

Symposium: Beyond a Physical Conception of the Fourth Amendment:  
Search and Seizure in the Digital Age

January 26, 2007

---

Associate Professor Paul Ohm  
University of Colorado School of Law

*Title: The Olmsteadian Seizure Clause*

Extended Abstract

*This is a very incomplete sketch of my ultimate argument. I hope it provides discussants enough to understand my proposal, but there is much more to come.*

INTRODUCTION

The Fourth Amendment's Seizure clause is mired in the Eighteenth century. Its counterpart, the Search clause, has evolved through a steady progression of Supreme Court cases interpreting it from *Katz* to *Berger* to *Kyllo*, no longer to be confined to the property-based notions of privacy embodied in *Olmstead v. United States*. Instead the modern Search clause is sensitive to modern privacy concerns; its Constitutional protections apply to any situation that satisfies the reasonable expectation of privacy test. While imperfect, the evolved Search clause has kept the protections of the Fourth Amendment relevant in an age of digital evidence, ubiquitous communication networks, and increasingly sophisticated and invasive surveillance capabilities.

In contrast, the Seizure clause is in an *Olmsteadian* holding pattern, consistently interpreted to protect only physical property rights and to regulate only the meaningful interference of possessory interests in tangible things. In particular, Courts interpreting the clause rarely consider what "interference" means when we are talking about intangible property such as digital evidence and voice and data communications.

In this essay, Professor Ohm argues for a Twenty-First century definition of Constitutionally-proscribed property deprivation. He argues that a Constitutionally significant "Seizure" occurs whenever the State obtains a copy of non-public data. By copying the data, the State deprives the owner of the ability to delete or alter the State-possessed copy of the data

The Supreme Court has implicitly adopted this definition, in *Berger*, *Katz*, and *Hoffa*, by holding in no uncertain terms that voice conversations are both searched and seized when recorded by the police. Professor Ohm traces lower-court cases that have

been decided since these three Supreme Court precedents and points out that many lower courts have ignored these holdings.

[Embracing a modern interpretation of the Seizure clause is consistent with the Framers' intent, because copying affects the property rights of owners of intangible property in many of the same ways that physical dispossession deprived property owners at the time the Fourth Amendment was adopted.]

Reconceiving the seizure clause in light of modern concerns about intangible property rights helps solve many vexing Fourth Amendment puzzles that arise if the sole test is the reasonable expectation of privacy. For example, does a bit-by-bit copy of a computer's hard drive implicate the Fourth Amendment, if the human operator does not "view" the contents as they are copied? Could the government lawfully capture all of the communications traversing a network without a warrant so long as they did not look at the contents without a subsequent warrant? Do government-run network intrusion detection systems implicate the Fourth Amendment?

Finally, an expanded approach to interpreting the Fourth Amendment is a useful counterpoint to the government's use of new technology to invade privacy and property. *Katz* epitomized this approach, but *Katz* is perhaps an incomplete revolution.

#### *I. Olmstead Redux: Today's Property-Based Seizure Clause*

In 1977, David Edward Thomas sent a package through UPS that never arrived at its destination.<sup>1</sup> It was neither snow nor rain nor heat nor gloom of night that kept his package from its appointed destination; he simply misaddressed it.<sup>2</sup> Unfortunately for him, the package "inadvertently" broke open in a UPS facility while UPS was deciding what to do with it, and UPS employees spied what they thought was child pornography inside and called the FBI.<sup>3</sup> The FBI photocopied the contents and returned the originals to UPS.<sup>4</sup> Thomas argued to the court that the documents had been seized by the FBI when photocopied, but his argument was rejected by the Tenth Circuit Court of Appeals. A photocopy, they held, is not a physical dispossession, so nothing was "seized".<sup>5</sup>

In 2000, the FBI duplicated the files of another person, Vasiliy Gorshkov.<sup>6</sup> Gorshkov's files were virtual: data files he had stored on a computer in Russia. Convinced that Gorshkov was hacking into computers and extorting money from American companies, the FBI lured him to Seattle with the promise of a job, observed him typing in his password to his Russian computer from a bugged system, and logged

---

<sup>1</sup> *United States v. Thomas*, 613 F.2d 787, 789 (10th Cir. 1980).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *Id.* at 793.

<sup>5</sup> *Id.* (citing *United States v. Lisk*, 522 F.2d 228, 230 (7th Cir. 1975) and *United States v. Haden*, 397 F.2d 460, 465 (7th Cir. 1968)).

<sup>6</sup> *See United States v. Gorshkov*, 2001 WL 1024026 at \*1 (W.D. Wash. 2001).

into that Russian computer and downloaded all of his files.<sup>7</sup> As in the Thomas case, the district court judge held that nothing had been seized.<sup>8</sup> "The data remained intact and unaltered. . . . The copying of the data had absolutely no impact on his possessory rights."<sup>9</sup>

These two cases harken back to an earlier time, when Courts embraced a physical, property-based vision of the Fourth Amendment. Almost eighty years after *Olmstead v. United States*,<sup>10</sup> and forty years after *Olmstead* was supposedly laid to rest in *Katz v. United States*,<sup>11</sup> the specter of the property-based Fourth Amendment still haunts our Constitutional hallways, perhaps a shadow of its former self, but still among us.

Under the traditional interpretation of the Fourth Amendment, the government *seizes* property only when it "meaningfully interfere[s]" with a "possessory interest."<sup>12</sup> Courts have not articulated precisely what is meant by this phrase, but cases like these suggest a physical-property-centric model of dispossession. The phrase is limited to the deprivation of rivalrous, discrete, tangible things that allow a binary state of possession: at any given time, they are either completely "in possession" or else "not in possession." It follows that intangible, nonrivalrous property that lack this possessional binary-ness cannot be seized unless and until the government deprives the owner of every last copy of the property.

The result is positively *Olmsteadian*. The Fourth Amendment protects tangible items and does not protect intangible information. Granted, under *Katz*, intangible information can be searched, but when no expectation of privacy has been breached, the Fourth Amendment plays no role. Taylor and Gorshkov no doubt felt wronged by what the FBI did to their intangible data, but their perceived harm did not rise to the level of government property invasion protected by the Government.

[This is inconsistent with *Hoffa*, *Katz*, and *Berger*.]

[This diminishes the protections of the Fourth Amendment, given the importance of intangible, intellectual property in today's economy, and the amount of important, private and valuable information people tend to keep "locked away" in intangible forms.]

---

<sup>7</sup> *Id.*

<sup>8</sup> *Id.* at \*3. In the alternative, the Court also held that the computers in Russia owned by a non-resident of the U.S. were unprotected by the Fourth Amendment under *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> 277 U.S. 438 (1928).

<sup>11</sup> 389 U.S. 347 (1967).

<sup>12</sup> *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) (quoting *Maryland v. Macon*, 472 U.S. 463, 469 (1985)). The word "seizure" in the amendment has also been interpreted to regulate the government's seizure of people, for example in investigatory situations. *See, e.g., United States v. Drayton*, 536 U.S. 194 (2002) (finding passenger questioned on a bus not seized). This essay is limited to property not personal seizure.

[This has allowed technology to affect privacy and property in a way inconsistent with what the Framers probably intended.]

## *II. The Gap in Fourth-Amendment Protection: Technologies of Reproduction*

That the *Olmsteadian* seizure clause persists four decades after *Katz* and eight decades after *Olmstead* is not entirely surprising for two reasons. First, at least historically, the government has usually had to deprive a person of physical property (even if momentarily) before it could make a copy of his intangible property. For example, in order to copy the bits from a hard drive, the government had to open the plastic or metal case of the computer containing the hard drive.<sup>13</sup> In a world of atoms-before-bits, it was hard to imagine situations where property could be seized intangibly without first being seized physically. Even so, the result was counter-intuitive; the Fourth Amendment protected that which we really cared about—our information—only because it happened to be encased in a physical box we cared very little about.

Second, even when the government could obtain information through no physical intrusion whatsoever, it usually had to invade a virtual space—and post-*Katz* a reasonable expectation of privacy—to get access to the data. Thus, in order to copy all of the e-mail messages from an inbox, the government first had to find a way to view the contents of the inbox, protected behind passwords, private third parties, and other virtual walls. Copying email without warrant or justification might not have been a seizure, but it was probably a search.

But physical and virtual walls mean less today than they once did, as advances in technology give the government new opportunities to copy data with no physical dispossession and arguably without intruding on expectations of privacy. Consider the following technologies of reproduction.

### *A. Hard Drive Images*

The first step in the analysis of a computer's hard drive is the bit-by-bit image copy. This is not analogous to ordinary copies that ordinary users make on their ordinary computers, but it is instead the thorough, detailed reproduction of every piece of data stored on a hard drive, performed on a specialized computer. An image copy allows the police to preserve for later study hidden pools of data—named by a technical jumble of terms such as slack space, cache, and deleted files—that most ordinary users do not realize exist.

### *B. Packet Sniffers*

Packet sniffers are wiretaps for computer networks. They are computer programs that collect any electronic communications that flow on the network past the computer on

---

<sup>13</sup> Cf. *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) (treating separately under the Fourth Amendment the government-employer's entry into the employee's office and computer to retrieve a hard drive from the monitoring of the employee's Internet traffic).

which the sniffer is running.<sup>14</sup> If the computer is located at a point in the network through which flow the communications of many people—imagine a large network switch operated by a large Internet Service Provider—the sniffer will capture everything: e-mail messages, instant messages, web page requests, and YouTube videos that happen to flow by.

The government's use of packet sniffers in massive data collecting programs has long been a prominent feature of many conspiracy theories,<sup>15</sup> academic arguments,<sup>16</sup> and, most recently, confirmed news stories.<sup>17</sup> Is it a Fourth Amendment seizure for the government to collect this information? Does it matter if a human being—the operator—has had a chance to peruse or keyword search through the information, or does a seizure occur as soon as the information is intercepted?

### *C. Wireless Networks*

[Here I will explain the growth of WiFi, 3G, and Bluetooth networks as well as RFID technology that give the government more opportunities to access data from a distance. Also, I will cite literature showing how this trend will continue to grow and spread.]

### *D. The Fourth Amendment and Technologies of Reproduction: The Modern Metaphysics of Search*

Traditionally, the search clause has been used to measure the Constitutionality of the use by the government of tools like these. Applying the *Katz* test, these government acts do not implicate the Fourth Amendment unless they violate a reasonable expectation of privacy; that is they must invade a person's subjective expectation of privacy, and the expectation must be one that society recognizes as reasonable.<sup>18</sup> Key to how these tools may be analyzed is the nature of the government invasion. At what point does a computer program invade an expectation of privacy: during initial collection of private information; when it makes that private information available to a human operator; or when the operator actually views the information?

The problem with this type of analysis is it invites the government to engage in a form of Constitutional gamesmanship: What if the packet sniffer is configured to seal its information away from police review until it is unlocked after judicial authorization? What if the image of the hard drive is stored on media that is locked inside a cabinet at police headquarters? Under the expectation of privacy test, the government has a non-

---

<sup>14</sup> A fundamental computer networking technology is Ethernet. See IEEE Standard for Information Technology, 802.3-2005 at <http://standards.ieee.org/getieee802/802.3.html> (last visited January 11, 2007). Ethernet allows multiple computers to communicate along a shared communications path, such as a network cable. This is designed to allow for efficient resource allocation and simpler hardware requirements, but it has the side-effect of allowing a computer to access communications that neither originate or are destined for it.

<sup>15</sup> [Echelon.]

<sup>16</sup> [Yale Comment on Net-wide search.]

<sup>17</sup> [Lichtblau on NSA Wiretapping Program, N.Y. TIMES]

<sup>18</sup> See *Katz* 389 U.S. at xxx.

laughable argument that these actions are not yet "invasions" or "intrusions" of any privacy. As long as none of the collected information is reviewed immediately, and especially if review requires an additional, tamper-evident step, the police can claim that they are not conducting a Fourth Amendment search. Unless and until the stored information is "exposed" in some way to a human being, the police will argue, the search is merely contingent, not completed.

Viewed as possible violations of the search clause, these arguments raise frustrating, metaphysical inquiries: If a bit falls in a packet sniffer, has it been searched? A situation that often raises the metaphysical conundrum is withdrawn consent. Consider the following hypothetical: the police interview a suspect of a crime and ask whether they can search his computer. He consents to the search. They haul the computer back to the lab and, before doing anything else, create an image copy. What happens if, after the copy is made, the suspect phones the officer to withdraw consent?<sup>19</sup> The police have no choice but to return the physical hardware in their possession; retention after withdrawn consent would be an unlawful seizure in violation of the Fourth Amendment.<sup>20</sup> But what about the digital image copy of the hard drive? Does the same prohibition on continued seizure apply, or is the lawfully-made image no longer protected by the Fourth Amendment? Can the police seal the image away in their locker, waiting for the day when they establish probable cause to search its contents? Once the suspect regains possession of his computer, after all, he is no longer "deprived" of the information on the drive.

#### *E. Other Technologies of Reproduction*

Even if the Seizure clause is interpreted too narrowly in the way I have described, some may find little cause for concern. The purported gaps in the Constitutional protection involve the government's use of technologies of reproduction that probably seem exotic to the average citizen who typically doesn't lay awake at night worried about packet sniffers and hard drive image duplicators. In fact, he probably doesn't even know what these things are. But the steady march of technology has a way of making the exotic exception the mundane median. We are in the age of Brandeis' "secret drawers," and the police have proven adept at removing papers from those drawers with little difficulty.<sup>21</sup>

---

<sup>19</sup> [Case on withdrawn consent.]

<sup>20</sup> If the police have found evidence of a crime during the period before the consent is withdrawn, they may be allowed to retain (but not search) the computer until a warrant can be obtained. [After viewing evidence of a crime stored on a computer, agents may need to seize the computer temporarily to ensure the integrity and availability of the evidence before they can obtain a warrant to search the contents of the computer. See, e.g., Hall, 142 F.3d at 994-95; *United States v. Grosenheider*, 200 F.3d 321, 330 n.10 (5th Cir. 2000).] *See generally* U.S. Department of Justice, *SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS* n.2 (2002).

<sup>21</sup> *Olmstead*, 277 U.S. at xxx (Brandeis, J., dissenting) ("The progress of science in furnishing the Government with means of espionage is not likely to stop with

Today, the police are quite adept at using tools that can duplicate the data stored in personal computers, corporate servers, and held by Internet service providers. These capabilities will be more important in the near term, as more devices store more information about different types of transactions. For example, the number of devices that track and record information about a person's physical location—from cell phones to toll payment transponders to RFID tags—is increasing, and the police no doubt are working on technology that can collect that information from centralized network servers as well as from the memory chips in the devices themselves.

#### *IV. Twenty-First Century Seizure*<sup>22</sup>

To determine whether the constitutional limit on unreasonable seizure protects anything other than our possessory interests in physical objects, it helps to ask the question, why is dispossession important? Supreme Court cases about physical seizure view dispossession as a matter of simple rivalry: if you have my locked box, I can't have it too. But in the age of nonrivalrous, perfect digital copying, this view of dispossession seems tautological and unhelpful.

I propose a new test for seizure in cases involving intangible property: Does the government's copying of intangible property produce negative effects on par with the effects of physical dispossession? In particular, does the government's copy prevent the owner from altering, destroying or otherwise changing the state of his property? If you take my physical box full of letters, I am dispossessed of them, which harms me because I cannot give away, alter, or destroy them. I have lost the ability to control my property. This not only diminishes the value of my property, but it also invades my privacy.

The text of the Fourth Amendment seems broad enough to protect this “right to destroy” or, in the computer context, “right to delete” by its terms through its prohibition on unreasonable seizure. It is not surprising that the Bill of Rights would protect such a right. There is a long tradition of recognizing the right to destroy in property law. As Lior Strahilevitz has discussed, at various times in legal history courts have identified the right to destroy property as one of the “bundle of rights” intrinsic to physical possession.<sup>23</sup> This right is tied to the rights of dominion and control. The right to is protected—even in instances where it may seem unsavory—because without the extreme

---

wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.”).

<sup>22</sup> Parts of this section are adapted from a forum-format essay I authored in the Harvard Law Review Forum, where I began to develop this idea. See Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2006). Some paragraphs are taken almost verbatim from that essay, and I have not separately cited each instance.

<sup>23</sup> Lior Strahilevitz, *The Right To Destroy*, 114 YALE L.J. 781, 794 (2005).

ability to change, delete, or destroy, virtually nothing will be left of the rights of dominion and control.<sup>24</sup>

As *Katz* demonstrated, property and privacy are bound up in one another. Protecting the property right to delete assures computer users that their words can be in some sense undone. This provides a sense of privacy that may lead to more candor in discussing sensitive matters electronically, and the increased candor benefits all of society, not only the owners of the data.

This privacy-reinforcing notion of the Fourth Amendment right to delete explains the reasoning and conclusions of the wiretapping courts. Although a wiretap does not dispossess me of my words, once it records my private conversation, my words have been in a sense taken from me — the wiretap deprives me of the ability to conceal or otherwise destroy those words. The right to delete can also explain cases that have held video recordings to be seizures under the Fourth Amendment.<sup>25</sup>

Similar logic helps answer the scenarios and technologies presented in Part III, the packet sniffer, hard-drive image, and withdrawn consent. Under my proposed definition for Seizure, these questions result in straightforward answers. In every one of these situations, a seizure has occurred. The owner of the information has lost the ability to delete, modify, secrete, or contextualize a copy of the information, even though he may have retained his own copy. No less than when the police commandeer an automobile or grab a box of records, the owner of the intangible property has lost dominion and control over his property. A seizure has occurred, and the Fourth Amendment should proscribe these acts absent warrant or exception.

Admittedly, there are differences between the change I propose and the revolution that was *Katz*. *Katz* represented a difference in kind—a refocus for "search" from property to privacy. The modern-day seizure, in contrast, is more of a difference in degree or definition. My view of seizure still rests on ideas about property, but a more modern, contemporary understanding of property.

*Katz* was, then, an incomplete revolution. The Fourth Amendment is more sensitive to modern realities of surveillance and search than it had been, but there remain anachronistic gaps in its protections.

[...]

## V. Conclusion

---

<sup>24</sup> See *id.* at 794–95 (describing the right to destroy as an extreme version of the rights to exclude, use, and control subsequent alienation).

<sup>25</sup> See *Ayeni v. Mottola*, 35 F.3d 680, 688 (2d Cir. 1994), *abrogated on other grounds* by *Wilson v. Layne*, 526 U.S. 603, 618 (1999).