

12-240

To Be Argued By:
SARALA V. NAGALA

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 12-240

UNITED STATES OF AMERICA,
Appellee,

-vs-

STAVROS M. GANIAS,
Defendant-Appellant.

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

PETITION FOR PANEL REHEARING

DEIRDRE M. DALY
*United States Attorney
District of Connecticut*

SARALA V. NAGALA
ANASTASIA E. KING
Assistant United States Attorneys
SANDRA S. GLOVER
Assistant United States Attorney (of counsel)

Table of Contents

Table of Authorities	ii
Preliminary Statement	1
Statement of the Case	2
Argument.....	5
A. The agents acted in good faith.....	7
B. The costs of suppression outweigh its benefits	13
Conclusion	15

Table of Authorities

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

Cases

<i>Arizona v. Evans</i> , 514 U.S. 1 (1995)	7
<i>Davis v. United States</i> , 131 S. Ct. 2419 (2011)	<i>passim</i>
<i>Herring v. United States</i> , 555 U.S. 135 (2009)	5, 6, 7
<i>Illinois v. Krull</i> , 480 U.S. 340 (1987)	7
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	11
<i>United States v. Ganas</i> , 755 F.3d 125 (2d Cir. 2014)	<i>passim</i>
<i>United States v. Getto</i> , 729 F.3d 221 (2d Cir. 2013)	12
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	<i>passim</i>
<i>United States v. Moore</i> , 968 F.2d 216 (2d Cir. 1992)	9

United States v. Park,
__ F.3d __, No. 13-4142,
2014 WL 3289493 (2d Cir. July 9, 2014)
(per curiam)..... 15

United States v. Riley,
906 F.2d 841 (2d Cir. 1990)..... 11

United States v. Triumph Capital Group, Inc.,
211 F.R.D. 31 (D. Conn. 2002) 10

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 12-240

UNITED STATES OF AMERICA,

Appellee,

-vs-

STAVROS M. GANIAS,

Defendant-Appellant.

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

PETITION FOR PANEL REHEARING

Preliminary Statement

The United States petitions for panel rehearing of the Court's ruling in *United States v. Ganiias*, 755 F.3d 125 (2d Cir. 2014). In *Ganiias*, this Court held that the defendant's Fourth Amendment rights were violated by the government's retention and subsequent search—pursuant to a validly-issued search warrant—of the defendant's computer files. *Id.* at 137-40. The govern-

ment does not challenge this portion of the Court's opinion.

In the next part of the opinion, however, a divided panel of the Court held that suppression of the computer files was warranted because (i) the agents did not act in good faith reliance on the law in searching the files in April 2006, and (ii) the costs of suppression were low. *Id.* at 140-41. The Court failed to consider, however, that the agents relied in good faith on the issuance of a *search warrant* to authorize the 2006 search. Furthermore, the Court significantly undervalued the costs of suppression in this case. Accordingly, for the reasons set forth below, the government respectfully requests that the Court reconsider its ruling that the exclusionary rule required suppression here.

Statement of the Case

The government's investigation here began in August 2003 when it received information that James McCarthy (and two of his businesses) were defrauding the Army in connection with maintenance and security contracts. *Id.* at 128. Stavros Gantias, a former IRS agent, had been the accountant for McCarthy's companies. *Id.* In connection with the fraud investigation, the government obtained a search warrant in November 2003 authorizing the seizure and search of computers at Gantias's accounting firm for files relating to the two companies. *Id.* Rather than seiz-

ing the computers themselves, the government copied images of the hard drives and left the computers onsite. *Id.* The district court found that Gantias was “present at the time of the search and spoke to the agents,” but the court made no findings about the content of those conversations. SA9.¹

It is undisputed that the agents did not exceed the scope of the November 2003 warrant in their review of the seized computer images for evidence of the alleged contracting fraud. *See* 755 F.3d at 129 (“Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.”); *id.* (noting that case agent did not believe she could review files beyond scope of the 2003 warrant even though they were already in her possession); Defendant’s Br. at 42.

As the investigation evolved, however, paper documents and other evidence led the agents to believe that Gantias was committing tax evasion in his own right. 755 F.3d at 129. In February 2006, the agents asked Gantias for permission to examine the computer images that had been seized in November 2003; receiving no response, the agents obtained a second search warrant in April 2006 authorizing them to review those im-

¹ The Special Appendix filed with the appellant’s brief in this appeal is cited as “SA__” and the Joint Appendix is cited as “JA__.”

ages for evidence of Ganiias's tax crimes. *Id.* at 130. The search warrant affidavit made clear to the magistrate judge that the search would be conducted on the images that had been in the government's possession since November 2003. JA461-72. The evidence revealed in the 2006 search of Ganiias's computer files—which only existed on the seized images because Ganiias had altered the originals, 755 F.3d at 130—was critical to the government's case.

As relevant here, a grand jury returned a superseding indictment charging Ganiias with tax evasion in December 2009. *Id.* In February 2010, Ganiias moved to suppress the evidence seized from his computer records. *Id.* Judge Alvin W. Thompson held a two-day hearing on the motion and denied it on April 14, 2010. *Id.* He wrote a 24-page opinion detailing his factual findings and legal conclusions. SA6-29. The case proceeded to trial before Judge Ellen Bree Burns, and the jury convicted Ganiias of two counts of tax evasion. 755 F.3d at 130. He was sentenced principally to 24 months' imprisonment but was released pending appeal. *Id.* at 131.

On appeal, this Court held that the government violated Ganiias's Fourth Amendment rights by retaining, and later searching, the November 2003 computer images. *Id.* at 137-40. Judges Chin and Restani further held that the exclusionary rule required suppression of the evidence because there was a widespread seizure,

the agents did not act in good faith, and the benefits of suppression outweighed the costs. *Id.* at 140-41. Judge Hall dissented from the Court's suppression holding, finding that the government had not acted in bad faith, that the agents' conduct did not need to be deterred, and that the panel majority erred in minimizing the defendant's dangerousness. *Id.* at 142 (Hall, J., concurring and dissenting). Nevertheless, because the panel majority concluded that suppression was warranted, the Court reversed the district court's denial of the suppression motion and vacated the judgment of conviction. *Id.* at 141.

Argument

The government respectfully requests that the Court reconsider its suppression holding. As the panel opinion acknowledged, even when government conduct violates the Fourth Amendment, suppression is not an automatic remedy. 755 F.3d at 136-37. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 136 (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)).

In particular, under *United States v. Leon*, 468 U.S. 897, 922 (1984), and its progeny, a court must assess the "flagrancy of the police misconduct" and the need to deter "deliberate,"

‘reckless,’ or ‘grossly negligent’” actions when deciding whether suppression is appropriate in a given case. *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) (quoting *Leon*, 468 U.S. at 909, and *Herring*, 555 U.S. at 144). But the court must consider as well the costs of suppression. *Davis* explained these costs as follows:

Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort.

Id. (internal citations and quotations omitted). Given these significant costs, the Court recognized that exclusion cannot “pay its way” when the police act with “an objectively ‘reasonable good faith-belief’ that their conduct is lawful.” *Id.* at 2427-28 (quoting *Leon*, 468 U.S. at 909).

Applying these standards in this case, suppression was not warranted. The undisputed facts show that the agents relied in good faith on a validly issued warrant and abided by the law in force at the time of the search. Furthermore, the heavy costs of suppression far outstrip any minimal deterrent benefit in this case.

A. The agents acted in good faith.

The agents' conduct was both reasonable and undertaken in good faith, based on the standards set forth by the Supreme Court. In *Davis*, the Supreme Court explained that the government can demonstrate good faith in a number of ways: (i) reasonable reliance on a warrant later held invalid, *see Leon*, 468 U.S. at 922; (ii) reasonable reliance on a subsequently-invalidated statute, *see Illinois v. Krull*, 480 U.S. 340 (1987); (iii) reasonable reliance on erroneous information in a database maintained by judicial employees, *see Arizona v. Evans*, 514 U.S. 1 (1995); (iv) reasonable reliance on erroneous information in a police database, *see Herring*, 555 U.S. at 137; or (v) reasonable reliance on binding judicial precedent that is later overturned. 131 S. Ct. at 2428-29. Thus, objectively reasonable reliance on any one of these types of authority—even if the authority is later invalidated—results in a finding of good faith that renders suppression unnecessary. *See id.* As the Court explained with respect to an officer's reliance on a subsequently-invalidated warrant, “[t]he error in such a case rests with the issuing magistrate, not the police officer, and punishing the errors of judges is not the office of the exclusionary rule.” *Id.* at 2428 (internal citations and quotations omitted).

Here, the panel majority appears to have overlooked the well-established rule that rea-

sonable reliance on a search warrant issued by a magistrate judge demonstrates the agents' good faith. *See Leon*, 468 U.S. at 922. The opinion states: "Government agents act in good faith when they perform 'searches conducted in objectively reasonable reliance on binding appellate precedent.'" 755 F.3d at 136 (quoting *Davis*, 131 S. Ct. at 2423-24); *see also id.* at 140. This limited statement of the rule suggests that reliance on binding appellate precedent is the *only* way to establish good faith—a conclusion belied by both *Davis* and *Leon*. *See Davis*, 131 S. Ct at 2429 (noting that "[i]f the police in this case had reasonably relied on a warrant in conducting their search," "the exclusionary rule would not apply"). The panel majority therefore incorrectly suggests that reliance on binding appellate precedent occupies the full field of good faith reliance, when in fact *Leon's* rule authorizing reliance on a warrant takes precedence and should have been applied here.

This legal error likely infected the panel majority's conclusion that the agents did not act in good faith. *See* 755 F.3d at 140 (failing to mention and apply *Leon*). Had the majority applied *Davis* and *Leon*, it would have concluded that suppression was unnecessary because the agents here relied on the April 2006 search warrant. Moreover, although *Leon* identified four circumstances where the good-faith-reliance-on-a-warrant rule would not apply, none of those cir-

cumstances are present here: (i) the issuing magistrate was not knowingly misled; (ii) the issuing magistrate did not wholly abandon his judicial role; (iii) the application was not so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (iv) the warrant was not so facially deficient that reliance upon it was unreasonable. *See United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992) (citing *Leon*, 468 U.S. at 923). And in fact, the application for the 2006 warrant made clear to the magistrate judge that the images to be searched were those retained by the government after the November 2003 seizure. JA454-72. Therefore, even if the magistrate judge erred in signing the warrant (because, as the panel found, the government had retained the 2003 images for an unreasonable length of time), that error does not and should not rest with the agents, who reasonably relied on the issuance of the warrant before conducting their search. *See Davis*, 131 S. Ct. at 2428.

Indeed, trial counsel below conceded that the agents had acted in good faith by relying on issuance of a warrant before they searched the computer files. *See* JA425 (“I think—there is a warrant that’s signed by a magistrate and I think in good faith, you know, that they could have relied at least for probable cause purposes on that. So that’s why I didn’t pursue that in my argument.”). In light of this concession, the ma-

jority could reasonably conclude that the agents reasonably relied on the issuance of the 2006 warrant to support their search.

Moreover, even if *Davis's* “binding appellate precedent” rule were the only way to establish good faith, the agents met that standard by conforming their conduct to precedent at the time. Judge Hall’s dissenting opinion correctly recognized that there was little case law “either at the time of the search or in the following years to indicate that the Government could not hold onto the non-responsive material in the way it did.” 755 F.3d at 142 (Hall, J., concurring and dissenting). In November 2003, when the initial searches were conducted, image copying of computers was still in its infancy and this Court had not announced any specific rules pertaining to the government’s retention and search of computer records. The sole case that guided agents on the contours of computer searches was a case that supported the agents’ actions here. *See United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 62 (D. Conn. 2002) (noting that the “seizure of any documents not named in the warrant [for a computer] resulted from a good faith response to the inherent practical difficulties of searching a computer’s hard drive for evidence of deleted data and files” and was not a general search; further holding that the computer agent acted in good faith).

Even by April 2006, no rule had developed prohibiting the government’s conduct. Indeed, the case law at that time suggested that obtaining a second warrant to search a lawfully-seized computer for evidence of a new crime—the precise course taken by the agents here—was the proper and lawful course of conduct. *See United States v. Carey*, 172 F.3d 1268, 1274-76 (10th Cir. 1999) (excluding evidence where agents did not obtain second warrant to search for evidence of a different crime); *see also United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990) (in non-computer context, agents obtained second warrant to search storage locker after developing probable cause during search of defendant’s home and car). As *Davis* makes clear, agents should not be punished for engaging in “conscientious police work,” 131 S. Ct. at 2429, when they abide by the law in force at the time of the search.²

² Although “general warrants” have been prohibited since the Fourth Amendment went into effect long ago, *Davis* contemplates a binding appellate precedent that is specific to the factual situation presented, such as the search of a car incident to arrest that was at issue in *Davis*. At no time before the *Ganias* opinion had this Court held that retention of computer records seized as a result of practical necessity and then required to be maintained for evidentiary integrity violated the Fourth Amendment.

Finally, the panel majority’s conclusion on good faith is inconsistent with the longstanding principle that factual findings of the district court are reviewed for clear error and should be viewed in the light most favorable to the government. *See* 755 F.3d at 131 (“As to the Fourth Amendment issue, we review the district court’s findings of fact for clear error, viewing the evidence in the light most favorable to the Government, and its conclusions of law *de novo*.”); *see also United States v. Getto*, 729 F.3d 221, 227 (2d Cir. 2013) (same). The panel majority’s conclusion rests on facts that were not found by the district court—including one key fact that was contested below.

First, the panel majority credited Ganas’s claim that an agent had told him certain files would be purged once the search was completed. 755 F.3d at 128; *id.* at 140. Second, the panel majority relied heavily on a purported “view” by government agents that the files were “government property.” 755 F.3d at 140; *see* JA145-46. Although both of these issues came up during the suppression hearing, the district court made no findings of fact on either topic. Thus, the panel majority’s reliance on these facts is inconsistent with its obligation to view the facts in the light most favorable to the government.

This is especially true with respect to the purported finding that an agent told Ganas that non-responsive files would be “purged” after the

search. That “fact” came from an uncorroborated and self-serving affidavit submitted by Ganius six-and-a-half years after the search. But this “fact” was certainly contested. Two agents testified at the suppression hearing that they had not heard anyone make any representations to Ganius about any information being purged. JA166-67, JA197. When, as here, this fact was disputed below, and when, as here, the district court did not resolve this dispute in its findings of fact, this Court’s reliance on the defendant’s version of the facts is inconsistent with its responsibility to view the facts in the light most favorable to the government.

In sum, where the agents acted in a good faith belief that their conduct was lawful—both under a warrant and the case law—the exclusionary rule cannot “pay its way.” *Davis*, 131 S. Ct. at 2428.

B. The costs of suppression outweigh its benefits.

The government also respectfully requests that the panel majority reweigh the substantial costs against the minimal benefits of suppression. The majority’s calculation of the benefits of suppression here rested largely on its conclusion that the agents acted in bad faith, an assessment the government challenges. *See supra*. The majority also relied, however, on a growing need to deter certain conduct related to computer

searches because of the rise in the use of mirror images. But the *future* deterrent value of a rule is irrelevant to the suppression analysis: the appropriate question is whether the agents' actions between 2003 and 2006, given the state of the law at the time, were flagrant and reckless. See *Davis*, 131 S. Ct. at 2427. Suppressing the evidence seized at a time when the agents could not have known their conduct was unlawful runs afoul of *Davis* and the purpose of the exclusionary rule.

Moreover, the panel majority undervalued the costs of suppression in this case. *Davis* made clear that there is always a cost to the judicial system and to society at large when reliable, trustworthy evidence is suppressed at the expense of both the truth and justice for a criminal like Ganius. 131 S. Ct. at 2427. These costs are especially salient when the government has invested several years in an investigation that culminates in a lengthy trial, as was the case here. In light of the “serious and nefarious effects of money fraud crimes on society,” 755 F.3d at 142 (Hall, J., concurring and dissenting), these costs are no less significant when the criminal has committed tax evasion than when he has committed a controlled substance or violent offense. And in the context of tax cases, the costs of suppression—including the cost of “set[ting] the criminal loose in the community without punishment,” *Davis*, 131 S. Ct. at 2427, also in-

clude the costs associated with reduced general deterrence. Indeed, just a few weeks after *Ganias*, another panel of this Court recognized that “general deterrence occupies an especially important role in criminal tax offenses, as criminal tax prosecutions are relatively rare.” *United States v. Park*, __ F.3d __, No. 13-4142, 2014 WL 3289493, *4 (2d Cir. July 9, 2014) (per curiam).

In short, the benefits of deterrence here were far outweighed by the costs of suppression.

Conclusion

For the foregoing reasons, the government respectfully requests panel rehearing on the suppression issue.

Dated: August 14, 2014

Respectfully submitted,

DEIRDRE M. DALY
UNITED STATES ATTORNEY
DISTRICT OF CONNECTICUT



SARALA V. NAGALA
ASSISTANT U.S. ATTORNEYS

Sandra S. Glover
Assistant United States Attorney (of counsel)

Addendum

755 F.3d 125
United States Court of Appeals,
Second Circuit.

UNITED STATES of America, Appellee,
v.
Stavros M. GANIAS, Defendant–Appellant.

Docket No. 12–240–cr. | Argued:
April 11, 2013. | Decided: June 17, 2014.

Synopsis

Background: Following denial of motion to suppress, 2011 WL 2532396, defendant was convicted in the United States District Court for the District of Connecticut, Ellen Bree Burns, Senior District Judge, of tax evasion. The District Court, 2011 WL 3563104, denied defendant's motion for judgment of acquittal, and denied reconsideration, 2011 WL 4738684. The defendant appealed.

Holdings: The Court of Appeals, Chin, Circuit Judge, held that:

[1] juror's use of social networking did not violate defendant's right to an impartial jury;

[2] government's seizure and retention of a mirror image of defendant's computer hard drive was unreasonable; and

[3] exclusionary rule applied to government's seizure and retention of a mirror image of defendant's computer hard drive.

Reversed, conviction vacated, and case remanded.

Peter W. Hall, Circuit Judge, filed an opinion concurring in part and dissenting in part.

Attorneys and Law Firms

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

Stanley A. Twardy, Jr. (Daniel E. Wenner, on the brief), Day Pitney LLP, Stamford, CT, for Defendant–Appellant.

Before: HALL and CHIN, Circuit Judges, and RESTANI, Judge.*

Opinion

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

CHIN, Circuit Judge:

In this case, defendant-appellant Stavros M. Ganas appeals from a judgment convicting him, following a jury trial, of tax evasion. He challenges the conviction on the grounds that his Fourth Amendment rights were violated when the Government copied three of his computer hard drives *128 pursuant to a search warrant and then retained files beyond the scope of the warrant for more than two-and-a-half years. He also contends that his right to a fair trial was violated when, during the trial, a juror posted comments about the case on his Facebook page and “friended” another juror. We reject the second argument but hold that the Government's retention of the computer records was unreasonable. Accordingly, we vacate the conviction and remand for further proceedings.

STATEMENT OF THE CASE

A. The Facts¹

In the 1980s, after working for the Internal Revenue Service (“IRS”) for some fourteen years, Ganas started his own accounting business in Wallingford, Connecticut. He provided tax and accounting services to individuals and small businesses. In 1998, he began providing services to James McCarthy and two of McCarthy's businesses, American Boiler and Industrial Property Management (“IPM”). IPM had been hired by the Army to provide maintenance and security at a vacant Army facility in Stratford, Connecticut.

In August 2003, the Criminal Investigative Command of the Army received a tip from a confidential source that individuals affiliated with IPM were engaging in improper conduct, including stealing copper wire and other items from the Army facility and billing the Army for work that IPM employees performed for American Boiler. The source alleged that evidence of the wrongdoing could be found at the

offices of American Boiler and IPM, as well as at the offices of "Steve Ganius [sic]," who "perform[ed] accounting work for IPM and American Boiler."²

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

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

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

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

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

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

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

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

In late 2004, IRS investigators discovered accounting irregularities regarding transactions between IPM and American Boiler in the paper documents taken from Ganius's office. After subpoenaing and reviewing the relevant bank records in 2005, they began to suspect that Ganius 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 Ganius. Further investigation in 2005 and early 2006 indicated that Ganius had been improperly reporting income for both of his clients, leading the Government to suspect that he also might have been underreporting his own income.

At that point, the IRS case agent wanted to review Ganius's personal financial records and she knew, from her review of the seized computer records, that they were among the files in the DVDs copied from Ganius's hard drives. The case agent was aware, however, that Ganius'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.

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

B. Procedural History

1. The Indictment

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

2. The Motion to Suppress

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

3. The Trial

In April 2010, the case was transferred to Judge Ellen Bree Burns for trial. In May 2010, the district court severed the two counts against Ganius for tax evasion with respect to his personal taxes from the other charges.³

Trial commenced on March 8, 2011, with jury selection, and testimony was scheduled to begin on March 10, 2011. At 9:34

p.m. on March 9, the evening before the start of the evidence, one of the jurors, Juror X, posted a comment on his Facebook page: "Jury duty 2morrow. I may get 2 hang someone ... can't wait."

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

March 10 at 3:34 pm:

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

March 15 at 1:41 pm:

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

March 17 at 2:07 pm:

Guiness for lunch break. Jury duty ok today.

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

On April 1, 2011, the jury convicted Ganius on both counts. Later that evening, at 9:49 pm, Juror X posted another comment on his Facebook page: "(GUILTY:)" He later elaborated:

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

4. The Motion for a New Trial

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

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

5. Sentencing

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

DISCUSSION

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

As to the Fourth Amendment issue, we review the district court’s findings of fact for clear error, viewing the evidence in the light most favorable to the Government, and its conclusions of law *de novo*. *United States v. Ramos*, 685 F.3d 120, 128 (2d Cir.), *cert. denied*, ___ U.S. ___, 133 S.Ct. 567, 184 L.Ed.2d 369 (2012). As to the issue of the district court’s denial of Ganius’s motion for a new trial for alleged juror misconduct, we review for abuse of discretion. *United States v. Farhane*, 634 F.3d 127, 168 (2d Cir.), *cert. denied*, ___ U.S. ___, 132 S.Ct. 833, 181 L.Ed.2d 542 (2011).

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

A. Juror’s Improper Use of Social Media

1. Applicable Law

[1] [2] [3] [4] [5] Defendants have the right to a trial “by an impartial jury.” U.S. Const. amend. VI. That right is not violated, however, merely because a juror places himself in a “potentially compromising situation.” *United States v. Aiello*, 771 F.2d 621, 629 (2d Cir.1985), *abrogated on other grounds by* *132 *Rutledge v. United States*, 517 U.S. 292, 116 S.Ct. 1241, 134 L.Ed.2d 419 (1996); *see also Smith v. Phillips*, 455 U.S. 209, 217, 102 S.Ct. 940, 71 L.Ed.2d 78 (1982) (“[I]t is virtually impossible to shield jurors from every contact or influence that might theoretically affect their vote.”). A new trial will be granted only if “the juror’s ability to perform her duty impartially has been adversely affected,” *Aiello*, 771 F.2d at 629, and the defendant has been “substantially prejudiced” as a result, *United States v. Fumo*, 655 F.3d 288, 305 (3d Cir.2011). Although courts are understandably reluctant to invade the sanctity of the jury’s deliberations, the trial judge should inquire into a juror’s partiality where there are reasonable grounds to believe the defendant may have been prejudiced. *United States v. Schwarz*, 283 F.3d 76, 97 (2d Cir.2002); *United States v. Sun Myung Moon*, 718 F.2d 1210, 1234 (2d Cir.1983). That inquiry should end, however, as soon as it becomes apparent that those reasonable grounds no longer exist. *See Sun Myung Moon*, 718 F.2d at 1234.

B. Application

A juror who “friends” his fellow jurors on Facebook, or who posts comments about the trial on Facebook, may, in certain circumstances, threaten a defendant’s Sixth Amendment right to an impartial jury.⁴ Those circumstances, however, are not present here. The district court inquired into the matter and credited Juror X’s testimony that he deliberated impartially and in good faith. The district judge’s credibility determination was not clearly erroneous, and thus she did not abuse her discretion in denying the motion for a new trial.

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

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

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

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

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

Here, while the district court gave an appropriate instruction at the start of the jury's deliberations, it does not appear that it did so earlier. As demonstrated by this case, instructions at the beginning of deliberations may not be enough. We think it would be wise for trial judges to give the Committee's proposed instructions both at the start of trial and as deliberations begin, and to issue similar reminders throughout

the trial before dismissing the jury each day. While situations like the one in this case will not always require a new trial, it is the better practice for trial judges to be proactive in warning jurors about the risks attending their use of social media.

B. The Seizure and Retention of Ganius's Computer Records

1. Applicable Law

[6] [7] The Fourth Amendment protects the rights of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV; *see, e.g., United States v. Ramirez*, 523 U.S. 65, 71, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998). A search occurs when the Government acquires information by either "physically intruding on persons, houses, papers, or effects," or otherwise invading an area in which the individual has a reasonable expectation of privacy. *See Florida v. Jardines*, — U.S. —, 133 S.Ct. 1409, 1414, 185 L.Ed.2d 495 (2013) (internal quotation mark omitted); *see also Katz v. United States*, 389 U.S. 347, 360–61, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). A seizure occurs when the Government interferes in some meaningful way with the individual's possession of property. *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 951 n. 5, 181 L.Ed.2d 911 (2012). Subject to limited exceptions,⁷ a search or seizure conducted without a warrant is presumptively unreasonable. *See Kyllo v. United States*, 533 U.S. 27, 31, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

[8] [9] We must construe the Fourth Amendment "in [] light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens." *Kyllo*, 533 U.S. at 40, 121 S.Ct. 2038. Applying 18th Century notions about searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the "computer age" against Fourth Amendment frameworks crafted long before this technology existed. *134⁸ As we do so, we must keep in mind that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Missouri v. McNeely*, — U.S. —, 133 S.Ct. 1552, 1569, 185 L.Ed.2d 696 (2013) (Roberts, C.J., concurring in part and dissenting in part) (internal quotation marks omitted). Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge

is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools.

"The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir.2013) (quoting *Payton v. New York*, 445 U.S. 573, 583, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980)) (internal quotation marks omitted). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King*, — U.S. —, 133 S.Ct. 1958, 1980, 186 L.Ed.2d 1 (2013). The British Crown had long used these questionable instruments to enter a political opponent's home and seize all his books and papers, hoping to find among them evidence of criminal activity. See *Stanford v. Texas*, 379 U.S. 476, 482–83, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965). The Framers abhorred this practice, believing that "papers are often the dearest property a man can have" and that permitting the Government to "sweep away all papers whatsoever," without any legal justification, "would destroy all the comforts of society." *Entick v. Carrington*, 95 Eng. Rep. 807, 817–18 (C.P. 1765).⁹

[10] [11] The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin*, 720 F.3d at 445. The latter requirement, in particular, "makes general searches ... impossible" because it "prevents the seizure of one thing under a warrant describing another." *Id.* at 446 (quoting *Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 (1927)) (internal quotation marks omitted). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described *135 in the warrant. See *Horton v. California*, 496 U.S. 128, 140, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir.1982). Certain exceptions have been made in those "comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site." *Tamura*, 694 F.2d at 595–96. But in those cases, the off-site review had to be monitored by a neutral magistrate and nonresponsive documents were to be returned after the relevant items were identified. *Id.* at 596–97.

[12] These Fourth Amendment protections apply to modern computer files. Like 18th Century "papers," computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted. See, e.g., *Galpin*, 720 F.3d at 446 ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir.2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs...."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

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

[13] In light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be. Indeed, the 2009 amendments to the Federal Rules of Criminal Procedure, which added Rule 41(e)(2)(B), clearly contemplated off-site review of computer hard drives in certain circumstances.¹⁰ Although Rule 41(e)(2)(B) was not in effect in 2003, when *136 the warrant was executed with respect to Ganius's computers, case law both

before and after the rule's adoption has recognized that off-site review of seized electronic files may be necessary and reasonable. *See, e.g., United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir.2013); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir.2012); *United States v. Hill*, 459 F.3d 966, 976–77 (9th Cir.2006); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999).

The off-site review of these mirror images, however, is still subject to the rule of reasonableness. *See, e.g., Ramirez*, 523 U.S. at 71, 118 S.Ct. 992 (“The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant.” (citation omitted)). The advisory committee’s notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is “reasonable” in this context. Specifically, the committee rejected “a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place.” Fed.R.Crim.P. 41(e)(2)(B) advisory committee’s notes to the 2009 Amendments. The committee noted that several variables—storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload—influence the duration of a forensic analysis and counsel against a “one size fits all” time period. *Id.* In combination, these factors might justify an off-site review lasting for a significant period of time. They do not, however, provide an “independent basis” for retaining any electronic data “other than [those] specified in the warrant.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir.2010) (en banc).

[14] [15] [16] 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, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). Suppression is required “only when [agents] (1) ... effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith.” *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir.2000) (internal quotation marks and citations omitted).

[17] [18] [19] [20] The Government effects “widespread seizure of items” beyond the scope of the

warrant when the Government’s search “resemble [s] a general search.” *Id.* at 140–41. Government agents act in good faith when they perform “searches conducted in objectively reasonable reliance on binding appellate precedent.” *Davis v. United States*, — U.S. —, 131 S.Ct. 2419, 2423–24, 180 L.Ed.2d 285 (2011). When Government agents act on “good-faith reliance [o]n the law at the time of the search,” the exclusionary rule will not apply. *United States v. Aguiar*, 737 F.3d 251, 259 (2d Cir.2013). “The burden is on the government to demonstrate the objective reasonableness of the officers’ good faith reliance.” *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir.2012) (internal quotation marks omitted).

[21] 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 *137 rule. *Herring*, 555 U.S. at 141, 129 S.Ct. 695; *see Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364–65, 118 S.Ct. 2014, 141 L.Ed.2d 344 (1998) (citing *United States v. Payner*, 447 U.S. 727, 734, 100 S.Ct. 2439, 65 L.Ed.2d 468 (1980)). “The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free—something that ‘offends basic concepts of the criminal justice system.’” *Herring*, 555 U.S. at 141, 129 S.Ct. 695 (quoting *United States v. Leon*, 468 U.S. 897, 908, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

2. Analysis

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

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

If the 2003 warrant authorized the Government to retain all the data on Ganius's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general warrant. The Government's retention of copies of Ganius's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled the Government to possess indefinitely personal records of Ganius that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganius's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment. See *United States v. Place*, 462 U.S. 696, 708, 103 S.Ct. 2637, 77 L.Ed.2d 110 (1983) (detaining a traveler's luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure); see also *Soldal v. Cook Cnty.*, 506 U.S. 56, 62–64, 68, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched and the owner's privacy was never violated); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435, 102 S.Ct. 3164, 73 L.Ed.2d 868 (1982) (“The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.”).

We conclude that the unauthorized seizure and retention of these documents was unreasonable. The Government had no warrant authorizing the seizure of Ganius's personal records in 2003. By December 2004, these documents had been separated *138 from those relevant to the investigation of American Boiler and IPM. Nevertheless, the Government continued to retain them for another year-and-a-half until it finally developed probable cause to search and seize them in 2006. Without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganius's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation.

The Government offers several arguments to justify its actions, but none provides any legal authorization for its continued and prolonged possession of the non-responsive

files. First, it argues that it must be allowed to make the mirror image copies as a matter of practical necessity and, according to the Government's investigators, those mirror images were “the government's property.” As explained above, practical considerations may well justify a reasonable accommodation in the manner of executing a search warrant, such as making mirror images of hard drives and permitting off-site review, but these considerations do not justify the indefinite retention of non-responsive documents. See *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1171. Without a warrant authorizing seizure of Ganius's personal financial records, the copies of those documents could not become *ipso facto* “the government's property” without running afoul of the Fourth Amendment.

Second, the Government asserts that by obtaining the 2006 search warrant, it cured any defect in its search of the wrongfully retained files. But this argument “reduces the Fourth Amendment to a form of words.” *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392, 40 S.Ct. 182, 64 L.Ed. 319 (1920). In *Silverthorne*, the Government, “without a shadow of authority[,] went to the office of [the defendants'] company and made a clean sweep of all the books, papers and documents found there.” *Id.* at 390, 40 S.Ct. 182. The originals were eventually returned because they were unlawfully seized, but the prosecutor had made “[p]hotographs and copies of material papers” and used these to indict the defendants and obtain a subpoena for the original documents. *Id.* at 391, 40 S.Ct. 182. Justice Holmes succinctly summarized the Government's argument supporting the constitutionality of its actions as follows:

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

Id. Unsurprisingly, the Supreme Court rejected that argument: “The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not

be used at all” unless some exception applies.¹¹ *Id.* at 392, 40 S.Ct. 182. The same *139 rationale applies here. If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant.

Third, the Government argues that it must be permitted to search the mirror images in its possession because the evidence no longer existed on Ganius's computers. But the ends, however, do not justify the means. The loss of the personal records is irrelevant in this case because the Government concedes that it never considered performing a new search of Ganius's computers and did not know that the files no longer existed when it searched the mirror images in its possession. And even if it were relevant, the Fourth Amendment clearly embodies a judgment that some evidence of criminal activity may be lost for the sake of protecting property and privacy rights. *See, e.g., United States v. Calandra*, 414 U.S. 338, 361, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974) (“The judges who developed the exclusionary rule were well aware that it embodied a judgment that it is better for some guilty persons to go free than for the [Government] to behave in forbidden fashion.”).

Fourth, the Government contends that returning or destroying the non-responsive files is “entirely impractical” because doing so would compromise the remaining data that was responsive to the warrant, making it impossible to authenticate or use it in a criminal prosecution. Appellee Br. at 34. We are not convinced that there is no other way to preserve the evidentiary chain of custody. But even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose.

Finally, the Government argues that Ganius's failure to bring a motion for the return of property, pursuant to Federal Rule of Criminal Procedure 41(g), precludes him from seeking suppression now. Although the district court accepted this argument, we find no authority for concluding that a Rule 41(g) motion is a prerequisite to a motion to suppress. *See* Fed.R.Crim.P. 41(g) (“A person aggrieved ... may move for the property's return.” (emphasis added)), Fed.R.Crim.P. 41(h) (“A defendant may move to suppress evidence....” (emphasis added)). Imposing such a prerequisite makes little sense in this context, where Ganius still had the

original computer files and did not need the Government's copies to be returned to him. Moreover, we fail to see what purpose a Rule 41(g) motion would have served, given the Government's position that non-responsive files in its possession could not feasibly have been returned or purged anyway.

Because the Government has demonstrated no legal basis for retaining the non-responsive documents, its retention and subsequent search of those documents were unconstitutional. The Fourth Amendment was intended to prevent the Government from entering individuals' *140 homes and indiscriminately seizing all their papers in the hopes of discovering evidence about previously unknown crimes. *See Entick*, 95 Eng. Rep. at 817–18; *see also Jones*, 132 S.Ct. at 949. Yet this is exactly what the Government claims it may do when it executes a warrant calling for the seizure of particular electronic data relevant to a different crime. Perhaps the “wholesale removal” of intermingled computer records is permissible where off-site sorting is necessary and reasonable, *Tamura*, 694 F.2d at 595–97, but this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations. *See Comprehensive Drug Testing*, 621 F.3d at 1171.

[24] We turn now to the application of the exclusionary rule. As discussed above, suppression is required when (1) there is a widespread seizure of items not covered by the warrant and (2) agents do not act in good faith. *United States v. Shi Yan Liu*, 239 F.3d 138, 141 (2d Cir.2000). There must also be a weighing of (3) the benefits of deterrence against (4) the costs of suppression. *Herring v. United States*, 555 U.S. 135, 141, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009).

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

Second, the agents here did not act in good faith. Government agents act in good faith when they conduct searches in objectively reasonable reliance on binding appellate precedent. *Davis v. United States*, — U.S. —, 131 S.Ct. 2419, 2423–24, 180 L.Ed.2d 285 (2011). It is the Government's burden—not Ganius's—to demonstrate the

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

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

*141 Finally, the costs of suppression are minimal here. This is not a case where a dangerous defendant is being set free. See *Herring v. United States*, 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) ("The principal cost of applying the [exclusionary] rule is, of course, letting [a] guilty and possibly dangerous defendant[] go free."). Even assuming Ganius committed tax evasion—a serious matter—this case does not involve drugs, guns, or contraband. Nor is this a case where police officers happened upon guns or drugs or other evidence they otherwise could not have found. Rather, early on, the evidence here was readily obtainable by subpoena or search warrant. Moreover, when guns or drugs are suppressed, that evidence is usually irreplaceable. The records here, however, conceivably are available elsewhere as hard copies or can be reconstructed from other records. As made clear by the Government's behavior, the costs of

suppression that the Government has asserted are outweighed by the benefits of deterring future misconduct.

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

CONCLUSION

We conclude that the Government violated Ganius's Fourth Amendment rights by seizing and indefinitely retaining non-responsive computer records, and then searching them when it later developed probable cause. Accordingly, Ganius's personal records, seized in the execution of the November 2003 warrant and retained for two-and-a-half years, should have been suppressed. For the reasons stated above, we REVERSE the district court's denial of the motion to suppress, VACATE the judgment of conviction, and REMAND for further proceedings not inconsistent with this opinion.

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

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

The exclusionary rule is a "deterrent sanction" created by the Supreme Court to "bar[] the prosecution from introducing evidence obtained by way of a Fourth Amendment violation." *Davis v. United States*, 564 U.S. —, 131 S.Ct. 2419, 2423, 180 L.Ed.2d 285 (2011). The Supreme Court has cautioned, however, that "exclusion [should be] 'our last resort, not our first impulse.'" *Herring v. United States*, 555 U.S. 135, 140, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)). This is so because the rule is "'not a personal constitutional right,' nor is it designed to 'redress the injury' occasioned by an unconstitutional search[.] ... [its] sole purpose ... is to deter future Fourth Amendment violations." *Davis*, 131 S.Ct. at 2426 (citations omitted). The rule specifically deters "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144, 129 S.Ct. 695. "To trigger the exclusionary rule, police conduct must be

sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Id.* In general, “searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule... [as] the harsh *142 sanction of exclusion ‘should not be applied to deter objectively reasonable law enforcement activity.’ ” *Davis*, 131 S.Ct. at 2423–24, 2429 (citation omitted).

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

scrupulously avoided reviewing files that it was not entitled to review before obtaining the 2006 search warrant.

With respect to the balancing between deterrence and the cost of suppression, because the Government’s actions did not violate established precedent at the time of the search, I do not perceive a need for deterrence. “[A]ll that exclusion would deter in this case is conscientious police work.” *Davis*, 131 S.Ct. at 2429. Additionally, as Ganius himself stated, the evidence to be suppressed in this case would not have existed but for the Government’s retention of the non-responsive materials. The evidence to be suppressed is thus, contrary to the majority’s conclusion, of the same irreplaceable nature as guns or drugs. Moreover, in light of the serious and nefarious effects of money fraud crimes on society, *see, e.g., United States v. Madoff*, No. 09 Crim. 213(DC), 2009 WL 3347945 (S.D.N.Y. Oct. 13, 2009), I am loathe to conclude that guns, drugs and/or contraband are the only indicia of a dangerous defendant. Accordingly, while I agree that the Government violated the defendant’s Fourth Amendment rights to be free from an unreasonable seizure because it held for a prolonged period of time mirror images of computer-generated records that were not responsive to the 2003 search warrant without returning them (or destroying them), I see no reason to suppress the evidence derived therefrom under the circumstances presented.

Footnotes

- * The Honorable Jane A. Restani, of the United States Court of International Trade, sitting by designation.
- 1 The facts relevant to the issues on appeal are largely undisputed and are drawn from the testimony at the hearing on Ganius’s motion to suppress, the decision of the district court (Thompson, *J.*) denying the suppression motion, and the transcript of the trial.
- 2 The record reflects that Ganius, whose first name is Stavros, was often referred to as “Steve.”
- 3 All the other counts were later dismissed.
- 4 *See, e.g., Fumo*, 655 F.3d at 331 (Nygaard, *J.*, concurring) (“The availability of the Internet and the abiding presence of social networking now dwarf the previously held concern that a juror may be exposed to a newspaper article or television program.”); *United States v. Juror Number One*, 866 F.Supp.2d 442, 451 (E.D.Pa.2011) (“[T]he extensive use of social networking sites, such as Twitter and Facebook, have exponentially increased the risk of prejudicial communication amongst jurors and opportunities to exercise persuasion and influence upon jurors.”). *See generally* Amy. J. St. Eve & Michael A. Zuckerman, *Ensuring an Impartial Jury in the Age of Social Media*, 11 *Duke L. & Tech. Rev.* 1 (2012).
- 5 Judicial Conference Comm. on Court Admin. & Case Mgmt., Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate about a Case (December 2009), available at www.uscourts.gov/uscourts/News/2010/docs/DIR10-018-Attachment.pdf.
- 6 *Id.*
- 7 In this case, the Government has conceded that it needed a warrant to search the non-responsive computer files in its possession and has not argued that any exceptions apply.
- 8 *See generally United States v. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (considering whether placing GPS tracking unit on vehicle constitutes search); *Kyllo*, 533 U.S. at 27, 121 S.Ct. 2038 (determining whether use of thermal imaging constitutes search); *United States v. Aguiar*, 737 F.3d 251 (2d Cir.2013) (determining whether warrantless placement of GPS tracking unit on vehicle fell within good-faith exception to exclusionary rule); *United States v. Galpin*, 720 F.3d 436 (2d Cir.2013) (analyzing

whether warrant to search computer satisfies particularity requirement); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L.Rev. 531 (2005); James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L.Rev. 2809 (2011); Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 Fordham Urb. L.J. 977 (2009).

9 The Supreme Court has explained that *Entick* was “undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure.” *Jones*, 132 S.Ct. at 949 (internal quotation marks omitted).

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

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

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

11 The Supreme Court has abrogated *Silverthorne*'s broad proposition that wrongfully acquired evidence may “not be used at all.” *See United States v. Havens*, 446 U.S. 620, 624–25, 100 S.Ct. 1912, 64 L.Ed.2d 559 (1980) (noting that this evidence may be used for purposes of impeachment); *see also Murray v. United States*, 487 U.S. 533, 537, 108 S.Ct. 2529, 101 L.Ed.2d 472 (1988) (explaining that the “independent source” doctrine allows the admission of “evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality”); *Nix v. Williams*, 467 U.S. 431, 444, 104 S.Ct. 2501, 81 L.Ed.2d 377 (1984) (explaining that “inevitable discovery” doctrine permits the admission of unlawfully obtained evidence if “[t]hat information ultimately or inevitably would have been discovered by lawful means”). The Government does not rely on any of these exceptions here. Indeed, it concedes that if it “had not preserved that data from the November 2003 seizure, it would have been lost forever.” Appellee’s Br. at 33. We do not hold that the Government has waived its right to use the evidence in question for impeachment purposes.