THE YALE LAW JOURNAL

ORIN S. KERR

Fourth Amendment Seizures of Computer Data

ABSTRACT. What does it mean to "seize" computer data for Fourth Amendment purposes? Does copying data amount to a seizure, and if so, when? This Article argues that copying data "seizes" it under the Fourth Amendment when copying occurs without human observation and interrupts the stream of possession or transmission. It offers this position by reaching back to the general purposes of regulating seizures in Fourth Amendment law and then applying those functions to the new environment of computers. The test prevents the government from copying data without regulation and yet also meets and answers the objections that have puzzled scholars and made it difficult to apply the old definition of seizures in the new computer environment.

AUTHOR. Professor, The George Washington University Law School. Thanks to Paul Ohm and Susan Brenner for comments on an earlier draft.

ARTICLE CONTENTS

INTRODUCTION

Imagine the police take away a suspect's computer, make a digital copy of its contents, and then give the computer back to the suspect. The police do not open the copy, but they keep it in their custody in case they need to access it later. Does the combined act of copying the files and retaining the copy trigger the Fourth Amendment?

Next imagine that FBI agents believe a particular person is using the Internet to commit a crime. Agents install a surveillance tool at the target's Internet service provider (ISP), and the tool generates copies of all of the target's incoming and outgoing email. The email is copied to a file, but no human being actually looks at the file. Instead, the agents keep the file in case they develop probable cause to look through it for evidence. Again, does the Fourth Amendment allow it?

The answer to both scenarios depends on whether copying computer files without looking at them constitutes a Fourth Amendment "seizure."[1] If copying a computer file amounts to a seizure, then the government cannot make and retain a copy absent special circumstances. On the other hand, if copying is not a seizure, then the government can make and retain the copy without restriction. The Fourth Amendment will limit looking through the copy because that is a Fourth Amendment "search."[2] But what if the government wants to make a copy and hold it? Does that constitute a "seizure"?

The answer is tremendously important, as it determines the legal framework that governs almost every digital evidence investigation. Computer search and seizure inverts the usual pattern of criminal investigations. When searching for traditional physical evidence, the police first search for property and then seize it. Computer technologies often require investigators to obtain a copy first and then search it later.[3] Nearly every case begins with copying data that will later be searched, and government investigators often will prefer to copy more rather than less if the Fourth Amendment allows it.

1. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

2. *See, e.g.*, United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991).

3. *See, e.g.*, United States v. Hill, 459 F.3d 966, 973-75 (9th Cir. 2006) (noting the technological reasons why the computer forensic process often does not permit an on-site search).

The question is also doctrinally uncertain. The Supreme Court has said that a seizure of property occurs when government action meaningfully interferes with an individual's possessory interests in that property.[4] This could be interpreted in two different ways. On one hand, perhaps copying does not interfere with a possessory interest because that interest is limited to hardware and the copy of the data it stores. On the other hand, perhaps copying interferes with a possessory interest because a possessory interest extends to both the original *and any copies made from it*. The test itself does not suggest an answer. To make matters more complicated, precedents from earlier technologies such as physical copying, photographic copying, and wiretapping are decidedly mixed.[5] The Supreme Court's decisions that touch on the question are rather hard to decipher. The Court held in one case that copying a number does not seize anything, while it strongly suggested in another case that copying data does seize it.[6] Whether and when copying amounts to a seizure remains an unsolved puzzle.

This Article attempts to solve the puzzle by offering a test for when copying data constitutes a Fourth Amendment seizure. It argues that copying data "seizes" it under the Fourth Amendment when copying occurs without human observation and interrupts the course of the data's possession or transmission. It arrives at this definition by reaching back to the general purposes of regulating seizures in Fourth Amendment law and then applying those functions to the new environment of computers. The test it offers prevents the government from copying data without regulation, and yet also answers the objections that have puzzled scholars and made it difficult to apply the old definition of seizures in the new environment.

Under my approach, copying is neither *never* nor *always* a seizure. Whether copying amounts to a seizure depends both on whether it is pre-observation or post-observation and on whether it interrupts the intended transmission or use of the data. Past technologies have not raised the need for these distinctions, as copying has always been post-observation: a person has needed to see data in order to copy it. Computers permit machine copying without human observation, which requires a more nuanced understanding of when copying constitutes a seizure. The new approach reconciles the case law from prior technologies and then suggests a workable definition that sensibly translates

4. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

5. *See infra* Section I.B.

6. *Compare* Arizona v. Hicks, 480 U.S. 321, 324 (1987) (holding that copying is not a seizure), *with* Berger v. New York, 388 U.S. 41, 54-55 (1967) (suggesting that electronic wiretapping is a "search and seizure").

the traditional physical concept of Fourth Amendment seizures to a digital environment.[7]

Finally, this Article acknowledges a change in my own thinking. A few years ago, I argued that mere copying should not be considered a Fourth Amendment seizure.[8] I acknowledged that copying ordinarily will be regulated by the Fourth Amendment. To my mind, however, copying was at most regulated by the restrictions on searches rather than seizures, and those restrictions were limited to copying that interfered with the operation of the machine from which the copy was made. I have now concluded that my prior approach was wrong. My earlier approach did not recognize the importance of access to data in the regulation of government evidence collection. Further, my earlier approach did not appreciate that a middle ground was possible to avoid some of the overbroad results that seem to follow from labeling copying a seizure. This Article identifies the new middle ground and explains why I now reject my earlier view.

The Article contains four Parts. Part I introduces the difficult question of whether copying data seizes it. Part II presents the basic argument for why copying should be considered a seizure. Parts III and IV introduce two key limitations. Part III limits seizures to copying without human observation, and Part IV limits seizures to copying outside the course of delivery or possession.

I. THE SEIZURE PUZZLE

Criminal investigators often obtain copies of computer files without first looking through them. Because computers can store a remarkable amount of information, sifting through the data can be very time-consuming. Faced with this reality, investigators often prefer to copy first and search later.[9] The digital copies remain on a government computer awaiting viewing and analysis. Whether that copying and storage amounts to a Fourth Amendment seizure

7. This Article deals only with the threshold question of when copying amounts to a seizure. The Fourth Amendment does not prohibit all seizures; it prohibits only those seizures that are constitutionally unreasonable. The next project for courts and commentators will be to determine when a seizure is lawful, and in particular when a warrantless seizure is lawful.

8. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 557-62 (2005).

9. *See* COMPUTER CRIME & 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) ("Because examining a computer for evidence of crime is so time consuming, it will be infeasible in almost every case to do an on-site search of a computer or other storage media for evidence of crime. . . . In many cases, rather than seize an entire computer for off-site review, agents can instead create a digital copy of the hard drive that is identical to the original in every relevant respect.").

remains unclear. This Part explains why the answer is unclear, setting up the puzzle that the rest of the Article will attempt to solve.

A. Introduction to the Seizure Puzzle

The Fourth Amendment rules for collecting physical evidence are well established. The Fourth Amendment prohibits unreasonable searches and seizures.[10] When the government invades a private space, violating a reasonable expectation of privacy, that invasion constitutes a search.[11] When the government then spots evidence or contraband and takes it away for use at trial, that physical taking of the evidence amounts to a seizure.[12] As the Supreme Court has explained, a seizure of property occurs when the government meaningfully interferes with a person's possessory interest in property.[13] The definition of a seizure is easy to apply to physical property. Physical property is possessed when a person has knowledge and control over it.[14] As a result, a seizure of physical property occurs when the government takes control of the property and denies control to others.

But how should this apply to computer data? If computer hardware stores data, and the government takes the hardware away, then surely the data it contains is seized along with the hardware.[15] But what if the government copies the data onto its own storage device and leaves the original copy undisturbed? At that point courts face a difficult choice. If the possessory interest that the Fourth Amendment protects refers only to the original, then the government's creation of a copy does not interfere with the owner's possessory interest and does not amount to a seizure. On the other hand, if the possessory interest that the Fourth Amendment protects refers to the data itself—the original, or any copy made from it—then the copying does interfere with the possessory interest and is a seizure. The question is this: does the possessory interest refer to control of the original data, or does it refer to control of the data itself, including any copies?

10. U.S. CONST. amend. IV.

11. *See* Smith v. Maryland, 442 U.S. 735, 739-40 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

12. United States v. Jacobsen, 466 U.S. 109, 120 (1984).

13. *Id.* at 113.

14. *See, e.g.*, Maryland v. Pringle, 540 U.S. 366, 369-72 (2003) (discussing Maryland narcotics law); United States v. Iafelice, 978 F.2d 92, 96 (3d Cir. 1992) (discussing federal narcotics law).

15. *Cf.* Brendlin v. California, 127 S. Ct. 2400, 2406 (2007) ("[D]uring a traffic stop an officer seizes everyone in the vehicle, not just the driver.").

B. Precedents on Copying as a Seizure

Existing precedents are divided on whether copying information constitutes a Fourth Amendment seizure. Some decisions hold or strongly suggest that copying is not a Fourth Amendment seizure, while others hold or strongly suggest that it is. The leading case for the view that copying does not constitute a seizure is *Arizona v. Hicks*.[16] In *Hicks*, a police officer searching an apartment under exigent circumstances saw an expensive stereo in an otherwise squalid apartment. He suspected that the stereo was stolen, so he lifted up the stereo, observed the serial number, and wrote the number down. The officer later used the number to confirm a match between the stereo he saw and equipment that had been reported stolen. The Supreme Court held that copying the serial number did not seize anything. "[T]he mere recording of the serial numbers did not constitute a seizure," the Court held, as "it did not 'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment."[17]

The Sixth Circuit followed *Hicks* in a case involving photography, *Bills v. Aseltine*.[18] In *Aseltine*, the police executed a warrant to search a home for stolen mechanical equipment. The officers took photographs inside the home of items beyond the scope of the warrant, including guns in a gun rack, a marijuana plant, and additional stolen property. The homeowner later sued, claiming that the government had seized items beyond the scope of the warrant by taking the photographs. The Sixth Circuit rejected the argument based on *Hicks*. According to the court, photographing the item in plain view was not a seizure: "the recording of visual images of a scene by means of photography does not amount to a seizure because it does not 'meaningfully interfere' with any possessory interest."[19]

Two district courts have applied this rationale to conclude that copying computer files does not seize them. In *United States v. Gorshkov*,[20] FBI agents downloaded a file stored on a remote server and held the copy of the file until a warrant was obtained. The district judge ruled that copying the file did not seize it because it "remained intact and unaltered," "accessible to Defendant and any co-conspirators or partners with whom he had shared access." As a result, the copying "had absolutely no impact on [the defendant's] possessory

16. 480 U.S. 321 (1987).

17. *Id.* at 324.

18. 958 F.2d 697 (6th Cir. 1992).

19. *Id.* at 707 (quoting *Hicks*, 480 U.S. at 324).

20. No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

rights."[21] Another district court suggested a similar result in a case on whether the Fourth Amendment requires notice, and to whom, when the government obtains a search warrant to collect the contents of an email account.[22] The judge noted that Rule 41 of the Federal Rules of Criminal Procedure provides for notice when property is seized, but then concluded that copying the contents of the account did not seize anything.[23] No property was "actually taken or seized as that term is used in the Fourth Amendment context," the court reasoned, "due to the nature of electronic information, which can be accessed from multiple locations, by multiple people, simultaneously."[24] The absence of a seizure meant that no notice was required.[25]

Other decisions have applied a very different approach. In *United States v. Jefferson*,[26] the FBI obtained a warrant to search a Congressman's home for evidence of fraud and bribery offenses. The agents located and removed paper documents described in the the warrant, but they also took high-resolution photographs of thirteen additional documents that were arguably beyond the warrant's scope.[27] When review of the photographs revealed criminal activity and the government sought to use them at trial, the district court ruled that photographing the additional documents had seized them.[28] According to the court, "the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself."[29] Taking photographs or writing down notes of what the officers saw interfered with the owner's "sole possession of the information contained in those documents" and was, therefore, a Fourth Amendment seizure.[30]

Although *Jefferson* is only a district court case, the Supreme Court has handed down several decisions that hint at a similar approach. In *Berger v. New York*,[31] the Supreme Court struck down a wiretapping statute on the grounds

21. *Id.* at *3.

22. In the Matter of the Application of the United States of America for a Search Warrant for Contents of Electronic Mail, __ F. Supp. 2d __, 2009 WL 3416240 (D. Or. June 23, 2009).

23. *Id.* at *10.

24. *Id.*

25. *Id.*

26. 571 F. Supp. 2d 696 (E.D. Va. 2008).

27. *Id.* at 699-700.

28. *Id.* at 704.

29. *Id.* at 702.

30. *Id.* at 703-04.

31. 388 U.S. 41 (1967).

that the statute did not provide sufficient constitutional protection. The majority opinion in *Berger* repeatedly referred to the act of wiretapping as a "search and seizure."[32] The Court used the same phrase in *Katz v. United States*,[33] a case on the constitutionality of bugging. Agents had placed a microphone on a public telephone and recorded one end of a suspect's conversation without a warrant. Although the Court's holding that this violated the Fourth Amendment has been understood to concern the search power, the Court repeatedly referred to the agents' conduct as a "search and seizure."[34] The conjunctive phrase in both *Berger* and *Katz* suggests that recording the surveillance was understood as a seizure.

The case law on Rule 41 of the Federal Rules of Criminal Procedure also suggests that copying information constitutes a seizure. Rule 41 governs search warrants, and it authorizes federal courts to issue warrants to "search for and seize" evidence.[35] In *United States v. New York Telephone Co.*,[36] the Supreme Court held that this power allowed the government to install a surveillance device that copied each number dialed from an outgoing telephone. According to the Court, the power to "'search for and seize'" evidence "encompass[ed] a 'search' designed to ascertain the use which is being made of a telephone suspected of being employed as a means of facilitating a criminal venture and the 'seizure' of evidence which the 'search' of the telephone produces."[37] Although not a model of clarity, *New York Telephone*, together with *Berger* and *Katz*, suggests that the recording of information "seizes" it.

Lower courts applying the Fourth Amendment to copied computer data have often echoed this approach by simply assuming that copying data seizes it. For example, in a recent en banc decision by the Ninth Circuit, *United States v. Comprehensive Drug Testing, Inc.*,[38] the court affirmed an order to return seized property consisting of a computer file copied from a third party's server

32. *See, e.g.*, *id.* at 54, 55, 57.

33. 389 U.S. 347 (1967).

34. *Id.* at 353-54 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a '*search and seizure*' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance. The question remaining for decision, then, is whether the *search and seizure* conducted in this case complied with constitutional standards." (emphasis added)).

35. FED. R. CRIM. P. 41(b)(1).

36. 434 U.S. 159 (1977).

37. *Id.* at 169 (quoting FED. R. CRIM P. 41(b)).

38. 579 F.3d 989 (9th Cir. 2009).

during an on-site search. The court repeatedly characterized the copied data as "seized data."[39] This assumption was made explicit in a section of the opinion announcing new prospective rules for the search and seizure of electronic evidence.[40] One of the new rules requires the government to justify the possession of data copied during the execution of a warrant that is beyond the scope of the warrant: "[i]f the government believes it is entitled to retain data as to which no probable cause was shown in the original warrant," the court ordered, "it may seek a new warrant or justify the warrantless seizure by some means other than plain view."[41] Although the opinion contains no analysis of why the copying or continued retention of the data counted as a seizure, it plainly suggests that the judges believed it was.

II. SOLVING THE SEIZURE PUZZLE

This Part solves the seizure puzzle by arguing that electronic copying by the government ordinarily constitutes a Fourth Amendment seizure. The reason is that the Fourth Amendment power to seize is the power to freeze. That is, the seizure power is the power to hold the crime scene and control evidence. Generating an electronic copy of data freezes that data for future use just like taking physical property freezes it: it adds to the amount of evidence under the government's control. From the standpoint of regulating the government's power to collect and use evidence, generating an electronic copy is not substantially different from controlling access to a house or making an arrest. Each of these seizures ensures that the government has control over the person, place, or thing that it suspects has evidentiary value. As a result, copying Fourth Amendment protected data should ordinarily be considered a Fourth Amendment seizure.

39. *See id.* at 995 ("The warrant also contained significant restrictions on how the seized data were to be handled."); *id.* at 999 ("A lack of candor in this or any other aspect of the warrant application shall bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."); *id.* ("The government also failed to comply with another important procedure specified in the warrant, namely that 'computer personnel' conduct the initial review of the seized data and segregate materials not the object of the warrant for return to their owner.").

40. *Id.* at 998-1001.

41. *Id.* at 1001.

A. The Power To Seize as the Power To Freeze

The general purpose of the Fourth Amendment is to regulate police collection and use of evidence so that police practices are reasonable. Police officers want to collect evidence to bring cases that prosecutors can charge, and they need two distinct types of power to do this successfully. First, they need the power to uncover and expose evidence so they can see it and recognize its importance to criminal cases. Second, they need the power to "freeze" evidence to maintain custody of it, preserve the status quo pending further investigation, and bring the evidence into court for prosecution. The first power is the power to expose what is hidden, and thereby learn facts that were previously unknown. The second power is the power to secure the scene and add to the potential evidence under the government's control so eventually it can be used in court.

The two powers work together. To see how, consider a typical automobile traffic stop in which a police officer is hoping to find drugs in the trunk of a car. First, the officer must freeze the scene and bring it under his control. That is, he needs to bring the car to a stop, and he needs to make sure the driver and any passengers are under his control so he can ask them questions and investigate further. After he gains control of the car, he needs to find the drugs in the car. He needs to open up the closed compartments of the car and open any wrappers to expose the drugs inside. Finally, the officer must take away the drugs and any evidence of their storage so he can bring them to the prosecutors. That is, he must freeze the scene as it relates to the evidence of the crime, establishing a chain of custody so the facts he observed can be proved at trial. The prosecutors will then build the case based on the drugs removed from the car and the officer's testimony of where and how he found them.

How does the Fourth Amendment regulate these two powers? The power to expose what is hidden falls under the Supreme Court's regulation of searches. Exposing what is hidden will ordinarily violate a suspect's reasonable expectation of privacy, and will therefore be a Fourth Amendment search that requires a warrant or some exception to the warrant requirement such as consent or exigent circumstances.[42] In contrast, the power to freeze the scene falls under the Supreme Court's precedents on seizures. Stopping the car amounts to a seizure of the car, its driver, and the passengers.[43] Taking away the drugs seizes the drugs.[44] The two powers reflect the two categories of police

42. *See* Katz v. United States, 389 U.S. 347 (1967).

43. *See* Brendlin v. California, 127 S. Ct. 2400 (2007).

44. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

conduct that the Fourth Amendment expressly regulates: the power to search is the power to expose, and the power to seize is the power to freeze.

A quick review of how the courts interpret the seizure power demonstrates that the power to seize is, at bottom, the power to freeze a scene for further investigation or prosecution. In the case of movable property, property is seized when it is taken away from the person who has lawful control over it.[45] At that stage, the person can no longer interfere with the item seized: it is in police custody, not the individual's. In the case of immovable property, such as a house, the house is seized when the police stop its residents from being able to enter. Blocking access to the home to stop individuals from entering and potentially destroying evidence inside amounts to a seizure of the home.[46]

The same principle governs seizures of individuals. If the police execute a *Terry* stop,[47] temporarily forcing an individual to stay where he is while police investigate, he is seized as soon as the police indicate that he is not free to go.[48] In that case, the power to seize is the power to temporarily stop a person for more investigation. And, of course, the same holds for arrests. When the police arrest a suspect, seizing him, they keep him from being able to get away pending charges and either pretrial detention or release on bond. In all of these settings, the power to seize is the power to freeze; that power to freeze adds to the evidence under the government's control.

B. Copying as Freezing

In my view, the most consistent way to apply the Fourth Amendment seizure doctrine to computer data is to hold that electronic copying ordinarily seizes it under the Fourth Amendment. When the government makes an electronic copy of data, it obtains possession of the data that it can preserve for future use. To be sure, subsequently viewing the data in the copy and thus exposing its contents ordinarily amounts to a Fourth Amendment search.[49] But obtaining the copy itself serves the traditional function regulated by the seizure power: it freezes whatever information is copied, preserving it for future access by government investigators. Generating an electronic copy of data freezes that

45. *See* Soldal v. Cook County, 506 U.S. 56, 61-62 (1992).

46. *See* Illinois v. McArthur, 531 U.S. 326 (2001) (holding that a seizure of a home occurred when police blocked the owner from reentering).

47. *See* Terry v. Ohio, 392 U.S. 1 (1968).

48. *Id.* at 16-20.

49. *See, e.g.*, United States v. David, 756 F. Supp. 1385, 1392 (D. Nev. 1991); Kerr, *supra* note 8, at 560-62.

data for future use just like taking physical property freezes it. From the standpoint of regulating the government's power to collect and use evidence, generating an electronic copy is no different from controlling access to a house or making an arrest: it ensures that the government has control over the person, place, or thing that it suspects has evidentiary value.

Granted, an important difference separates physical seizures from electronic seizures. When the government conducts a physical seizure, it interferes with the owner's right to control the item seized. If the government seizes a person's car, the person cannot drive it; if the government arrests a person, he cannot walk away. Only one person can control the physical item at a time, and freezing by the government means that the suspect loses control. That is not true with data, of course. Data is nonrivalrous, so the government can create a copy of the data in a way that does not take away the suspect's possession of his own copy.[50] As a result, computer data severs the connection between the information and the storage device. The question is, should the law focus on when a person loses exclusive rights to the device, or when a person loses exclusive rights to the data?

The law should focus on when the person loses exclusive rights to the data. The reason is that computer environments are data environments. In a world of data, whether an individual has access to a particular copy of her data has much less significance than whether the government has obtained a copy of the data for possible government use in the future.[51] This is true for three reasons. The first reason is that in an environment of data, data is simply more important than hardware. Hardware is increasingly fungible. Hard drives crash. Thumb drives get lost. Networks go down. To most users, what matters is the data. Users 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. Given the importance of data, and the frequent existence of multiple copies of it, there is little difference between (a) taking a physical device that contains data and (b) copying the data without taking the device.

The second reason is related, but more specific: when the government takes away hardware, agents can generate a copy of data from seized devices and provide the copy to the suspect. Given this reality, it makes little sense to draw a distinction between copying data and removing physical storage devices.

50. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001); Kerr, *supra* note 8, at 560-62.

51. *See* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf.

Imagine two scenarios. In the first scenario, the government copies the data on the suspect's machine but allows the suspect to keep the physical hardware. In the second, the government takes away the suspect's machine but quickly generates an electronic copy and provides it to him to minimize his inconvenience. No one questions that the latter is a seizure. The target's computer plainly has been seized, along with the data it contains. But the only serious difference between these two scenarios is that the government keeps the hardware in one but not in the other. That difference seems quite minor; loss of hardware is a small burden relative to loss of data. The same legal rule should regulate both situations.

Finally, in computer search cases, the data—not the hardware—is normally the key evidence the government needs to prove its case and obtain a conviction. Data reigns supreme. Government control of data provides the link that empowers the prosecution to charge people with crimes that will take away their freedom. As a result, the difference between merely copying data and actually taking away hardware is a modest one. To be sure, access to hardware is important to many people. But the power to deny a person his hardware does not measure on the same scale as the power to deny a person his freedom. The law should focus on the more important question of the government's power to control evidence rather than the less important question of a person's access to his computer.

For these reasons, courts should construe the seizure power so that electronically copying data ordinarily "seizes" it. The government should not be able to copy a person's protected information without triggering the Fourth Amendment's seizure authority and, therefore, requiring justification such as a warrant or an exception to the warrant requirement.[52] In the next two Parts, I explain two limitations on this rule. Not all copying is a seizure. Instead, only copying without human observation that interrupts the intended transmission or possession of the data triggers the seizure authority.

52. I, therefore, conclude that the district court's contrary analysis in *Gorshkov*, 2001 WL 1024026, is incorrect. Assuming Gorshkov had Fourth Amendment rights under *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), the copying of his Fourth Amendment-protected files did seize them. The district court should then have turned to whether the seizure was constitutionally reasonable because the officers could not have obtained a warrant to seize files in Russia, and they did obtain a warrant in the United States before searching the copied files.

III. THE LIMITATION OF COPYING WITHOUT HUMAN OBSERVATION

The conclusion that electronically copying data "seizes" it will have a satisfying ring for most readers. It avoids the Orwellian result that the government can copy everyone's data and then hold it without any Fourth Amendment oversight. So far, so good. But this approach raises a serious difficulty: How should courts distinguish the cases holding that taking a photograph and writing down observed numbers do not "seize" anything? Are those cases simply incorrect? Or are they somehow distinguishable? And if they are distinguishable, what do those cases tell us about when copying amounts to a seizure?

In an earlier article, I argued that these precedents rendered it difficult to conclude that electronic copying was a seizure.[53] I recognized that some limitation on electronic copying was needed; as I wrote then, "[t]he idea that the government could freely generate copies of our hard drives and indefinitely retain them in government storage seems too Orwellian—and downright creepy—to be embraced as a Fourth Amendment rule."[54] But *Hicks* and *Aseltine* seemed correct to me, and I could find no way to distinguish them from digital copying. I, therefore, reasoned that the intuitively necessary limitations should come from the Fourth Amendment's regulations on searches instead of seizures.[55]

I now see that my earlier approach was wrong, and that electronic copying of computer files is different in a critical way from writing down information or taking a photograph. Writing down information or taking a photograph merely preserves the human observation in a fixed form. In contrast, electronic copying adds to the information in the government's possession by copying that which the government has not observed. The two types of copying should be treated differently; the former should not be treated as a seizure while the latter should.

This distinction explains why cases such as *Arizona v. Hicks*[56] and *Bills v. Aseltine*[57] are both correct, and why these cases are distinguishable from the context of electronic copying. Not all copying amounts to a seizure. Only copying of data that has not been exposed to human observation by a government agent amounts to a seizure, because only that copying involves

53. *See* Kerr, *supra* note 8, at 562.

54. *Id.* at 560.

55. *Id.* at 561-62.

56. 480 U.S. 321 (1987).

57. 958 F.2d 697 (6th Cir. 1992).

freezing the scene and adding to the information in the government's possession. Because electronic copying normally involves copying without observation, electronic copying amounts to a seizure even though taking a photograph or writing down information does not "seize" anything for Fourth Amendment purposes.

A. Copying as Freezing Versus Copying as an Aid to Memory

Recall the two basic powers that the Fourth Amendment regulates. The first power is the government's power to expose, regulated by the prohibition on unreasonable searches, and the second power is the government's power to freeze the scene, regulated by the prohibition on unreasonable seizures.[58] In the course of investigating a case, government agents will need to do more than just expose evidence and freeze the scene. After a government agent has exposed private material, constituting a search, the agent may recognize that his observation has possible use in a future criminal prosecution. The officer will want to preserve what he has learned. He will take steps to remember what he has seen in order to generate reliable evidence.

Police officers often generate copies to preserve what they have observed. After investigating a crime scene, the officer may write a report. When called to the scene of a car accident, he might take pictures to reconstruct the accident more accurately. To create a record of the event, the officer might record a suspect's confession. In all of these cases, the officer uses devices to record what he has already observed. Making the recording and writing down what he has observed both serve as reminders to the officer of what he saw, helping his memory, and also serve as evidence superior to the officer's own first-hand recollection when he takes the stand to testify. Instead of simply recalling what he saw from memory alone, the officer can take the stand at trial and authenticate the recording or text as an accurate rendition of what he observed. The jury can then view the recording or read the contemporaneously written text and can assess whether the government has established proof beyond a reasonable doubt.

Critically, the power to preserve what an officer observes is different from the power to freeze the scene. The end result is the same, as the government gets a copy. But the two powers are different. The power to record what has been observed is designed to minimize loss; government agents use tools to avoid forgetting what they have learned. In contrast, the power to freeze the scene adds to what the government controls. Government agents take some

58. *See supra* Section II.A.

evidence that was beyond the government's control and bring it within the government's control. The power to freeze the scene thus provides the opportunity for the government to use its search powers to collect evidence and then use it against a suspect. The power to preserve observations does not add to the government's power to collect evidence; it merely provides a way to retain information already collected.[59]

B. Copying as an Aid to Memory in Hicks *and* Aseltine*, and the Close Case of* Jefferson

The distinction between copying-to-aid-memory and copying-to-add-to-government-control explains why cases such as *Arizona v. Hicks*[60] and *Bills v. Aseltine*[61] do not compel the result that digital copying does not seize anything. Recall that in *Hicks*, the officer picked up a turntable, observed the serial numbers on the bottom, and then wrote down the serial numbers he observed.[62] The writing down of the numbers itself did not freeze the scene, adding to that which was under the government's control. Rather, it simply recorded what already was in the officer's own mind. When the officer wrote down the numbers, he recalled what he had just observed and transferred that imprint from his mind to the piece of paper. The act of copying simply acted as an aid to the officer's memory of what he had already observed.

The same is true of *Bills v. Aseltine*.[63] In *Aseltine*, an officer took pictures in the plaintiff's home while executing a warrant there. The plaintiff sued, arguing that taking photographs in the home "seized" images of it. Once again, the creation of an image merely recorded what the officer had already seen: it acted as a permanent version of his memory. The technology used was more sophisticated than just writing down numbers or trying to make an accurate drawing of what the officer observed. The camera enabled a more accurate and trustworthy "writing down" of what the officer saw. But the function remained the same: the officer used tools to generate a copy of what he had already seen, thus aiding his memory and creating a reliable evidentiary record.

59. *Cf.* Illinois v. Andreas, 463 U.S. 765, 771 (1983) ("[O]nce police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost.").

60. 480 U.S. 321.

61. 958 F.2d 697.

62. 480 U.S. at 324.

63. 958 F.2d 697.

In my 2005 article,[64] I concluded that cases like *Hicks* and *Aseltine* compelled the conclusion that generating a copy of a computer file did not seize it. As I wrote at the time, a contrary approach would require "[d]eparting from *Hicks*."[65] I now see, however, that I overlooked the distinction between pre-observation copying-as-freezing and post-observation copying-as-aid-to-memory. The key distinction is that computer technologies allow the creation of a copy without the intermediary of human observation. As a result, they allow the creation of a copy to freeze the scene, rather than merely as an aid to memory. When a government agent copies a file or drive, he generates a copy in order to freeze the scene. The agent generally will not know the contents he has copied; he simply knows that he is obtaining a copy of whatever happens to be on the storage device.

Hicks and *Aseltine* are distinguishable from cases involving electronic copies because they involve a different kind of copying. Copying an electronic file will ordinarily seize it, because it brings a copy of the data into the government's possession. It freezes the scene, adding to what the government controls, just like a traditional seizure. *Hicks* and *Aseltine* deal with a different type of copying, a more traditional copying in which the copying merely preserves what has been already observed by police investigators to counter the inevitable fading of human memory. As a result, it merits different treatment under the Fourth Amendment.

The basic distinction between copying-to-aid-memory and copying-as-freezing resolves many cases, but it is worth noting that it leaves others unclear. The facts of *United States v. Jefferson*[66] demonstrate the difficulty. In *Jefferson*, FBI agents took high-resolution photographs of documents that helped reveal evidence of public corruption. The district court's opinion does not indicate how closely the agents looked at the documents before photographing them, but assume the agents saw enough to think the documents might help the investigation but not enough to understand what they observed. Did the photography merely aid the agents' memory or did it freeze the scene? The precise line is difficult to draw, because brief viewing does not necessarily imply the mental appreciation needed to make copying merely an aid to memory. Should brief viewing suffice? Or should the law require more, such as subjective understanding or a level of appreciation of the information viewed?

64. Kerr, *supra* note 8.

65. *Id.* at 562.

66. 571 F. Supp. 2d 696 (E.D. Va. 2008).

This Article will not attempt to resolve all the difficult cases, as they may only rarely arise in practice. In my view, however, *Jefferson*'s holding that taking the photographs constituted a seizure seems plausible because the agents testified that they devised the scheme to photograph the documents as a substitute for removing them.[67] That is, the agents photographed the documents to analyze them later rather than merely to remember what they observed in the course of the search. Although the line between copying to aid memory and copying to freeze the scene can be a hazy one, the purpose of the copying may provide a useful way to distinguish the two in close cases such as *Jefferson*.

C. *Alternative Ways of Distinguishing* Hicks *and* Aseltine

The distinction between copying-as-aid-to-memory and copying-as-freezing proves superior to other ways of reconciling constitutional limits on digital copying with precedents like *Hicks* and *Aseltine*. This Section will address two competing approaches: one proposed by Paul Ohm,[68] and another offered by Susan Brenner and Barbara Frederiksen.[69]

Paul Ohm contends that the Fourth Amendment should be read as implying a "previously unidentified Fourth Amendment interest: the right to delete."[70] In Ohm's view, the right to delete is the right to control what happens to your property, including the copies of it, which implies a right to destroy your property so the police cannot have it.[71] *Hicks* and *Aseltine* are distinguishable because the right to delete evaporates when items are in plain view.[72] Because the officers in *Hicks* and *Aseltine* had each observed first and

67. *Id*. at 700. The agents testified that they photographed the documents as a way to obtain copies of all of the documents while formally complying with the direction of attorneys working on the case to only remove the specific documents listed in the warrant. *Id*. Although the *Jefferson* court's holding that photographing the documents "seized" the information is plausible, the court's *dicta* that writing down notes of what they observed would also constitute a seizure seems plainly incorrect. *See* Illinois v. Andreas, 463 U.S. 765, 771-72 (1983) ("[O]nce police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost.").

68. Paul Ohm, *The Fourth Amendment Right To Delete*, 119 HARV. L. REV. F. 10 (2005), http://www.harvardlawreview.org/forum/issues/119/dec05/ohm.pdf.

69. Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2002).

70. Ohm, *supra* note 68, at 11.

71. *Id*. at 13-15.

72. *Id*. at 16.

copied later, the right to delete had already been lost and the subsequent copying did not seize anything.[73]

My approach replicates Ohm's results without his legal fiction. It situates the right to control property directly within the traditional seizure power rather than through a new right to delete. This has two major benefits. First, it is much simpler. Most obviously, it avoids the need to identify exactly what the new right entails. For example, if you have email stored on a server and you decide you want to delete it, does the right to delete provide you with a right to order the ISP to delete it, or is the right only to stop the government from making a copy of your files? Ohm's approach raises such questions; mine does not. Second, my approach offers an explanation for Ohm's conclusion that the right to delete evaporates when items are in plain view. Ohm states that it does, but he offers no reason why.[74] My approach explains why: copying an item already in plain view merely records an observation and does not add to the government's power to collect evidence, while copying an item that has not been in plain view freezes the scene and adds to the information in the government's control. Exposure to plain view causes the observation. My approach therefore provides an explanation for Ohm's intuitive judgment. It achieves the result Ohm seeks without introducing the legal fiction of a right to delete.

Susan Brenner and Barbara Frederiksen agree that copying data seizes it,[75] and they attempt to distinguish *Hicks* on the ground that Hicks did not have a lawful property interest in the serial numbers the officer observed:

> The officer did not record information that belonged to Hicks. Serial numbers are not property in the sense that the number [sic] belong to one person, but are more analogous to license plates or other public records. Serial numbers are assigned by the manufacturer of a product and are used to track and identify that product. Hicks had no interest in these serial numbers because the stereo equipment was stolen from its rightful owners. Hicks had no lawful possessory interest in the equipment or in the serial numbers on the equipment.[76]

73. *See id.*

74. *See id.*

75. Brenner & Frederiksen, *supra* note 69, at 109 ("When copying files, officers physically remove files from the owner's possession. Therefore, it seems the act of copying should be a seizure. The officers are taking the owner's property—the information contained in the files.").

76. *Id.* at 111.

This theory is unpersuasive because the Fourth Amendment seizure power regulates interference with possessory interests, not property interests. A person has a possessory interest in property if he has knowledge of and control over it.[77] This does not imply lawful control. Indeed, crimes of possession such as narcotics offenses necessarily involve unlawful possession.[78] The very definition of contraband is property that is unlawful to possess.[79] As a result, a person who possesses stolen property, cocaine, or child pornography has no lawful interest in it.[80] The Fourth Amendment, however, applies to the taking away of contraband just as it does to the taking away of a person's property: under *Warden v. Hayden*,[81] the rules are the same. It is therefore difficult to explain the absence of a Fourth Amendment violation from copying the numbers in *Hicks* by the absence of a lawful interest in the equipment or the serial numbers.[82]

IV. THE LIMITATION OF INTERRUPTING THE COURSE OF POSSESSION

The final problem to address is how the definition of data seizures deals with routine computer usage. Computers work by making copies. Routine computer usage requires the frequent, if not constant, generation of new copies of data. If every copying of every file constitutes a seizure, then arguably every use of a computer by the government constitutes a seizure.[83] If a government employee uses the Internet, the network makes copies; if a private citizen sends

77. *See, e.g.*, United States v. Katz, 582 F.3d 749, 752 (7th Cir. 2009) (noting that "[c]onstructive possession may be established by demonstrating that the defendant knowingly had the power and intention to exercise dominion and control over the object").

78. *See, e.g.*, 21 U.S.C. § 844 (2006).

79. *See* BLACK'S LAW DICTIONARY 365 (9th ed. 2009) (defining contraband as goods over which the possession or distribution is illegal).

80. *See, e.g.*, 18 U.S.C. § 2252 (2006) (child pornography); 21 U.S.C. § 844 (narcotics).

81. 387 U.S. 294 (1967) (abolishing the "mere evidence" rule that had forbidden the government from obtaining a search warrant for evidence).

82. Brenner's and Frederiksen's effort to distinguish *Hicks* is also difficult to square with the Court's conclusion (in the paragraph immediately following its holding) that lifting up the turntable constituted a Fourth Amendment search even though it did not uncover anything of "great personal value" to Hicks. Arizona v. Hicks, 480 U.S. 321, 325 (1987). If lifting the turntable was a search even though the information exposed had no personal value to Hicks, it seems odd to rest the explanation that copying the numbers was not a seizure on that fact. If the nature of the information mattered, exposing the information to the police presumably would not have been a Fourth Amendment search.

83. Kerr, *supra* note 8, at 562.

an email that passes through a government server, the server makes a copy. Are all of these routine steps Fourth Amendment seizures? And if so, isn't it unworkable to say that government copying constitutes a Fourth Amendment seizure?

This Part explains that copying data in the ordinary course of use will not constitute a seizure. A seizure of moving or movable property occurs only when government action alters the path or timing of its intended possession or transmission. Copying data as part of its usual course of transmission or storage does not seize anything, because its intended path or timing has not been interrupted. As a result, treating copying as a seizure does not require the conclusion that routine computer use implicates constant Fourth Amendment seizures. Government copying of computer data seizes that data only when it copies the data outside the expected course of its transmission or possession.

A. Seizures and the Stream of Transmission

If generating an electronic copy constitutes a seizure, then it becomes possible to argue that all computer use by the government becomes a constant string of seizures.[84] Although I once thought so,[85] I now realize that these concerns are unwarranted. The reason is that the Fourth Amendment seizure authority applies differently to property in transit than to other kinds of property. The test for whether property in transit has been seized is not whether it is at rest or standing still, but whether government action has altered its path.[86] That is, whether the government seizes property that is moving is measured not by whether the government physically takes the item away, but rather by whether the government action changes the predetermined path of the item by some intentional action.

This underappreciated aspect of the Fourth Amendment seizure power explains why electronic copying of data in the ordinary course of transmission should not constitute a seizure at all. Routine copying of data in the course of surfing the Internet and facilitating data transfers does not seize anything even though it copies data: because the copying does not alter the path of the data or occur outside the intended scope of transmission, the copying is not a seizure. As a result, the Fourth Amendment seizure doctrine is implicated only when

84. Indeed, I have argued this myself. *See id.*

85. *Id.* at 560-62.

86. *See* Brendlin v. California, 127 S. Ct. 2400, 2407 (2007) (noting that a traffic stop is a seizure of a car and its passengers, because it "necessarily curtails the travel a passenger has chosen just as much as it halts the driver, diverting both from the stream of traffic to the side of the road").

the government copies a person's private data outside the intended scope of transmission or use.

B. Precedents from Postal Letters and Packages

Precedents from postal letters and packages demonstrate how these principles apply in a physical setting. If a person sends a package through the postal mail, the postal service does not need a warrant to accept it. Giving the package to the government does not initiate a "seizure." To be sure, the package comes into the government's possession. In a colloquial sense, the government has taken control of it. But by accepting the package, the government is merely acting as the sender's agent: the government controls the package because it is part of the ordinary course of the business of delivering the package at the sender's request. At this stage, no seizure has occurred.[87] This remains true even as the package is shipped on to its destination, stopping and resuming its journey along the way as it passes through the Postal Service's network. No seizure has yet occurred, and the Fourth Amendment is not implicated.

Now assume that a government agent comes to believe that the package contains drugs, and he wants to grab the package and open it. The package becomes "seized" at the moment that its path is appreciably altered by the government action.[88] The moment this act occurs can be difficult to identify, but clearly a key variable is time: if a package is held up that would have moved on if it had been in the ordinary course of transmission, then a "seizure" has occurred. At that point, the courts ordinarily engage in an analysis of whether the seizure was constitutionally reasonable. If the police have good cause to get a warrant and proceed expeditiously to obtain one after seizing the package, the seizure will be deemed reasonable and the warrantless seizure will not violate

87. *See* United States v. England, 971 F.2d 419, 421 (9th Cir. 1992).

88. *See* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.2(b) (3d ed. 2007) (noting that in the case of postal mail and packages, "[d]elaying a movable item in the course of transit will eventually cause a 'meaningful interference' with 'possessory interests,' triggering a seizure," and stating that "[t]he question appears to be whether a temporary detention caused identifiable delay in when the letter or package arrived").

the Fourth Amendment.[89] On the other hand, if the police lack probable cause or act too slowly, the seizure will be unconstitutional.[90]

C. Applying Course-of-Transmission Principles to Computers

These same principles should apply to computer data. Copying that is incidental to transmission should not amount to a seizure of data, much like holding or moving a physical package incident to delivery does not "seize" it. Copying that is appreciably outside the intended and common path of data communication, however, should constitute a seizure of that data, much like it would for physical property. The exact moment that this occurs can be difficult to identify in some cases, but this is the same issue that arises in the context of physical seizures. The same concept can apply in the computer context without the need for substantial revision.

Applying this test may require establishing a factual record of how the data obtained is normally delivered or stored. In the case of a communication in transit, a record could be established showing how that sort of communication would normally be delivered. In the case of a stored file, a record could be established showing how and when the file would normally be accessed or retained. With that record in place, courts could then examine whether the government's act of copying the data altered the intended or natural path of that data in an appreciable way. Where it does so, the copying should be deemed a seizure that implicates the Fourth Amendment.

Although some cases will prove difficult, many important examples should be clear. If the government wiretaps an email account and generates copies of all of the emails incoming and outgoing from the account for law enforcement use, all of the communications are "seized" for Fourth Amendment purposes at the moment the copies are generated. The usual and expected path of transmission of email includes passage through mail servers across the Internet, but it does not include an effectively compulsory "bcc" to the government. Such copying is outside the usual and expected path of transmission. It therefore constitutes a seizure.

Similarly, a government request to an ISP to make a copy of a suspect's remotely stored files and to hold it while the government obtains a warrant

89. *See, e.g.*, United States v. Mayomi, 873 F.2d 1049, 1054 (7th Cir. 1989) (upholding a seizure over a weekend as reasonable when the police worked hard and had good reason for delay).

90. *See, e.g.*, United States v. Dass, 849 F.2d 414, 415 (9th Cir. 1988) (holding that a delay of a week was not reasonable when the police could have worked "more diligently" to determine if the package contained contraband).

would also constitute a seizure.[91] In such a case, the government uses a private actor as its agent, and it so happens that this agent might need to copy the target's files for back-up purposes of its own. The government's action, however, changes the path of the communication of contents that would have occurred in the ordinary course of business. Generating the copy freezes the scene at the government's request, preserving evidence for government use. Generating such a copy should also be a seizure.

Finally, a government request to an ISP not to delete contents of communications that would have been deleted in the ordinary course of business would also be considered a seizure. For example, imagine that an Internet user always deletes his old emails after ninety days. On day eighty-nine, the government asks the ISP to hold the copy of the email and deny access to the user so the user cannot delete it. The ISP agrees. On day ninety, the user tries to access the account and fails. At that stage, the files would be seized. The government conduct has altered the path of the communication by blocking its deletion.

CONCLUSION

This Article has argued for a specific understanding of when copying data constitutes a Fourth Amendment seizure. Copying is a seizure when it interferes with the intended course of possession or transmission of data that has not been observed by government actors. This approach reconciles the cases, avoids the objections that scholars (including me) have made, and creates a set of sensible results that can guide courts and commentators.

More broadly, this Article suggests that the bridge from a physical conception of the Fourth Amendment to a virtual conception of the Fourth Amendment can, at least in some cases, be reasonably straightforward to cross. It is possible to translate the familiar principles of the Fourth Amendment from the physical world and to apply them to computers and computer data in a way that restores the function of the old doctrine in the new environment. The way forward may not be obvious. Indeed, in this instance I started out with the wrong approach. But at least in some cases, the basic principles of the Fourth Amendment can be readily translated from the old to the new.

91. *Cf.* 18 U.S.C. § 2703(f) (2006) (authorizing such requests).