

12-240-cr

IN THE
United States Court of Appeals
FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

—against—

STAVROS M. GANIAS,

Defendant-Appellant.

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

**BRIEF FOR *AMICUS CURIAE* NEW YORK COUNCIL OF DEFENSE
LAWYERS IN SUPPORT OF APPELLANT**

MICHAEL L. YAEGER
BARRY A. BOHRER
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, New York 10022
(212) 756 -2000

*Counsel for New York Council
of Defense Lawyers*

July 29, 2015

TABLE OF CONTENTS

	<u>Page</u>
INTEREST OF <i>AMICUS CURIAE</i> AND SUMMARY OF ARGUMENT	1
ARGUMENT	3
I. By Admitting that to Copy a Computer Is to Seize Its Data, the Government Has Effectively Conceded that It Violated the Fourth Amendment in this Case.....	3
II. The Papers Clause Covers Information Regardless of the Medium in Which It Is Recorded.....	7
A. From its Inception, the Fourth Amendment Protected Information, Not Just Objects.....	7
B. The Papers Clause Extends to Information Transmitted over the Wires and Stored in Computers	13
III. To Copy a Computer Is to Seize the Data It Contains	15
CONCLUSION	18

TABLE OF AUTHORITIES

Cases

Altman v. City of High Point, N.C.,
330 F.3d 194 (4th Cir. 2003)12

Boyd v. United States,
116 U.S. 616 (1886)..... 9, 10, 15

Brower v. County of Inyo,
489 U.S. 593 (1989).....10

Entick v. Carrington,
(1765) 95 Eng. Rep. 807 (K.B.), 19 How St. Tr. 1029 passim

Ex parte Jackson,
96 U.S. 727 (1878).....13

*In re Warrant to Search a certain Email Account Controlled and Maintained by
Microsoft Corp.*,
2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (Nos. M9-150, 13-MJ-2814).....7

Katz v. United States,
389 U.S. 347 (1967).....13

Kyllo v. United States,
533 U.S. 27 (2001).....7, 9

Oliver v. United States,
466 U.S. 170 (1984).....12

Stanford v. Texas,
379 U.S. 476 (1957).....9

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013)14

United States v. Jones,
— U.S. —, 132 S. Ct. 945 (2012)..... 7, 14, 16

United States v. Riley,
134 S. Ct. 2473 (2014)..... 14, 15

Wilkes v. Wood,
19 How. St. Tr. 1153 (1763).....10

Other Authorities

Computer Crime and Intellectual Prop. Section, U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed. 2009).....2

Donald A. Dripps, “Dearest Property”: *Digital Evidence and the History of Private “Papers” as Special Objects of Search and Seizure*,
103 J. Crim. L. & Criminology 49 (2013)..... 8, 9, 10

LaFave et al., *Search & Seizure* (5th ed.)16

Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*,
119 Yale L.J. 700 (2010) 16, 17, 18

Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*,
45 Gonz. L. Rev. 1 (2009–2010)9

The Complete Bill of Rights: The Drafts, Debates, Sources, and Origins
(Neil H. Cogán, ed., 1997)..... 10, 11

Thomas K. Clancy, *The Framers’ Intent: John Adams, His Era, and the Fourth Amendment*, 86 Indiana L.J. 979 (2011).....8

William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602-1791* (2009)8

**INTEREST OF *AMICUS CURIAE*
AND SUMMARY OF ARGUMENT**

The New York Council of Defense Lawyers (“NYCDL”) is a not-for-profit professional association of approximately 250 lawyers, including many former federal prosecutors, whose principal area of practice is the defense of criminal cases in the federal courts of New York.¹ NYCDL’s mission includes protecting the individual rights guaranteed by the Constitution, enhancing the quality of defense representation, taking positions on important defense issues, and promoting the proper administration of justice.

The rise in the use of personal computers, email accounts, and mobile devices has brought with it an increase in the seizure of computer evidence. Because of the voluminous and burdensome nature of such evidence, seizures have led to more frequent and extensive offsite review. And the convenience of offsite review, in turn, often spurs the Government to forgo removing the original computers and data in favor of creating “mirror images” of the originals, as it did here.² In 2003 the Government obtained a warrant to search Stavros Ganiias’s

¹ This brief is filed with leave of the Court. *See* Order, 12-240-cr, Docket No. 102 (June 29, 2015) (“We invite amicus curiae briefs from interested parties.”). Pursuant to Fed. R. App. P. 29, *amicus* affirms that no counsel for a party authored this brief in whole or in part, nor did any person, other than *amicus* or its counsel, make a monetary contribution to the preparation or submission of this brief.

² Gov’t Br. to Panel at 13 n.7 (“[A] mirror image of a computer is an exact copy of the data contained in . . . a computer hard drive.”).

accounting business for evidence against him and his clients, but in executing the warrant the Government did not remove Ganias's three computers from his office. Instead, the Government "copied every file on [the] three computers – including files beyond the scope of the warrant, such as Ganias's personal financial records." *United States v. Ganias*, 755 F.3d 125, 128 (2d Cir. 2014). But for this copying in 2003, the Government would not have possessed the files in 2006, when it applied for a warrant to search "images of three (3) hard drives seized on November 19, 2003 from the office of Steve M. Ganias" for evidence that Ganias violated "Title 26 United States code Sections 7201 and 7206(1)." (JA457.)

The Government's decision to image Ganias's computers is not surprising. In fact, such decisions are acknowledged and anticipated in a manual promulgated by the Justice Department's Computer Crime and Intellectual Property Section. The manual states that "[i]t will be infeasible in almost every case to do an on-site search of a computer In many cases, rather than seize an entire computer for off-site review, agents can instead create a digital copy of the hard drive."³ Given the Justice Department's opinion about the necessity of off-site review and the advisability of copying, the issues presented in this case are likely to be repeated in many criminal cases. NYCDL therefore has a strong interest in an important

³ Computer Crime and Intellectual Prop. Section, U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 77-78 (3d ed. 2009).

question this Court has never expressly addressed: whether the creation of a mirror image of a computer's data amounts to a seizure under the Fourth Amendment.

We submit that it does. In particular, we write to explain why a historically informed reading of the Fourth Amendment, and specifically its protection of “[t]he right of the people to be secure in their . . . papers,” makes clear that such copying of data constitutes a seizure even before an investigator actually examines the data. U.S. Const., amend. IV. The Amendment's protection of “papers” (the “Papers Clause”) embraces not only the physical object on which information is written, but also the information itself, and thus provides a sound basis for protecting computer data.

ARGUMENT

I. By Admitting that to Copy a Computer Is to Seize Its Data, the Government Has Effectively Conceded that It Violated the Fourth Amendment in this Case

The Government has conceded the key point in this case: when it made forensic mirror images of Ganias's computers in 2003, it seized the data that those computers contained. (*See, e.g.*, JA 457 (warrant to search “images of . . . hard drives *seized* on November 19, 2003 from the office of Steve M. Ganias”); and Gov't Br. to Panel at 11 (“But the warrant under which the data was *seized*...”) and 19 (“the Taxes International data that it had *seized* in November 2003”) (emphasis

added.) There is a straight line from that concession to the conclusion that the Government violated the Fourth Amendment here.

There is no dispute that in 2003 the Government lacked probable cause, and knew it lacked probable cause, to seize *all* the data on the computers; the Government has admitted as much. *Ganias*, 755 F. 3d at 137 (“The parties agree that the personal financial records at issue in this appeal were not covered by the 2003 warrant.”) The 2003 warrant authorized a seizure of hardware, software, and records relating to potential False Claims Act and theft of government property charges against Ganias’s clients; the 2003 warrant said nothing about tax charges against Ganias himself. (JA 435.)

The only reason that the Government offers for its seizure of all the data in 2003 – as opposed to just the data within the scope of the warrant – is feasibility. The Government has stated that if it could not have made a mirror image of the computers (or simply taken the original computers away), federal agents doing the review would have had to occupy Ganias’s offices for weeks or months.⁴

⁴ See Tr. Suppression Hearing, JA 397 (“Now when the warrant was actually executed at Ganias’ office, they took a mirror image of the entire set of three computers. That was a necessary requirement of practicability in that . . . it would take weeks or months to go through and find documents that are precisely identified under the list of items to be seized.”); see also Special Agent Michael Conner, Affidavit for 2003 Warrant, JA 449-51 (review had to be conducted off-site because the government needed “a controlled environment,” and because it

Practical concerns are also the Government's only basis to justify retention of the beyond-the-scope data in the years that followed the 2003 seizure. The Government states that it had to retain its complete copy of the computers in order "to prove that the image copy was identical to the original computer on the day of the search" and thereby authenticate the properly seized data for admission in court.⁵ In other words, the Government justifies its continued possession of the beyond-the-scope data after November 2003 by arguing that the data was needed to prove charges against Ganias's clients.

Despite this limited justification, in 2006 the Government obtained a warrant to search the beyond-the-scope data for evidence of an unrelated charge against Ganias himself. But regardless of what new evidence was used to support the 2006 warrant, the 2006 warrant could not, and did not, change the facts and justification of the 2003 seizure. The 2006 warrant could not provide the Government with authority to use the previously seized data in a new way. To conclude otherwise – to allow the Government to use the beyond-the-scope data for something other than authentication – would be to retroactively convert the 2003 warrant into an unlawful general warrant. Moreover, allowing a new use of the beyond-the-scope data would also create an incentive for the Government to engage in over-seizures.

was difficult to know beforehand what expertise, and thus which expert, was needed to examine a particular computer).

⁵ Gov't Br. to Panel 34; *see also Ganias*, 755 F.3d at 139.

With such a rule in place, the Government could over-seize and retain data by citing practical reasons, but with the knowledge and intent that, at some later time, it could develop independent evidence to justify a search of the data it had over-seized years before. Practical necessity in a particular case could be used to justify the assemblage and curation of a vast database for future, potential investigations.

In sum, the Government's use of the beyond-the-scope data against Ganius violated the Fourth Amendment because it exceeded the bounds of the original, authorized seizure. *See United States v. Jacobsen*, 466 U.S. 109, 124 (1984) (“[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment’s prohibition on ‘unreasonable seizures.’”) Instead of exploiting the over-seized data, the Government should have returned to Ganius’s office with its new warrant and seized the data there. The Government’s concession that imaging Ganius’s computers was a seizure therefore leads to the conclusion that the Government violated the Fourth Amendment in this case.

But the Government (or a state prosecutor) might not make such a concession in the next case. It might instead argue, as it has in other cases, that imaging a computer does not amount to seizing the data it contains, and/or that

imaged data is not “seized” until a human investigator actually looks at the data.⁶

We write to address such arguments, which may be laid to rest with a historically informed reading of the Fourth Amendment.

II. The Papers Clause Covers Information Regardless of the Medium in Which It Is Recorded

A. From its Inception, the Fourth Amendment Protected Information, Not Just Objects

The Supreme Court has declared that the Fourth Amendment’s guarantee against unreasonable searches “must provide *at a minimum* the degree of protection it afforded when it was adopted.” *United States v. Jones*, — U.S. —, 132 S. Ct. 945, 953 (2012) (emphasis in original); *see also Kylo v. United States*, 533 U.S. 27, 34 (2001). Historical inquiry into the origins of the Fourth Amendment shows that the Amendment is concerned with protecting not only the physical object on which information is written, but also, crucially, the information

⁶ *See, e.g.*, Government Brief in Support of the Magistrate’s Decision at 15 n.8, *In re Warrant To Search a certain Email Account Controlled and Maintained by Microsoft Corp.*, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (Nos. M9-150, 13-MJ-2814) (“The mere gathering of data by [an electronic communications services provider] in anticipation of disclosing it to law enforcement is not a ‘seizure’”); *see also United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026 at *3 (W.D. Wash. May 23, 2001) (copying a computer file did not amount to seizure because file “remained intact and unaltered” and “accessible to . . . any co-conspirators” of the defendant who shared access with him); *In the Matter of the Application of the United States of America for a Search Warrant for Contents of Electronic Mail*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009) (notice not required under Rule 41 of the Fed. R. Crim. P. in part because copying of an email account did not amount to seizure).

itself. For that reason, the degree of protection afforded by the Fourth Amendment at the time of its adoption provides a basis for protecting all private writings, including those in digital form.

The Fourth Amendment's protection of "papers" owes much to the controversy in England in the 1760s over general warrants, libels, and the seizure of papers in search of the authors of libels.⁷ The events were followed closely in the American colonies⁸ and later mentioned in the debates of the states' conventions to ratify the Constitution.⁹ Further, published reports of an English case arising from the controversy, *Entick v. Carrington*, (1765) 95 Eng. Rep. 807

⁷ Donald A. Dripps, "Dearest Property": *Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 61 (2013) ("The Fourth Amendment is generally seen as a response to two protests against particular abuses, the first against Writs of Assistance in the colonies in 1761–1762 and the second against general warrants in England in 1764–1765. The inspiration for singling out 'papers' in the Fourth Amendment lies in this later controversy. . . . [The Writs of Assistance] did not authorize seizure of papers, only of undutied goods.").

⁸ *Id.* at 72-77, and William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602-1791* (2009), at 583.

⁹ See, e.g., Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Indiana L.J. 979, 1036 n. 354 (2011) ("[I]n the Pennsylvania ratifying convention "Robert Whitehill . . . argued that the proposed Constitution offered "no security . . . for people's houses or papers" and that "[t]he case of [John] Wilkes, and the doctrine of general warrants show that judges may be corrupted.") (citations omitted).

(K.B), 19 How St. Tr. 1029, have been found in colonial libraries¹⁰ and discussed in Supreme Court opinions. *See, e.g., Boyd v. United States*, 116 U.S. 616 (1886); *Stanford v. Texas*, 379 U.S. 476, 483-484 (1957); and *Kyllo*, 533 U.S. at 31.

The controversy began with the publication of an anonymously authored article in *The North Briton*, a weekly periodical. The King and his ministers decided that the article contained a seditious libel and set out to find and punish its author. One of the ministers issued a general warrant to search for, seize, and arrest “the Authors, Printers, and Publishers” of the relevant article “together with their papers.”¹¹

Suspicion centered on John Wilkes, *The North Briton*’s publisher, who was a Member of Parliament and a Whig. “Every closet, bureau, and drawer in one Wilkes Residence was opened in an effort to find and confiscate the entirety of his papers.”¹² The papers included not only correspondence and manuscripts, but also books. After the search, Wilkes and others who had been arrested or searched

¹⁰ There were two published reports of *Entick v. Carrington*, Serjeant Wilson’s reports and Howell’s State Trials. The latter report is longer, and the standard citation to it is “19 How. St. Tr. 1029.” *See Dripps, supra* n. 7, at 65 n. 80. For evidence that longer report was available in America when the Fourth Amendment was proposed and ratified (between September 1787 and December 1791), see Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 Gonz. L. Rev. 1, 41 n. 260 (2009–2010).

¹¹ Dripps, *supra* n. 7, at 62.

¹² Cuddihy, *supra* n. 8, at 442.

successfully sued the officers who signed and executed the warrant.¹³

Observing Wilkes's success, John Entick, another writer whose home had been searched pursuant to warrant, brought his own suit,¹⁴ which became *Entick v. Carrington*, 95 Eng. Rep. 807, 19 How St. Tr. 1029, one of the most important precedents for the Fourth Amendment. Indeed, the Supreme Court has described *Entick* as a “‘monument of English freedom’ ‘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’” on search and seizure. *Brower v. County of Inyo*, 489 U.S. 593, 596 (1989) (quoting *Boyd*, 116 U.S. at 626).

The warrant that Entick challenged had sought his “books and papers,” and counsel for the officers argued that the search was justified because the officers were looking for a seditious libel.¹⁵ But the court held that the warrant was illegal and void,¹⁶ finding that “without any previous summons, examination, hearing . . . or proof that [Entick] was the author of the supposed libel . . . the law did not allow

¹³ *Wilkes v. Wood*, 19 How. St. Tr. 1153 (1763).

¹⁴ Dripps, *supra* n. 7, at 64.

¹⁵ *Id.* at 65; *Entick v. Carrington*, (1765) 95 Eng. Rep. 807 (K.B), reprinted in *The Complete Bill of Rights: The Drafts, Debates, Sources, and Origins* (Neil H. Cogan, ed., 1997) at 259-260.

¹⁶ Dripps, *supra* n. 7, at 65-66.

a warrant to “search for and take away all his books.”¹⁷ The court also remarked that “we can safely say there is not law in this country to justify [the King’s ministers] in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have.”¹⁸ In addition, in another, longer published report of the opinion (which has also been found in colonial libraries) the court describes papers as items that deserved protection because of their “secret nature”:

Papers . . . 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.

19 How. St. Tr. 1029. This is why papers have to be protected; the secret information they contain “will hardly bear an inspection,” much less a seizure.

The precedent that inspired the Fourth Amendment thus recognized the need to protect the privacy of people’s thoughts as reflected in two very different forms: the papers they have written without publishing (*e.g.*, manuscripts) and the papers that they have read or collected in private (*e.g.*, books). Such thoughts could not be protected merely by letting the author or reader keep the papers after government agents had reviewed them because “inspection” itself would destroy

¹⁷ Cogan, *supra* n. 15, at 259.

¹⁸ *Id.*

their “secret nature.” The point is that private thoughts and ideas, not just the objects they are written on, must be protected.

A straightforward reading of the Amendment’s text, and in particular its express protection of both “papers” and “effects,” supports the same conclusion. The category of “effects” includes physical books and manuscripts. *See Oliver v. United States*, 466 U.S. 170, 177 n.7 (1984) (“The Framers would have understood the term ‘effects’ to be limited to personal, rather than real, property.”) (citations omitted); *Altman v. City of High Point, N.C.*, 330 F.3d 194, 201 (4th Cir. 2003) (“[I]n 1791 when the Fourth Amendment was ratified, the term ‘effects’ meant goods and moveables.”).¹⁹ Thus, there would be no need to specifically protect “papers” if the Amendment were concerned only with protecting physical property such as expensive parchment or book bindings. “Papers” are specified in order to secure the words written on them—words that might show the Government the private thoughts of their author or reader. There is no good reason that recording words in digital form would change that result.

¹⁹ In *Altman* the Fourth Circuit cites *Dictionarium Britannicum* (Nathan Baily ed., 1730), which defines “effects” as “the goods of a merchant, tradesman, [etc.]”; Samuel Johnson’s *A Dictionary of the English Language* (1755), which defines the plural of “effect” as “Goods; moveables”; and the first volume of Noah Webster’s *First Edition of an American Dictionary of the English Language* (1828), which defines “effect” as “[i]n the plural, effects are goods; moveables; personal estate.”

B. The Papers Clause Extends to Information Transmitted over the Wires and Stored in Computers

Indeed, the Supreme Court followed similar logic when it recognized that the Papers Clause covered phone calls in a public phone booth. In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court held that such a call was protected despite the necessary involvement of the phone company in transmitting the call. To justify that result, *Katz* cited *Ex parte Jackson*, 6 U.S. 727 (1878), a case in which the Supreme Court wrote that sealed envelopes were protected “whilst in the mail” because “[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.” 96 U.S. at 733. By citing the relevant page from *Ex Parte Jackson*, *Katz* therefore founded its protection of phone calls on the protection for papers:

What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. *Ex parte Jackson*, 96 U.S. 727, 733.

Katz, 389 U.S. at 351-52 (other citations omitted). The Papers Clause thus safeguards both the mails and the wires.

In other words, there is ample basis to conclude, as the Panel did here, that the Fourth Amendment’s protections “apply to modern computer files.” *Ganias*, 755 F.3d at 135. “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." *Id.*; *see also United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) ("Our Founders were indeed prescient in specifically incorporating 'papers' within the Fourth Amendment. . . . The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities.").

In fact, as the Panel also noted, it is conceivable that computer data deserves "even greater protection" than traditional, "analog" papers. 755 F.3d at 135. The issue is not only that millions of people now use computers to store greater *quantities* of information than they ever kept on paper, but also that they are storing new *categories* of information—information they never wrote down before. As the Supreme Court has observed, "certain types of [computer] data are qualitatively different [from physical records] [Internet] browsing history, for example . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *United States v. Riley*, 134 S. Ct. 2473, 2490 (2014); *see also United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Website they had visited in the last week, or month, or year.")

In sum, computers contain information that is as private as traditional papers, only more so: “With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’” *Riley*, 134 S. Ct. at 2492-95 (citing *Boyd*, 116 U.S. at 630). “[S]uch information is . . . worthy of the protection for which the Founders fought.” *Id.*

III. To Copy a Computer Is to Seize the Data It Contains

A historically informed reading of the Papers Clause thus leads to the recognition that the Papers Clause protects the privacy of information regardless of whether it is written in ink or code. That recognition, in turn, leads to the understanding that to image a computer’s data is to seize it. A diarist’s possessory interest in her diary is not simply that she is allowed to write in it and read it, but that she can keep its contents private. As the court in *Entick v. Carrington* observed, “where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass.” 19 How. St. Tr. 1029. The diarist’s possessory interest includes the ability to reasonably exclude others. So, too, with Ganius’s personal financial records before the Government imaged his computers; his possessory interest in the records included their privacy.

Once the Government imaged the data on Ganius’s computers, however, the situation changed. Any choice by Ganius to alter or delete records on the original computers could not alter the potential evidence in the Government’s possession;

the Government was in control. As the panel stated in its opinion, “a seizure occurs when the Government interferes in some meaningful way with the individual’s possession of property.” *Ganias*, 755 F.3d at 133 (citing *Jones*, 132 S. Ct. at 951 n.5). That is precisely what happened here. When the Government imaged Ganias’s computers it undermined the privacy of Ganias’s data just as if the computers themselves had been actually “removed and carried away.” 19 How. St. Tr. 1029. Ganias’s ability to delete, alter, or correct some of the original data was thwarted by the Government’s possession of a mirror image copy.

None of this is to say that all copying of information is always a seizure. When a government investigator observes items in plain view,²⁰ and writes down or photographs what she observes, that act of recording does not transform the human observation into a seizure. It “merely preserves the human observation in a fixed form.” Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 714 (2010); *see also id.* at 716. Whether the item observed happens to be written text does not affect the analysis. In *Arizona v. Hicks*, 480 U.S. 321 (1987), the Supreme Court held that when a government investigator observed and then wrote down serial numbers on a stereo, “the mere recording of the serial

²⁰ Under the “plain view” doctrine, government agents can ordinarily seize evidence or contraband without a warrant if the initial intrusion that brought the agents within plain view of the item was itself lawful and the incriminating nature of the item is immediately apparent. *See generally* 3 Wayne LaFave et al., *Search & Seizure* § 7.5(a) (5th ed.).

numbers did not constitute a seizure” because it “did not meaningfully interfere with [the] respondent’s possessory interest in either the serial numbers or the equipment.” *Id.* at 324 (quotations omitted).

But electronic copying of the kind needed to image a computer is different. It “adds to the information in the government’s possession by copying that which the government has not observed.” Kerr, *Seizures* at 714. The creation of such a copy is not merely “an aid to memory,” it “freeze[s] the [crime] scene.” *Id.* at 717.²¹ Furthermore, computers contain so much data that it is unlikely, to say the least, that the majority of what they contain will be observed on-site by Government investigators while they search a house or office. It would be absurd to assume that the mirror imaging of a hard drive (or in Ganas’s case, three hard drives) was merely an aid to an investigator’s memory.

Further, imaging a computer is also different from photographing objects such as stereos or guns because the latter are not “papers” for purposes of the Papers Clause. Despite their not-infrequent importance in criminal cases, the serial numbers on guns do not transform guns into informational goods like books or manuscripts. In contrast, the words written in a diary and the data contained in an

²¹ Similarly, photocopying or photographing documents should, in general, be considered a seizure. Kerr, *Seizures* at 717-18 (discussing *United States v. Jefferson*, 571 F. Supp. 2d 696 (E.D. Va. 2008).)

internet browsing history are not incidental to the diary or the computer, they are central to the diary or computer's value to their users. "[C]omputer environments are data environments," and in a data environment "data is simply more important than hardware." Kerr, *Seizures* at 712. In fact, because computer users are aware that "[h]ardware is increasingly fungible," . . . [u]sers often generate multiple copies of their most valuable data to ensure that their data is protected from destruction no matter what happens to the hardware that happens to store it." *Id.* In other words, users treat their computer data like their personal papers. This Court should too.

CONCLUSION

For the reasons stated above, the Court should vacate the judgment of conviction and reinstate the panel's holding.

Dated: New York, New York
July 29, 2015

Respectfully submitted,

NEW YORK COUNCIL OF DEFENSE LAWYERS

By: /s/ Michael L. Yaeger

Michael L. Yaeger
Barry A. Bohrer
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, New York 10022
Telephone (212) 756-2000
Facsimile (212) 593-5955

Attorneys for New York Council of Defense Lawyers

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, I certify that, according to the word-count feature of the word processing program, this brief contains 4,617 words, including headings, footnotes and quotations, but excluding the parts exempted by Fed. R. App. P. 32(a)(7)(B)(iii), and therefore is in compliance with the type-volume limitations set forth in Rule 32(a)(7)(B).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in proportionately spaced typeface using Microsoft Word 2010 and in 14-point Times New Roman font.

Dated: New York, New York
July 29, 2015

Respectfully submitted,

NEW YORK COUNCIL OF DEFENSE LAWYERS

By: /s/ Michael L. Yaeger

Michael L. Yaeger
Barry A. Bohrer
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, New York 10022
Telephone (212) 756-2000
Facsimile (212) 593-5955