CHIN, *Circuit Judge*, dissenting:

I respectfully dissent.

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

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

Id. at 1066.

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

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

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

---

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

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

---

services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

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

I disagree. I would hold, as the panel held unanimously, that the Government violated Ganias's Fourth Amendment rights when it retained Ganias's non-responsive files for nearly two-and-a-half years and then reexamined the files for evidence of additional crimes. *United States v. Ganias*, 755 F.3d 125, 133-40 (2d Cir. 2014). I would also hold, as two members of the panel did, that the Government's actions are not excused by the good faith exception. *Id.* at 140-41. *But see id.* at 141 (Hall, *J.*, dissenting in part).[3] Accordingly, I dissent.

I.

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

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

as well as eight *amicus* briefs,[4] the Court declines to rule on the question, "offer[ing] no opinion on the existence of a Fourth Amendment violation in this case." *Id.* at 22. I would reach the question, and I would hold, as did the panel, that the Fourth Amendment was indeed violated.[5]

---

[4] All eight *amici* urged that we find a Fourth Amendment violation. Brief for *Amicus Curiae* Center for Constitutional Rights as *Amicus Curiae* in Support of Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597942; Brief for *Amici Curiae* Center for Democracy & Technology, ACLU, et al. in Support of Defendant-Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597943; Brief of *Amici Curiae* Electronic Privacy Information Center in Support of Appellant and Urging Affirmance, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4610149; Brief on Rehearing *En Banc* for *Amici Curiae* Federal Public Defenders Within the Second Circuit in Support of Appellant Stavros M. Ganias, No. 12-240-cr (July 29, 2015), 2015 WL 4597956; Brief of Google Inc. as Amicus Curiae Supporting Defendant-Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597960; *Amicus Curiae* Brief of the National Ass'n of Criminal Defense Lawyers in Support of Defendant-Appellant and Urging Reversal , *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597959; Brief for *Amicus Curiae* New York Council of Defense Lawyers in Support of Appellant, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597958; Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Defendant-Appellant Stavros M. Ganias, *Ganias*, No. 12-240-cr (July 29, 2015), 2015 WL 4597961.

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

A.

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

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

---

recognized the importance of the particularity requirement in the context of electronic evidence," but arguing that the panel could have "issued a narrower opinion"). *But see* Note, *Digital Duplications and the Fourth Amendment*, 129 Harv. L. Rev. 1046, 1059-64 (2016) (arguing the retention at issue should have been considered as a "search" and not a "seizure"). Others have likewise commented that the panel opinion fits with current Supreme Court jurisprudence, including, in particular, *Riley v. California*, 134 S. Ct. 1473. *E.g.*, Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 112-13 (2014) ("The rule adopted in *Ganias* is consistent with the scope of privacy interests in digital data outlined in *Riley*, and other courts will be more likely to adopt the rule in light of the Supreme Court's decision."); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117, 238-41 (2015) (commenting that, like the panel opinion, *Riley* "similarly supports a Fourth Amendment use restriction on lawfully obtained information" and concluding that "[e]ven though the government might have legally obtained the information at the front end, it could not search the information for evidence of criminal activity absent a warrant, supported by probable cause"); Paul Ohm, *The Life of* Riley *(*v. California*)*, 48 Tex. Tech L. Rev. 133, 138-39 (2015) (anticipating that future courts could find *Ganias* supportable under *Riley*).

J. App. 433. Two Army computer specialists and another Army investigator came to Ganias's office, and they saw three computers. They made identical copies of the hard drives of those computers to take with them -- that is, they cloned the hard drives by making exact replicas ("mirror images") on blank hard drives. In the course of doing so, they took data and files *not* "relating to the business, financial and accounting operations of [IPM] and American Boiler." *Id.* In fact, they took from those hard drives *all* of Ganias's data, including files relating to his personal affairs.

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

By December 2004, approximately thirteen months after the seizure, some four months of which was spent locating a copy of the off-the-shelf

consumer software known as QuickBooks, Army and IRS investigators were able to isolate and extract the files covered by the warrant, that is, the files relating to IPM and American Boiler. The investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records. Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.

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

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

normally go into electronic data and start deleting evidence off of DVDs stored in my evidence room." *Id.* at 122.

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

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

believe that she could review the non-responsive files, even though they were already in the Government's possession.

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

B.

"[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). In adopting the Fourth Amendment, the Framers were principally concerned about "indiscriminate searches and seizures" conducted "under the authority of 'general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King*, 133 S. Ct. 1958,

1980 (2013). The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin*, 720 F.3d at 445-46.

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

to be monitored by a neutral magistrate and non-responsive documents were to be returned after the relevant items were identified. *Id.* at 596-97.

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

But these practical necessities must still be balanced against our possessory and privacy interests, which have become more susceptible to

deprivation in the computer age. A computer does not consist simply of "papers," but now contains the quantity of information found in a person's residence or greater. *See Riley v. California*, 134 S. Ct. 2473, 2489 (2014); *Galpin*, 720 F.3d at 446. Virtually the entirety of a person's life may be captured as data: family photographs, correspondence, medical history, intimate details about how a person spends each passing moment of each day. GPS-enabled devices reveal our whereabouts. A person's internet search history may disclose her mental deliberations, whether or not those thoughts were favored by the Government, the public at large, or even that person's own family. Smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 134 S. Ct. at 2489; *see also* Michael D. Shear, David E. Sanger & Katie Benner, *In the Apple Case, a Debate Over Data Hits Home*, N.Y. Times (Mar. 13, 2016) ("It is a minicomputer stuffed with every detail of a person's life: photos of children, credit card purchases, texts with spouses (and nonspouses), and records of physical movements."). From a mere data storage device, a forensic analyst could reconstruct a "considerable chunk of a person's life." Kerr, *supra* note 1, at 569.

All of this information is captured when the Government, in executing a search warrant, makes a mirror image of a hard drive.

We know only general descriptions of what was in Ganias's three hard drives -- "personal and financial information," including information on other tax and accounting clients (*e.g.*, social security numbers) that was private to them -- but the Fourth Amendment requires us to consider broadly the ramifications of computer seizures. J. App. 428. If Ganias were a doctor, his computer might have contained the entire medical history of hundreds of individuals. If Ganias were a teacher, his computer could have contained educational information on dozens of students and communications with their families. If Ganias were not an individual but a corporation like Apple, Dropbox, Google, or Microsoft that stores individuals' information in the "cloud," the Government would have captured an untold vastness of information on millions of individuals. *See* Jim Kerstetter, *Microsoft Goes on Offensive Against Justice Department*, N.Y. Times (Apr. 15, 2016) ("When customer information is stored in a giant data center run by companies like Google, Apple and Microsoft, investigators can go straight to the information they need, even getting a judge to order the company to keep quiet about it."); *see also* Andrew Keane Woods,

Against Data Exceptionalism, 68 Stan. L. Rev. 729, 743 (2016) ("Twenty years ago, a kidnapper might have confessed to a crime by writing in his diary. . . . Today the same admission is just as likely to be stored online. . . .").

To safeguard individuals' possessory and privacy interests, when the Government seeks to review mirror images off-site, we are careful to subject the Government's conduct to the rule of reasonableness. *See, e.g.*, *United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)). The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's notes to 2009 amendments. The committee noted that several variables -- storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload -- influence the duration of a forensic analysis and counsel against a "one size fits all" time period. *Id.* In combination, these factors

might justify an off-site review lasting for a significant period of time. They do not, however, provide an "independent basis" for retaining any electronic data "other than [those] specified in the warrant." *United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1171 (9th Cir. 2010) (*en banc*) (*per curiam*).

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

But once the Government is able to extract the responsive documents, its right to the overseizure of evidence comes to an end. This obvious principle has long been adhered to in the context of physical documents, such as when the Government seizes entire file cabinets for off-site review. *See Tamura*, 694 F.2d at 596-97 ("We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper."); *see also Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("[T]o the extent such papers were not within the scope of the warrants or were otherwise improperly

seized, the State was correct in returning them voluntarily . . . ."). By logical extension, at least in a situation where responsive computer files can be extracted without harming other government interests, this principle would apply with equal force. *See CDT*, 621 F.3d at 1175-76 (using "file cabinets" as a starting analogy for analyzing digital privacy issues). Once responsive files are segregated or extracted, the retention of non-responsive documents is no longer reasonable, and the Government is obliged, in my view, to return or dispose of the non-responsive files within a reasonable period of time. *See CDT*, 621 F.3d at 1179 (Kozinski, *J.*, concurring) ("Once the data has been segregated . . . any remaining copies should be destroyed or . . . returned . . . ."). At that point, the Government's overseizure of files and continued retention of non-responsive documents becomes the equivalent of an unlawful general warrant. *See CDT*, 621 F.3d at 1176 (majority opinion) (noting "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *cf. United States v. Jones*, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, *J.*, concurring) (warning that "Government can store . . . records and efficiently mine them for information years into the future").

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

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

> There does come a point where we often identify a subset of documents that are responsive, *and you could even call it segregating*. In this case, they put them onto a

> separate disc as working copies and sent [them] to the case agents.

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

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

down the road does not defeat the rights protected by the Fourth Amendment. *Cf. Riley*, 134 S. Ct. at 2491 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

C.

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

At the outset, in evaluating the legitimacy of these reasons in relation to this case, I note what is *not* implicated here. This is not a case where the defendant's non-responsive files had independent evidentiary value -- for instance, in a prosecution where the charge was that evidence had been

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

destroyed, *e.g.*, 18 U.S.C. § 1519, it would be relevant that certain documents were *not* on the hard drive.[8] This is also not a case where the manner in which a responsive file was stored could be used to prove knowledge or intent, as might be the situation in a child pornography prosecution. And this is not a case where the physical hard drive itself is of evidentiary value -- the fact that Ganias's files were actually found inside a computer did not make his guilt more or less probable. Finally, this is not a case where the Government seized Ganias's hard drive to proceed against him. Instead, the Government retained Ganias's hard drive for some two-and-a-half years without suspecting him of criminal wrongdoing, and the agency that ultimately suspected him of illicit tax activity (the IRS) was not even involved at the outset.

The Government argues that it has the right to retain non-responsive files so that, at trial, *responsive* files will be more easily authenticated or of greater evidentiary weight. Once again, the Government's argument obscures the issues

---

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

in *this* case. The agents could not have been keeping non-responsive files for the purpose of proceeding against Ganias, as they did not yet suspect Ganias of criminal wrongdoing.

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

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

hash values would not match. Hash values thus make authentication easy. *See* Fed. R. Evid. 901(b)(4).

The hashing argument, however, is not persuasive. First, the Government would have to call an expert just to explain to a jury what a hash value was, as it did here. *See* Fed. R. Evid. 702(a); Trial Tr. 128-30. This is no less burdensome than simply having an agent testify as to the chain of custody. Second, as the Government acknowledged at rehearing *en banc*, it can hash individual files that it has segregated. *See* Oral Arg. 31:08-30. This practice is not a hypothetical possibility: the Government has done so before, *see, e.g.*, *United States v. Hock Chee Koo*, 770 F. Supp. 2d 1115, 1123 (D. Or. 2011), and the Government did so in this very case for Ganias's QuickBooks files, *see* Trial Tr. 147-54. *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 40-41 (2005) ("Many digital analysis tools can be configured to calculate separate hash values of each individual file . . . ."). The Government's ability to authenticate individual files by hashing them undercuts its assertion that it must retain non-responsive files to authenticate responsive ones. Hashing appears to make it easier for the Government to comply with the Fourth Amendment, not harder.

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

In a similar vein, the Government argues that retention of mirror images "preserves the evidentiary value of computer evidence itself" and might "refute claims . . . of data tampering." Gov't Br. 31-34. As a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image.[9] More generally, the Government can argue in every case that overseized

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

evidence will have some bearing on the "evidentiary value" of other, properly seized evidence at trial. When the Government makes authorized seizures of folders of financial information from a file cabinet, it could argue that it is entitled to seize the entire cabinet to demonstrate to a jury that folders were preserved in their original form. Or the Government might like to seize nearby, carefully organized folders of medical information to rebut a claim of incompleteness by showing how meticulous the defendant was. Or the Government might seek to seize a folder of children's report cards to show that the defendant normally kept information from a certain time period. Permitting the Government to keep non-responsive files merely to strengthen the evidentiary value of responsive files would eviscerate the Fourth Amendment.

Remarkably, the Government also argues that it should be allowed to hold on to overseized data for the *defendant's* benefit -- so that it can comply with its discovery obligations and duty to disclose exculpatory materials under *Brady*. *See generally Brady v. Maryland*, 373 U.S. 83 (1963). The Government is essentially arguing that it must hold on to the materials so that it can give them back to the defendant. Of course, this is not a genuine concern -- the problem can

be obviated simply by returning the non-responsive files to the defendant in the first place.

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

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

The Government's arguments thus fail. In my view, Ganias's Fourth Amendment rights were violated when the Government unreasonably continued

to hold on to his non-responsive files long after the responsive files had been extracted to reexamine when it subsequently saw need to do so.

II.

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

A.

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

To balance these interests, we have adopted the "good faith" exception, in certain circumstances, as a carve-out to the exclusionary rule. *See*

Davis v. United States, 564 U.S. 229, 237-39 (2011). When a warrant is present, an agent's objectively reasonable good faith reliance on and abidance by the warrant generally makes exclusion an inappropriate remedy. *See United States v. Leon*, 468 U.S. 897, 922 (1984). Likewise, government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate precedent." *Davis*, 564 U.S. at 232. When agents act in good faith, the exclusionary rule will usually not apply. *See United States v. Aguiar*, 737 F.3d 251, 259 (2d Cir. 2013). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance." *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)).

Furthermore, evidence will be suppressed only where the benefits of deterring the Government's unlawful actions appreciably outweigh the costs of suppressing the evidence -- "a high obstacle for those urging . . . application" of the rule. *Herring*, 555 U.S. at 141 (quoting *Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998)); *see Davis*, 564 U.S. at 232. "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the

resulting costs." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). "The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free -- something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908).

B.

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

(1)

I first turn to the 2003 warrant. The Government's retention of Ganias's non-responsive files pursuant to the 2003 warrant was hardly lawful or in good faith. The Government, in keeping the entirety of the mirror images, kept substantial amounts of "computer associated data" that did not "relat[e] to

the business, financial and accounting operations of [IPM] and American Boiler." J. App. 433. This sort of retention following a "widespread seizure" was not explicitly authorized by the 2003 warrant, *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (quoting *United States v. Matias*, 836 F.2d 744, 748 (2d Cir. 1988)), and, as discussed, amounted to a general search. Likewise, the Government points to no binding appellate precedent that allows it to retain files outside the scope of a warrant when the responsive files can be feasibly extracted. Instead the Fourth Amendment baseline is that the Government may not take and then *keep* papers without a warrant "particularly describing . . . the persons or things to be seized." U.S. Const. amend. IV.

The Government argues nonetheless that the agents had an objectively reasonable good faith belief that their post-warrant conduct was lawful, because no precedent held that they could *not* do what they did. The argument fails, in my view, for the precedents are absolutely clear that general warrants are unconstitutional and that government agents authorized to come into one's home to seize papers for a limited purpose may not indiscriminately seize and retain all papers instead. Any agent who professes to have the ability to do so merely because computers are involved is not acting in good faith.

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

continued retention of Ganias's non-responsive files. *See CDT*, 621 F.3d at 1179 (Kozinski, *J.*, concurring). Once the responsive files were extracted, the Government could have asked to keep non-responsive files for use during a prosecution or for the purpose of trial and allowed a magistrate to balance the Government's need against Ganias's Fourth Amendment interests. *See Leon*, 468 U.S. at 916 (noting we would not "punish the errors of judges and magistrates"). The Government did not do that, but instead retained the non-responsive files for another year and a half before seeking judicial guidance.

More troublingly, the agents here knew what they were supposed to do -- their actions were "deliberate." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). The agents *knew* they were supposed to return or delete overseized data. When asked whether he was "to return those items or destroy those items that don't pertain to your lawful authority to seize those particular items" after a "reasonable period" of off-site review, the testifying agent answered, "Yes, sir." J. App. 145-46; *see also id.* at 428 (Ganias corroborating that the agent "assured me that those materials and files not authorized under the warrant and not belonging to American Boiler and IPM would be purged once they completed their search"). Instead of following this protocol, that agent testified that the

investigators "viewed the data as the government's property, not Mr. Ganias' property." *Id.* at 146; *see also id.* at 122 ("And you never know what data you may need in the future."). In other words, the agents "knew that limits of the warrant w[ere] not be[ing] honored." *United States v. Foster*, 100 F.3d 846, 852 (10th Cir. 1996). This knowledge of the need to return or delete non-responsive files compels a conclusion that the agents did not rely in good faith on the 2003 warrant or any appellate precedent (binding or non-binding) and that the deterrence value of suppression here is substantial.

(2)

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

For the purpose of deterring Fourth Amendment violations, the relevant inquiry is whether the agents acted in good faith when they committed the violation. *See Leon*, 468 U.S. at 916 ("[T]he exclusionary rule is designed to deter police misconduct . . . ."). The agents here could not have relied in good

faith on the 2006 warrant because it was issued almost two-and-a-half years after the files were first overseized, and some sixteen months after the responsive files had been extracted. That is, the agents did not rely on the 2006 warrant to retain non-responsive files because that warrant came into being only *after* the Fourth Amendment violation occurred. An agent can only rely on something that exists "at the time of the search." *Aguiar*, 737 F.3d at 259; *see Davis*, 131 S. Ct. at 2418 (asking if search was in "objectively reasonable reliance on binding judicial precedent" as of "the time of the search").

In other words, the later 2006 warrant could not cure the prior illegal retention of Ganias's data when agents did not rely on it to retain that data. A warrant is not a Band-Aid that the Government may seek when it realizes its Fourth Amendment violation has been discovered. *See* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 1.3(f) (5th ed. 2015) ("When the magistrate issued the warrant, he did not endorse past activity; he only authorized future activity."). As we have previously held, "Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996).

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

In this case, the agents did *not* present to the magistrate judge all of "the details of their dubious pre-warrant conduct." *Id.* at 1282. Though the majority points out that the agents disclosed to the magistrate judge in 2006 that the mirror images were seized in November 2003, that Ganias was not then

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

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

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

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

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

At bottom, in holding that the Government acted with objectively reasonable reliance on the 2006 warrant, the majority condones creative uses of government power to interfere with individuals' possessory interests and to invade their privacy. Without specifically opining on whether the Government can retain overseized, non-responsive files, the majority has crafted a formula for the Government to do just that. The Government only needs to: obtain a warrant to seize computer data, overseize by claiming files are intermingled (they always will be), keep overseized data until the however distant future, and then (when probable cause one day develops) ask for another warrant to search what it has kept. The rule that we have fashioned does nothing to deter the Government from continually retaining papers that are, though initially properly

seized, not responsive to or particularly described in a warrant. Instead of deterring future violations, we have effectively endorsed them.

The Government bears the burden of proving "the objective reasonableness of the officers' good faith reliance." *Voustianiouk*, 685 F.3d at 215 (quoting *George*, 975 F.2d at 77). It has not met that burden here. To the contrary, the agents exhibited a deliberate or reckless or grossly negligent disregard for Ganias's rights, *see Davis*, 564 U.S. at 238, and, in my view, the benefits of deterring the Government's unlawful actions here appreciably outweigh the costs of suppression, *see Herring*, 555 U.S. at 141; *see also Davis*, 564 U.S. at 232; *Pa. Bd. of Prob. & Parole*, 524 U.S. at 364-65.

III.

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

The wheels of justice have spun ever so slowly in this case. The Government seized Ganias's files in November 2003, nearly thirteen years ago.

He was indicted, in 2008, some eight years ago. He waited two-and-a-half years for a trial, and after he was found guilty, he waited roughly another ten months to be sentenced. He appealed his conviction, but it took another year for his appeal to be heard, and then another year for the appeal to be decided.

The panel issued its decision on June 17, 2014. The panel held that the Government violated Ganias's Fourth Amendment rights and rejected its reliance on the good faith exception. On August 15, 2014, the Government filed a petition for rehearing, seeking panel rehearing only, not rehearing *en banc*, and seeking rehearing only with respect to the good faith exception. In other words, the Government did not seek rehearing on whether the Fourth Amendment was violated, and it did not seek rehearing *en banc* on either issue.

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

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

I respectfully dissent.