

FOURTH AMENDMENT SEIZURES OF COMPUTER DATA

*Orin S. Kerr**

YALE LAW JOURNAL
(forthcoming 2009-10)

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 essay argues that copying data “seizes” it under the Fourth Amendment when copying occurs without human observation and interrupts the stream of its possession or transmission. It offers this position by reaching back to the general purposes of regulating seizures in Fourth Amendment law and then applying that function 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.

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

2009] *Seizures of Computer Data* 1

Table of Contents

Introduction	3
I. The Seizure Puzzle	6
II. Answering the Seizure Puzzle	10
a. The Power to Seize as a Power to Freeze	10
b. Copying as Freezing	12
III. The Limitation of Copying Without Human Observation	15
a. Copying as Freezing Versus Copying As Aid to Memory	15
b. Copying as An Aid to Memory in <i>Hicks</i> and <i>Aseltine</i>	16
c. Alternative Ways of Distinguishing <i>Hicks</i> And <i>Aseltine</i>	18
IV. The Limitation of Interrupting the Course of Possession	23
a. Seizures and the Stream of Transmission	24
b. Precedents From Postal Letters and Packages	25
c. Applying Stream-of-Transmission Principles to Computers	26
Conclusion	27

Introduction

Imagine the police take away a suspect's computer, copy all of its contents, and then give the computer back before the owner realizes it is missing. The government retains the files indefinitely until the police have probable cause to get a warrant to search the computer. Does copying the files without looking at them violate the Fourth Amendment?

Next, imagine the government seizes a person's computer at the border. Agents copy all the files on the computer at the border under the border search exception to the Fourth Amendment.¹ The agents then decide to hold the suspect's computer files indefinitely until they need the files on the computer at a later time. Does the Fourth Amendment allow it?

Finally, imagine officers believe a particular person is using the Internet to engage in criminal activity. Agents install a surveillance device at the target's ISP, and they generate copies of all of the target's e-mail and websurfing. The data is collected and stored in a file, but no human being actually looks at the file. Instead, the agents store the file and wait for a future time when they will have probable cause to look through it for evidence. Again, does the Fourth Amendment allow it?

The answer to all three scenarios depends on whether copying computer files without looking at them constitutes a Fourth Amendment "seizure."² 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 a file does not seize it, then the government can make and retain the copy without restriction. The Fourth Amendment will

¹ See, e.g., *United States v. Arnold*, 522 F.3d 1003 (9th Cir. 2008) (applying the Fourth Amendment to the border search of a laptop computer).

² 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.

limit looking through the copy: Looking through the copy is a Fourth Amendment search.³ But what if the Government wants to make a copy and hold it? Does that “seize” anything?

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: While the police traditionally search for information and then seize it, computer technologies require the government to generate the copy first and then search it later.⁴ Nearly every case begins with copying data that will later be searched.

As a doctrinal matter, whether copying computer data amounts to a seizure remains unclear. The Supreme Court has said that a seizure of property occurs “when there is some meaningful interference with an individual’s possessory interest in that property.”⁵ This could be interpreted in two different ways. Perhaps copying doesn’t interfere with a possessory interest because that interest is limited to hardware and the copy of the data that 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 provide the answer. Which of these approaches is right?

In addition, precedents from earlier technologies such as physical copying, photographic copying, and wiretapping are decidedly mixed.⁶ 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 in fact seize it.⁷ As a result, whether copying amounts to a seizure remains an unsolved puzzle.

³ See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L.Rev. 531, 548-54 (2005).

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

⁵ See Part II, *infra*.

⁶ Compare *Arizona v. Hicks*, 480 U.S. 321 (1987) (copying is not a seizure) with *Berger v. New York*, 388 U.S. 41 (1967) (suggesting that copying is a seizure).

This essay attempts to solve the puzzle by offering a new test to determine 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 its 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 that function to the new environment of computers. The test it offers 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 environment.

The approach offered here also provides a new way to make sense of the mixed caselaw on whether copying constitutes a seizure. It explains that copying is neither *never* nor *always* a seizure: Whether a copying amounts to a seizure depends both on whether it is pre-observation or post-observation and also on whether it interrupts the intended transmission or use of the data. This approach explains and reconciles the caselaw from prior technologies. In so doing, it suggests a sensible definition to apply when the government generates copies of computer data that sensibly translates the traditional physical concept of Fourth Amendment seizures to a digital environment.

Finally, this essay offers a correction of some of my prior work. In a 2005 article published in the *Harvard Law Review*,⁸ I concluded somewhat uncomfortably that copying should never be considered a Fourth Amendment seizure.⁹ At the time, I was influenced by the cases holding that photographing and writing down numbers were not a seizure, as well as by what seemed to be considerable practical problems with calling all copying a seizure.¹⁰ I now see I was wrong. A middle ground is not only possible but also most consistent with both the cases and common

⁸ Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L.Rev. 531, 548-54 (2005).

⁹ See *id.* at 557-62.

¹⁰ *Id.* at 560 (calling the result “troublesome,” but arguing for ways to limit its impact and contending that the alternatives raised considerable practical difficulties.)

sense. This essay identifies the new middle ground and explains why I now disavow my earlier approach.

The essay 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

The government often obtains copies of computer files without first looking through them. The digital copies are stored on a government computer awaiting viewing and analysis. Whether that copying and storage amounts to a Fourth Amendment seizure remains unclear. This section explains why the answer is unclear, setting up the puzzle that the rest of the article will attempt to answer.

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.¹¹ When the government invades a private space, violating a reasonable expectation of privacy, that invasion becomes a search.¹² 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.¹³ As the Supreme Court has explained, a seizure of property occurs

¹¹ See U.S. Const. Amend. IV.

¹² 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)).

¹³ *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984).

when the government "substantially interferes" with a person's "possessory interest" in property.¹⁴

The definition of a seizure is easy to apply to physical property but difficult to apply to computer data. Physical property is possessed when a person has knowledge and control over it. 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?

B) Precedents on Copying as a Seizure

Existing precedents are mixed. Some cases suggest that copying does not seize anything, such that the possessory interest refers only to control of the original. In *Arizona v. Hicks*,¹⁶ 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 it down before checking to see if the number matched that of equipment reported stolen. The

¹⁴ *Id.*

¹⁵ *Cf.* *Brendlin v. California*, 551 U.S. 249, 255 (2007) ("[D]uring a traffic stop an officer seizes everyone in the vehicle, not just the driver.")

¹⁶ 480 U.S. 321 (1987).

Supreme Court held that copying the serial number did not seize anything: "the mere recording of the serial numbers did not constitute a seizure. . . . [I]t did not 'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure."¹⁷

Lower courts have followed *Hicks* in cases involving photographs and photocopies. In *Bills v. Aseltine*,¹⁸ the Sixth Circuit held that the police didn't "seize" anything when they took photographs of the scene when executing a warrant. According to the court, "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 One district court followed this approach in a computer case, as well. In *United States v. Gorshkov*,²⁰ FBI agents downloaded a file stored on a remote server and held the copy of the file in the FBI's possession until a warrant was obtained. The District Judge ruled that the copying of the file did not seize it because it did not alter or make it inaccessible.²¹

Other precedents point the other way, however. In *Berger v. New York*,²² the Supreme Court struck down a wiretapping statute on the grounds that the statute did not reflect sufficient constitutional protection. The majority opinion in *Berger* repeatedly referred to the act of wiretapping as a "search and seizure." Although the Court did not explain exactly what part of wiretapping constituted a seizure, Justice Harlan's dissenting opinion suggests, albeit only obliquely, that the majority likely saw some act of recording a conversation as a seizure.²³ *Katz v.*

¹⁷ *Id.* at 324.

¹⁸ 958 F.2d 697 (6th Cir. 1992).

¹⁹ *Id.* at 707.

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

²¹ *Id.* at *3.

²² 388 U.S. 41 (1967).

²³ *Id.* at 98 (Harlan, J., dissenting) ("There is no need for present purposes to explore at length the question's subtleties; it suffices to indicate that, in my view, conversations are not "seized" either by eavesdropping alone, or by their recording so that they may later be heard at the eavesdropper's convenience. Just as some exercise of dominion, beyond mere perception, is necessary for the seizure of tangibles so some use of the conversation beyond the initial listening process is required for the seizure of the spoken word.").

*United States*²⁴ is similar. In *Katz*, agents had placed a microphone next to a public telephone and recorded one end of the 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" – suggesting that some sort of seizure was afoot, as well.²⁵

The caselaw on Rule 41 of the Federal Rules of Criminal Procedure also points towards copying information as a seizure. Rule 41 governs search warrants, and it authorizes federal courts to issue warrants to "search for and seize" evidence.²⁶ In *United States v. New York Telephone*,²⁷ the Supreme Court held that this power allowed the government to install a surveillance device that copied the 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."²⁸ Although not a model of clarity, *New York Telephone* together with *Berger* and *Katz* seem to suggest that at least in some cases the recording of information "seizes" it.

²⁴ 389 U.S. 347 (1967).

²⁵ See *Katz*, *supra* note 24, at 353:

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.

Id. (emphasis added).

²⁶ See Fed. R. Crim. Pro. 41.

²⁷ 434 U.S. 159 (1977).

²⁸ *Id.* at 169.

The precedents appear divided. Some cases suggest that copying data does not seize it, and others suggest it does. The correct answer remains unclear.

II. Answering the Seizure Puzzle

The uncertainty of how the Fourth Amendment's concept of "seizures" applies to computer data cannot be resolved by doctrine alone. Instead, it should be resolved first by understanding how copying intangible data bifurcates the interests the Fourth Amendment traditionally protects, and then by choosing the interpretation that most closely matches the traditional function of the Fourth Amendment seizure power. This section uses that approach to explain why electronic copying by the government should trigger a Fourth Amendment seizure at least in some circumstances.

The core reason is that the Fourth Amendment power to seize is the power to freeze – the power to hold the scene and control evidence, adding to the amount of evidence under the government's control. 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. It 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 a seizure.

A. The Power to Seize as a 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 so the police can maintain custody of it, maintain 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 therefore 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 ordinarily will violate a suspect’s reasonable expectation of privacy, and will therefore be a search that requires a warrant or some exception to the warrant requirement such as consent or

exigent circumstances.²⁹ 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.³⁰ Taking away the drugs "seizes" the drugs.³¹ The two distinct powers end up dividing along the lines of the two categories 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. At that stage, the person can no longer interfere with the item seized: It is in police custody, not the individual's. Control shifts from the individual to the police. 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.³²

The same principle governs seizures of individuals. If the police execute a *Terry* stop,³³ forcing an individual to stay where he is temporarily while police investigate, he is "seized" as soon as the police indicate that he is not free to go.³⁴ 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

²⁹ *Katz v. United States*, 389 U.S. 347 (1967).

³⁰ *Brendlin v. California*, 551 U.S. 249 (2007).

³¹ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

³² *Illinois v. McArthur*, 531 U.S. 326 (2001) (seizure of home when police block owner from re-entering).

³³ *Terry v. Ohio*, 392 U.S. 1 (1968).

³⁴ *Id.* at 16-20.

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 authority to computer data is to hold that electronic copying ordinarily "seizes" it. 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.³⁵ But obtaining the copy 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 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.

To be sure, 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 the 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 non-rivalrous, 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.³⁶ As a result, computer data severs the connection between the information and the storage device. The question is, should the

³⁵ See Kerr, *supra* note 4, at 560-61.

³⁶ See Gorschkov, *supra* note 22; Kerr, *supra* note 4, at 560-62.

law focus on when a person loses exclusive rights to the device, or when a person loses exclusive rights to the data?

In my view, 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.³⁷ 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 can crash. Thumb drives can get lost. Networks can 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 of 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 and often do generate a copy of data from seized devices and provide the copy to the suspect.³⁸ Given this reality, it makes little sense to draw a distinction between copying data and removing physical storage devices. 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 a copy on a CD 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

³⁷ Accord Paul Ohm, 2008 *The Olmsteadian Seizure Clause: The Fourth Amendment And The Seizure Of Intangible Property*, 2008 Stan. Tech. L. Rev. 2.

³⁸ See generally Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 Miss L.J. 85, 124-25 (2005).

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. Government control of data provides the link that empowers the prosecution to charge a person with a crime that will take away their freedom. As a result, the difference between merely copying a person's private data and actually taking away their physical devices is a modest one. To be sure, a person's access to their 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. Access to hardware is a convenience, not a human right. 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 cause such as a warrant or an exception to the warrant requirement. In the next two sections, 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.

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 does 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 concluded that these precedents rendered it difficult to conclude that electronic copying was a seizure.³⁹ I could not see a persuasive way to distinguish those cases, and overruling them seemed unlikely. I have now concluded that my earlier approach was wrong. I now see that electronic copying of a computer files is different in a critical way from writing down information or taking a photograph. The difference is that electronic copying adds to the information in the government's possession by copying that which the government has not observed. The copy takes something that has not been observed, processes it through a machine, and ends up with a copy. In contrast, writing down information or taking a photograph merely saves what the government has observed as an aid to its memory. The copy merely *memorializes the human observation* in a fixed form. It neither interferes with the item copied or adds to the amount of information exposed to a human being.

This distinction explains why cases such as *Arizona v. Hicks*⁴⁰ and *Bills v. Aseltine*⁴¹ 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 freezing the scene and adding to information in the government's possession. Because electronic copying normally involves copying without observation, electronic copying amounts to a seizure even

³⁹ See Kerr, *supra* note 4, at 562.

⁴⁰ 480 U.S. 321 (1987).

⁴¹ 958 F.2d 697 (6th Cir. 1992).

though taking a photograph or writing down information does not “seize” anything for Fourth Amendment purposes.

A. Copying as Freezing Versus Copying As Aid to Memory

Although “making copies” may seem like a generic act,⁴² it is actually a result that can be produced in two relatively distinct ways. 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.⁴³ 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 memorialize what he knows. He’ll take steps to remember what he has seen in order to aid his memory and generate reliable evidence of what he has observed. That is, he will make a copy of what he has already observed.

Police officers often generate copies to memorialize what they have observed. After investigating a crime scene, the officer may write up a report. When called to the scene of a car accident, he might take pictures to reconstruct the accident more accurately. To create 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 serves as a reminder to the officer as to what he saw, helping his memory, and also serves as

⁴² This is particularly true for fans of Rob Schneider. See, e.g., <http://snltranscripts.jt.org/91/91grichmeister.phtml>. An excerpt:

Richmeister: Ran-dyyy! The Rand-man! Randatollah!
Randy: Hi, Richard. Just making some copies.
Richmeister: Alright! The Rand Old Opry, makin' copies!

Id.

⁴³ See notes [] to [], *infra*.

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 memorialize what an officer observes is different from the power to freeze the scene. The differences can appear subtle, to be sure, and the end result is the same: The government gets a copy. But the two powers are different. The power to memorialize what has been observed uses tools to help the government from forgetting what it has already learned. In contrast, the power to freeze the scene adds to what the government controls. It takes some evidence that was beyond the government control and brings 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.

B. Copying as An Aid to Memory in Hicks and Aseltine.

The distinction between copying-to-aid--memory and copying-to-add-to-government-control explains why cases such as *Arizona v. Hicks*⁴⁴ and *Bills v. Aseltine*⁴⁵ do not compel the result that digital copying does not seize anything.

Recall that in *Hicks*, the officer picked up the turntable, observed the serial numbers on the bottom, and then wrote down the serial numbers he observed.⁴⁶ The writing down of the numbers itself did freeze the scene, adding to that which was under the government's control. Rather, it simply memorialized what already was in the officer's own mind. When the officer wrote down the numbers, he recalled what he had observed and transferred that memory from his mind to the piece of paper.

⁴⁴ 480 U.S. 321 (1987).

⁴⁵ 958 F.2d 697 (6th Cir. 1992).

⁴⁶ *Hicks*, 480 U.S. at 324.

Writing down the contents of the officer's mind did not freeze the scene or add to what the government controlled. It simply acted as an aid to the officer's memory of what he had already observed.

The same is true of *Bills v. Aseltine*.⁴⁷ Recall that in *Aseltine*, an officer took pictures of the plaintiff's home while executing a warrant there. The plaintiff sued, arguing that taking photographs of 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 the numbers or trying to make an accurate drawing of what the officer observed. The camera tool 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 of what had seen.

In my 2005 article in the *Harvard Law Review*,⁴⁸ 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*."⁴⁹ However, I now see that I overlooked the distinction between pre-observation copying-as-freezing and post-observation copying-as-aid-to-memory. The key dynamic 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 to 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 therefore distinguishable from cases involving electronic copies because they involve a different kind

⁴⁷ 958 F.2d 697 (6th Cir. 1992).

⁴⁸ See Kerr, *supra* note 4.

⁴⁹ *Id.* at 562.

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. It merits different treatment under the Fourth Amendment because it involves a different kind of copying.

C. Alternative Ways of Distinguishing Hicks And Aseltine

Distinguishing *Hicks* and *Aseltine* from digital copying based on the distinction between copying-as-memory and copying-as-adding proves significantly easier and more persuasive than other approaches various scholars have recommended. This section will briefly address the two most important competing proposals: One by Professor Susan Brenner and Barbara A. Frederiksen and another by Professor Paul Ohm.

In an article a few years ago,⁵⁰ Brenner and Frederiksen argued that *Hicks* is distinguishable because *Hicks* did not have a lawful property interests 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 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

⁵⁰ Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L. Rev. 39 (2002).

possessory interest in the equipment or in the serial numbers on the equipment.⁵¹

The difficulty with this approach is that a possessory interest is different from a property interest. A person has a possessory interest in property if he has knowledge of and control over it.⁵² This doesn't imply that the control is lawful. Indeed, crimes of possession such as narcotics offenses necessarily involve unlawful possession.⁵³ The very definition of contraband is property that is unlawful to possess.⁵⁴ As a result, a person who possesses stolen property has no lawful interest in it, as does someone who possesses cocaine or child pornography.⁵⁵ The Fourth Amendment applies to the taking away of contraband just as it does to the taking away of a person's property: Under *Warden v. Hayden*,⁵⁶ the rules are the same. For this reason, it is difficult to conclude that the officer did not violate Hicks' Fourth Amendment rights because Hicks did not have a lawful interest in the equipment or the serial numbers.⁵⁷

The approach I offer is also superior to Professor Paul Ohm's proposal offered in his essay, *The Fourth Amendment Right to Delete*.⁵⁸ Ohm argues that *Hicks* and *Aseltine* are distinguishable because the Fourth should be read as implying a "previously unidentified Fourth Amendment interest: the right to delete."⁵⁹ In Ohm's view, the right to delete is the right to control

⁵¹ *Id.* at 111.

⁵² *Maryland v. Pringle*, 540 U.S. 366 (2003) (possession of narcotics under Maryland law).

⁵³ *See, e.g.*, 21 U.S.C. § 844.

⁵⁴ *See* Black's Law Dictionary (defining contraband as goods over which the possession or distribution is illegal).

⁵⁵ *See, e.g.*, 21 U.S.C. § 844 (narcotics); 18 U.S.C. § 2522 (child pornography).

⁵⁶ 387 U.S. 294 (1967).

⁵⁷ Brenner & Fredericksen's effort to distinguish *Hicks* is also difficult to square with the Court's conclusion in the very next paragraph that lifting up the turntable constituted a Fourth Amendment search even though it did not uncover anything of "great personal value" to Hicks. *Hicks*, 480 U.S. at 324. 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.

⁵⁸ 119 Harv. L. Rev. F. 10 (2006).

⁵⁹ *Id.* at 11.

what happens to your property, including the copies of it, which implies a right to destroy your property so the police cannot have it.⁶⁰ He then argues that *Hicks* and *Aseltine* are distinguishable because the right to delete evaporates when items are in plain view.⁶¹ Because the officers in *Hicks* and *Aseltine* had observed what they copied first, the right to delete the number had been lost and the subsequent copying was no longer a seizure.⁶²

The difficulty with Ohm's approach is that it creates a legal fiction. It envisions a new "right to delete" solely to enable the desired results. As is true with most legal fictions, however, the right ends up raising more questions than it answers. For example, Ohm does not say exactly what this right entails. Imagine you have e-mail stored on a server, and you decide you want to delete it. Does the Fourth Amendment provide you with a right to order the ISP to delete it? Or is the right only to stop a copy of your files being made by the government? And even if we accept that the Fourth Amendment includes a "right to delete," why does that right disappear when the government views property in plain view? Ohm states it does, but he does not explain why.⁶³ In light of these difficulties, distinguishing *Hicks* and *Aseltine* through recognition of a "right to delete" seems to raise more questions than it answers.

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

⁶⁰ *Id.* at 12-15.

⁶¹ *Id.* at 16.

⁶² See *id.*

⁶³ *Id.* at 16. Granted, Ohm and I end up largely agreeing as to the result. Ohm's assertion that the "right to delete" disappears when the government views property ends up tracking my own distinction between copying-as-freezing and copying-as-aid-to-memory.

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.⁶⁴ If a government employee uses the Internet, he is making copies; if a private citizen sends an e-mail that passes through a government 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 causes a Fourth Amendment seizure?

This section answers these objections and explains why they have no merit. Typical computer usage will not cause a seizure because a seizure of moving or movable property occurs only when government action alters the path or timing of its intended possession or transmission. When computer data has been sent across the Internet, or is otherwise being used in the proper intended fashion, no seizure occurs because its intended path or timing has not been interrupted. As a result, the concern that treating copying as a seizure will force general computer use to implicate constant Fourth Amendment seizing is unwarranted. Copying in the ordinary course of use will not constitute a seizure.

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.⁶⁵ When data passes through a government network, the network makes copies; when a government employee surfs the Internet network makes copies. If copying constitutes a seizure, then aren't all of these everyday occurrences seizures – and therefore Fourth Amendment events that require a warrant or some sort of exception to the warrant requirement? If so, then that may provide a good reason not to accept that copying data seizes it, as the definition may be elegant in theory but create odd results in practice.

⁶⁴ Kerr, *supra* note 4, at 561-62.

⁶⁵ Indeed, I have argued this myself. *See id.*

Although I once thought so,⁶⁶ I now realize that these concerns are unwarranted. The reason is that the Fourth Amendment seizure authority applies differently to property *in transit* than other kinds of property. The effective 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*.⁶⁷ 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 the transfer of data does not seize anything even though it copies data: Because the copying does not alter the path of the data or occur outside the intent scope of transmission, the copying isn't a seizure. As a result, the Fourth Amendment seizure doctrine becomes implicated only when government action 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 "seize" anything.⁶⁸ 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

⁶⁶ *Id.*

⁶⁷ See *Brendlin v. California*, 551 U.S. 249 (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.") (emphasis added).

government is merely acting as the sender's agent: The government controls the package because it's part of the ordinary course of the business of delivering the package at the sender's request. At this stage, no seizure has occurred.⁶⁹ This remains true even as the package was shipped on to its destination, stopping and starting its journey along the way as it passes through the Postal Network's service. No seizure has yet occurred, and the Fourth Amendment is not implicated.

Now let's 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.⁷⁰ The act moment this 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 the altering of the package's path triggers a "seizure." At that point, the courts then 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 it, the seizure will be deemed reasonable and the warrantless seizure will not violate the Fourth Amendment.⁷¹ On the other hand, if the police have no cause or act too slowly, the seizure will be unconstitutional.⁷²

C. Applying Course-of-Transmission Principles to Computers

These same principles should apply in the setting of 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. However, copying that is outside the intended and common path of

⁶⁹ *United States v. England*, 971 F.2d 419 (9th Cir. 1992).

⁷⁰ *United States v. van Leeuwen*, 397 U.S. 249 (1970).

⁷¹ *See, e.g., United States v. Mayomi*, 873 F.2d 1049, 1054 (7th Cir. 1989) (upholding seizure over a weekend as reasonable when the police worked hard and had good reason for delay).

⁷² *See, e.g., United States v. Dass*, 849 F.2d 414 (9th Cir. 1988) (holding that delay of a week was not reasonable when the police could have used other techniques to determine if package contained contraband).

communication or data in an appreciable way should trigger a seizure of that data, much like it would for physical property. The exact moment that 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 applies 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 and common path of that data in an appreciable way. Where it did so, the copying must be deemed a seizure that triggers the Fourth Amendment.

Although some cases will prove difficult, many important examples should be clear. For example, if the government wiretaps an e-mail account and generates copies of all of the e-mails 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 have been generated. The usual and expected path of transmission of e-mail 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 Internet Service Provider to run off a copy of a suspect's remotely stored files and to hold them pending the obtaining of warrant should also constitute a seizure.⁷³ In such a case, the government has used 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.

⁷³ Cf. 18 U.S.C. § 2703(f) (authorizing such requests).

However, the government's action has changed the path of the communication of contents that would have occurred in the ordinary course of business. Generating the copy froze the scene at the government's request, generating a copy 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 should also be considered a seizure. For example, imagine that an Internet user always deletes his old e-mails after 90 days. On day 89, the government asks the ISP to hold the copy of the e-mail and deny access to the user so the user cannot delete it. The ISP agrees. On day 90, 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, so a seizure of the files will have occurred.

Conclusion

This essay has argued for a new understanding of when copying data triggers Fourth Amendment "seizures." It has argued for a middle ground: Copying is a seizure when it interferes with the intended course of possession or transmission and collects data that is Fourth Amendment protected and has not been observed by government actors. This approach reconciles the cases, avoids the objections that scholars (including myself) have made, and creates a set of sensible results that can guide courts and commentators alike.

More broadly, this essay 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

2009]

Seizures of Computer Data

27

environment. The way forward may not be obvious. Indeed, in this instance I started out with the wrong approach that I am disavowing in this essay. But at least in some cases, the basic principles of the Fourth Amendment can in fact be translated readily from the old to the new.