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

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term 2015

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

No. 12-240-cr

UNITED STATES OF AMERICA,

Appellee,

-v.-

STAVROS M. GANIAS,

Defendant-Appellant.

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,

[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.

and Taxes International for evidence of criminal 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

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

protocols were permitted.[3] The warrant authorized seizure of all hardware relevant to the alleged crimes.[4]

---

[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;
> (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

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

---

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).

[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.

copies of his three hard drives had been created and taken off-site.[6] There is no dispute that the forensic 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.

---

[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 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

[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).

began to analyze the non-digital files seized pursuant to the warrant. These files suggested that IPM had made payments to a third 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

[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.

"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.

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

[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.

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]

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

[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.

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*,

[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.

No. 3:08cr224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 1. 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 with Taxes International.[15] Instead, Agent Hosney subpoenaed Ganias's bank records from 1999 to 2003 and accessed his income

[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.

[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.

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 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

[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.

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

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

[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.

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

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

---

> (2) Considering all relevant factors, whether the 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.).

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 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

[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

government 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 that contains data that, as here, cannot feasibly be

---

'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. 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))).

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 mirrored drives — including storing one

[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.

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

[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.

documents violated the Fourth Amendment.[25] *Id.* at 595, 597; *see also Andresen 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

[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.

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 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

[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.

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 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

[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 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").

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.

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

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*

---

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

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), 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

[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?").

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 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]

---

[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 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

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

---

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-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.

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 preservation of data, moreover, is not simply a concern for law enforcement.

[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 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.

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 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]

---

[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 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

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 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] Nor do we gainsay the privacy concerns implicated when the

---

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).

[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

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

---

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 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.

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]

[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 "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.

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

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

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

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 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

[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 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.

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 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]

[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

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 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

---

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.

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

---

[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 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.

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

---

[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.

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 (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 investigation, J.A. 461, ¶ 3; that, "[p]ursuant to [that initial warrant]," Agent Hosney could not search Ganias's personal or business files as

[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.

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

[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

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.

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.

---

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.

* * *

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.