defendant shall adhere to an installment schedule to pay that fine;

■ (6) The defendant shall (A) make restitution in accordance with 18 U.S.C. sections 2248, 2259, 2264, 2327, 3663, 3663A, and 3664;

and (B) pay the assessment imposed in accordance with 18 U.S.C. section 3013;

□ (7) (A) In a state in which the requirements of the Sex Offender Registration and Notification Act (see 42 U.S.C. §§ 16911 and 16913) do not apply, a defendant convicted of a sexual offense as described in 18 U.S.C. § 4042(c)(4) (Pub. L. 105-119, § 115(a)(8), Nov. 26, 1997) shall report the address where the defendant will reside and any subsequent change of residence to the probation officer responsible for supervision, and shall register as a sex offender in any State where the person resides, is employed, carries on a vocation, or is a student; or

(B) In a state in which the requirements of Sex Offender Registration and Notification Act apply, a sex offender shall (i) register, and keep such registration current, where the offender resides, where the offender is an employee, and where the offender is a student, and for the initial registration, a sex offender also shall register in the jurisdiction in which convicted if such jurisdiction is different from the jurisdiction of residence; (ii) provide information required by 42 U.S.C. § 16914; and (iii) keep such registration current for the full registration period as set forth in 42 U.S.C. § 16915;

■ (8) The defendant shall cooperate in the collection of a DNA sample from the defendant.

While on supervised release, the defendant shall also comply with all of the following Standard Conditions:

STANDARD CONDITIONS

(1) The defendant shall not leave the judicial district or other specified geographic area without the permission of the court or probation officer;
(2) The defendant shall report to the probation officer in a manner and frequency directed by the court or probation officer;
(3) The defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
(4) The defendant shall support the defendant's dependents and meet other family responsibilities (including, but not limited to, complying with the terms of any court order or administrative process pursuant to the law of a state, the District of Columbia, or any other possession or territory of the United States requiring payments by the defendant for the support and maintenance of any child or of a child and the parent with whom the child is living);
(5) The defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other acceptable reasons;

(6) The defendant shall notify the probation officer at least ten days prior to any change in residence or employment, or if such prior notification is not possible, then within five days after such change;

(7) The defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance, or any paraphernalia related to any controlled substance, except as prescribed by a physician;

(8) The defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered, or other places specified by the court;

(9) The defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer;

(10) The defendant shall permit a probation officer to visit the defendant at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view by the probation officer;

(11) The defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;

(12) The defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court;

(13) The defendant shall pay the special assessment imposed or adhere to a court-ordered

installment schedule for the payment of the special assessment;

(14) The defendant shall notify the probation officer of any material change in the defendant's economic circumstances that might affect the defendant's ability to pay any unpaid amount of restitution, fines, or special assessments.

The defendant shall report to the Probation Office in the district to which the defendant is released within 72 hours of release from the custody of the U.S. Bureau of Prisons. Upon a finding of a violation of supervised release, I understand that the court may (1) revoke supervision and impose a term of imprisonment, (2) extend the term of supervision, and/or (3) modify the conditions of supervision.

These conditions have been read to me. I fully understand the conditions and have been provided a copy of them.

(Signed)_____ _____
Defendant **Date**

_____ _____
U.S. Probation Officer/ Designated Witness **Date**

APPENDIX E

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

CASE NO. 3:08CR00224(AWT)

[Filed June 24, 2011]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
STAVROS M. GANIAS	)
	)

RULING ON MOTION TO SUPPRESS EVIDENCE

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 contract was re-bid and IPM lost the contract, but before November 17, 2003, the contract was 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 was operated by 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.

The warrants authorized the seizure from all three locations 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

---

[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

CCIU Agents chose to make mirror images 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

---

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.

disguised through encryption of the data or by simply renaming a file to have a different extension.[2]

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.

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,

---

[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.

[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.

along with a copy of one of the search warrants. The Criminal Investigation Laboratory's duty was to review the computer data for information that was generally 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 case agent for Army CID. In early May 2004, the IRS was officially authorized to join the investigation. At that

[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.

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.

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 Paukstelis until she received the DVDs at the end of June, and 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 she nor Conner looked at any QuickBooks files 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 to use her computer to browse the files on the 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.

Around November 30, 2004, McEachern provided Hosney with 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 issued by a magistrate judge.

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 computer data set forth in United States v. Comprehensive Drug Testing, 579 F.3d 989, 1006-07 (9th 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 in Comprehensive 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 property pursuant to Federal Rule of Criminal Procedure 41(g). The present case, by contrast, involves a motion to suppress evidence. The significance of this distinction is highlighted by the Ninth Circuit's opinion in United 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.

Because of the timing of the decision and the procedural posture, Tamura is the more relevant case in assessing the reasonableness of the agents' actions in the present case. The 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

---

[5] The court did note that the case was a close one. See id. In Tamura, however, as in one of the orders addressed in Comprehensive 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.

> removal must be monitored by the judgment of a neutral, detached magistrate.[6]

Id. at 595-96.

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 outside of a file cabinet for the 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;

---

[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.

> (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. Comprehensive Drug Testing, 579 F.3d at 1006. As noted above, the opinion in 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 states that "[t]he government must destroy or, if the recipient may lawfully possess it, return 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 2003 Warrant. Cf. United States v. 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 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 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 images" of the hard drives 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 imposed upon them in the 2003 Warrant. It would require a hypertechnical 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) (quoting United 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.

Signed this 24th day of June, 2011 at Hartford, Connecticut.

/s/AWT
Alvin W. Thompson
United States District Judge