Stanford Technology Law Review

The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property

PAUL OHM *

CITE AS: 2008 STAN. TECH. L. REV. 2
http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf

I. INTRODUCTION

¶1 The Fourth Amendment's[1] Seizure Clause is mired in the eighteenth century. Its counterpart, the Search Clause, has evolved through a steady progression of Supreme Court cases from *Berger*[2] to *Katz*[3] to *Kyllo*,[4] no longer confined to the property-based interests embodied in *Olmstead v. United States*.[5] Instead, the Search Clause is sensitive to modern privacy concerns by extending constitutional protection to situations that satisfy 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.

¶2 In contrast, the Seizure Clause is in an *Olmsteadian* holding pattern, consistently interpreted to protect only physical property rights and to regulate only the deprivation of tangible things.

¶3 This Article argues for a twenty-first century definition of constitutionally proscribed property deprivation. A constitutionally significant "seizure" occurs whenever the state takes dominion or control of personally owned data or meaningfully interferes with an individual's right to control his data.

¶4 The Supreme Court implicitly supported this rule in *Berger* and *Katz*, holding in no uncertain terms that voice conversations are both searched and seized when recorded by the police.[6] Initially, many lower-court cases extended these rulings and applied the Fourth Amendment's Seizure Clause

---

* © 2008, Paul Ohm, Associate Professor, University of Colorado Law School. I would like to thank the editors and other members of the Stanford Technology Law Review and The Center for Internet and Society for their enlightening symposium and expert editing. In particular, I would like to thank Eric Chan for his help and enthusiasm. Thanks also to my co-panelists and the other attendees of the symposium for their comments, including Don Dripps, Richard Downing, Lauren Gelman, Kevin Bankston, Jennifer Granick, Orin Kerr, Richard Salgado and Jim Dempsey. I would also like to thank my excellent research assistant, Rose Banning. Thanks also to Kaleb Sieh for help cite-checking. Finally, thank you to Declan McCullagh for authoring a scintillating news account of my comments at the symposium.

[1] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

[2] Berger v. New York, 388 U.S. 41 (1967).

[3] Katz v. United States, 389 U.S. 347 (1967).

[4] Kyllo v. United States, 533 U.S. 27 (2001).

[5] 277 U.S. 438 (1928).

[6] *See* Part I.C.

to intangible things,[7] but after a few "clarifying" statements of the Supreme Court, particularly some dicta in *Arizona v. Hicks*,[8] recent courts faced with intangible seizure have ignored the statements in *Berger* and *Katz*.[9] The Article explores the evolution of the rule in Part I.

¶5 Reconceiving the Seizure Clause in light of modern concerns about intangible property rights can solve many vexing Fourth Amendment puzzles, discussed in Part II, 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 it did not look at the contents without a subsequent warrant?

¶6 Part III urges courts to return to its prior interpretations of the seizure clause, proposing several possible rule formulations. Finally, Part IV wades tentatively into the age-old search to identify the Fourth Amendment's protected values. Does the Amendment protect privacy, property, security, or something else? For the forty years between *Olmstead* and *Katz*, the Courts answered this question too narrowly, choosing property over the others in the list. *Katz* recognized the Fourth Amendment's other values, but subsequent decisions have cut back on its important insights.

¶7 It has been forty years again since *Katz*. Awesome technologies have arisen in the meantime that none of the justices in 1967, much less in 1928, could have foreseen. Modern surveillance technologies can duplicate without revelation. Courts might hold that these tools neither search nor seize, unaware that by doing so, they breathe new life into *Olmstead's* once-dead legacy.

II. *OLMSTEAD* REDUX: TODAY'S PROPERTY-BASED SEIZURE CLAUSE

A. Olmstead *and* Katz

¶8 *Olmstead v. United States* involved a Prohibition-era police investigation into bootlegging and liquor smuggling.[10] The police wiretapped several phone lines at homes and offices, taking care to install the wiretaps in publicly accessible locations like office basements and phone lines along public streets.[11] The Court refused to suppress the wiretapped communications, embracing an unequivocal, property-based conception of the Fourth Amendment.[12] "The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses of [sic] offices of the defendants."[13]

¶9 *Olmstead's* property-based conception of the Fourth Amendment was steadily eroded over time,[14] yet it held powerful sway until the Warren Court in the 1960s. The unofficial death knell was the 1967 case, *Katz v. United States*.[15]

¶10 Two generations of scholars have commented on the shift from *Olmstead's* property-based conception of the Fourth Amendment to *Katz's* privacy-based reasonable expectation of privacy test.[16] Although some scholars disagree,[17] *Katz* represents to most observers of criminal procedure a

---

[7] *See* Part I.D.

[8] 480 U.S. 321 (1987).

[9] *See* Part I.E.

[10] 277 U.S. 438 (1928).

[11] *Id.* at 456-57.

[12] *Id.* at 463-64, 66.

[13] *Id.* at 464.

[14] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974) ("[T]he process of whittling it away began in 1961 . . . .").

[15] 389 U.S. 347 (1967).

[16] *See, e.g.*, Morgan Cloud, *Pragmatism, Positivism and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 248-49 (1993).

[17] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2004) ("*Katz* has had a surprisingly limited effect on the largely property-based contours of traditional Fourth Amendment law.").

strong signal that the Fourth Amendment will not be constrained to crabbed, property-based rules.[18] The *Katz* revolution, however, is fundamentally incomplete, and a lurking property-based view of the Fourth Amendment still prevails in courts when seizure, not search, is the issue.

B. Olmstead *Redux*

¶11 In 1977, David Edward Thomas sent a misaddressed package through UPS that never arrived at its destination.[19] Unfortunately for him, the package broke open in a UPS facility while the shipper was deciding what to do with it. UPS employees spied inside what they thought was pornography and called the FBI.[20] The FBI photocopied the enclosed papers and returned the originals to UPS.[21] 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. A photocopy, the court held, is not a physical dispossession, so nothing had been "seized."[22]

¶12 In 2000, the FBI duplicated the files of another person, Vasiliy Gorshkov.[23] Gorshkov's files were intangible: 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 from Russia to Seattle with the promise of a job, secretly observed him typing in a password to his Russian computer from a bugged system, and logged into that Russian computer and downloaded copies of his files.[24] As in the *Thomas* case, the district court judge held that nothing had been seized.[25] "The data remained intact and unaltered. . . . The copying of the data had absolutely no impact on [Gorshkov's] possessory rights."[26]

¶13 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*,[27] and four decades after *Olmstead* was supposedly laid to rest in *Katz v. United States*,[28] the specter of the property-based Fourth Amendment still haunts our constitutional hallways.

¶14 Under the modern interpretation of the Fourth Amendment, the government *seizes* property only when it "'meaningfully interfere[s]' with [a] possessory interest."[29] Courts have not articulated precisely what is meant by this phrase, and "possession" seems broad enough to embrace interests in intangible things, but cases like those cited above reveal that the test applies a physical property-centric model of dispossession. The phrase has been 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 possessional binary-ness cannot be seized unless and until the government deprives the owner of every last copy of the property.

---

[18] For example, this is how treatise writers usually discuss *Katz*. *See, e.g.*, JEROLD H. ISRAEL & WAYNE R. LAFAVE, CRIMINAL PROCEDURE IN A NUTSHELL 60 (5th ed. 1993) ("Th[e] property approach was rejected in Katz v. U.S. (1967), in favor of a privacy approach.").

[19] United States v. Thomas, 613 F.2d 787, 789 (10th Cir. 1980).

[20] *Id.*

[21] *Id.* at 793.

[22] *Id.* (citing United States v. Lisk, 522 F.2d 228, 230 (7th Cir. 1975); United States v. Haden, 397 F.2d 460, 465 (7th Cir. 1968)).

[23] *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001).

[24] *Id.*

[25] *Id.* at *3. In the alternative, the court also held that the computers in Russia owned by a non-resident of the United States were unprotected by the Fourth Amendment under *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[26] *Id.*

[27] 277 U.S. 438 (1928).

[28] 389 U.S. 347 (1967).

[29] Arizona v. Hicks, 480 U.S. 321, 324 (1987) (quoting Maryland v. Macon, 472 U.S. 463, 469 (1985)); *see also* United States v. Jacobsen, 466 U.S. 109, 113 (1984). The word "seizure" in the Fourth 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 Article is limited to seizure of property.

¶15 The result is positively *Olmsteadian*. The Fourth Amendment protects tangible items and does not protect intangible information. Although intangible information can be searched when the government invades a reasonable expectation of privacy protecting it, when that expectation of privacy is not breached, the Fourth Amendment plays no role. Thomas and Gorshkov no doubt felt wronged to learn that the FBI had copied their intangible data without warrants, but this felt harm did not rise to the level of a constitutional property invasion.

¶16 *Thomas* and *Gorshkov* are consistent with a long line of cases stretching back two decades and leading back to Supreme Court cases that have held that seizure means physical dispossession. These two decades, however, themselves represent a break without reason or justification from what the Supreme Court and lower courts had done in the prior twenty years. To explain the shift, we can start back at the beginning, with *Berger* and *Katz*.

C. The Voice Cases

¶17 The first, most straightforward evidence that cases like *Gorshkov* and *Thomas* have misconstrued constitutional seizure is that the Supreme Court has expressly held that the recording of the human voice is a seizure for Fourth Amendment purposes. Obviously, nobody is deprived of any possessory interest in his voice when a police tape recorder or wiretap records his conversations. Nonetheless, in *United States v. Berger*, the Court struck down New York State's statute governing wiretaps as insufficiently protective of Fourth Amendment interests because it "permit[ted] a trespassory invasion of the home or office, by general warrant, contrary to the command of the Fourth Amendment."[30] Along the way, the Court, in the words of Justice Douglas's concurring opinion, overruled *Olmstead* "sub silentio."[31]

¶18 In so ruling, the Court made it plain that the wiretaps authorized by the New York statute were seizures, as well as searches. It held that "the statute's failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations."[32] Furthermore, the Court held that "authorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause,"[33] and also that during this time "the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately."[34]

¶19 Similarly, in *Katz v. United States*,[35] which extended the Fourth Amendment to recorded voice conversations, the Supreme Court, in response to the government's argument that the Fourth Amendment "was thought to limit only searches and seizures of tangible property,"[36] noted that "(t)he premise that property interests control the right of the Government to search and seize has been discredited."[37] "[T]he Fourth Amendment governs not only the seizure of tangible items," the Court continued, "but extends as well to the recording of oral statements overheard without any 'technical trespass under * * * local property law.'"[38] On this point, the Court was unambiguous: "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."[39]

---

[30] 388 U.S. 41, 64 (1967).

[31] *Id.* at 64 (Douglas, J., concurring).

[32] *Id.* at 59; *see also id.* (holding that the statute's requirement that persons be named "does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions *to be seized*") (emphasis added).

[33] *Id.*

[34] *Id.*

[35] 389 U.S. 347 (1967).

[36] *Id.* at 352-53.

[37] *Id.* at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

[38] *Id.* at 353 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)) (omission in original).

[39] *Id.* at 353.

¶20 It may be argued that the Court was talking loosely about the "search and seizure" requirements, demonstrated by the fact that subsequent cases have focused almost exclusively on the search that occurs during a wiretap. Perhaps the Court was speaking about the Fourth Amendment *writ large*, without focusing on a search and a seizure as two separate acts. This argument is refuted by the fact that the opinions in both cases sit alongside forceful dissents by Justice Black that specifically raise arguments against finding these acts to be seizure.

¶21 In *Berger*, Justice Black opined that "[i]t simply requires an imaginative transformation of the English language to say that conversations can be searched and words seized."[40] In *Katz*, Justice Black argued that "the language of the second clause indicates that the Amendment refers not only to something tangible so it can be seized but to something already in existence so it can be described."[41] Also, the Fourth Amendment's "words connote the idea of tangible things with size, form, and weight, things capable of being searched, seized, or both."[42] Furthermore, the Amendment is designed "to protect against warrantless searches of buildings and seizures of tangible personal effects."[43]

¶22 Also in *Katz*, Justice Black took issue with the majority's use of an earlier case, *Warden v. Hayden*,[44] declaring that the prior case "upholds the seizure of clothes, certainly tangibles by any definition," reading the case to involve "only . . . the common-law rule that the right to seize property depended upon proof of a superior property interest."[45] In the face of the specificity in Justice Black's dissents, it is hard to imagine that the majority was being careless in considering constitutional "seizure" as a distinct doctrine from search.

D. Early Intangible Seizure Cases

¶23 In the first two decades following *Berger* and *Katz*, a number of lower courts cited the pair of cases to support holding that intangible items can be seized. For example, in *LeClair v. Hart*, the Seventh Circuit held that IRS agents seized documents by dictating their contents verbatim into a tape recorder and by taking copious notes.[46] Pointing to *Berger*, the court ruled that these acts constituted seizure under the Fourth Amendment:

> Following *Berger*, it has been clear that the Fourth Amendment embraces more than just the forced physical removal of tangible objects . . . . Indeed, *Berger* stands for the proposition that the government may seize intangible items such as the information contained in the financial documents which the IRS agents copied.[47]

¶24 Questions of intangible seizure have often arisen when the police have copied down the serial numbers inscribed on suspected stolen property. Until the Supreme Court mis-analyzed this issue in *Hicks*, discussed in the next Subpart, a number of lower courts had held that the act of copying down numbers amounted to a seizure. For example, in *United States v. Gray*, the Sixth Circuit held that an officer seized the serial numbers inscribed on rifles when he copied them down.[48] The Fifth Circuit came to a similar conclusion in a case involving serial numbers on air conditioners.[49]

---

[40] 388 U.S. 41, 78 (1967) (Black, J., dissenting).

[41] 389 U.S. 347, 365 (1967) (Black, J., dissenting).

[42] *Id.*

[43] *Id.* at 367.

[44] 387 U.S. 294 (1967).

[45] *Id.* at 372.

[46] 800 F.2d 692 (7th Cir. 1986).

[47] *Id.* at 695. In this *Bivens* action, the Court declined to decide whether the access to the records was also an unlawful search. Because the ruling arose in response to a motion for summary judgment due to qualified immunity, by holding that the seizure was illegal under "clearly established law," the motion was properly denied, and a ruling on the extent of the constitutional violation could be deferred. *Id.* at 694.

[48] 484 F.2d 352 (6th Cir. 1973).

[49] United States v. Sokolow, 450 F.2d 324 (5th Cir. 1971) (holding that taking serial numbers from air conditioners found in a garage is a seizure).

¶25 All of these cases place the seizure of intangible property squarely within the ambit of the Constitution.[50] Also, in every one of the cases cited, the court also held that the seizure was unlawful. The trend recognizing intangible seizure is even broader if one also takes into account cases that have found intangible seizure reasonable or otherwise constitutional, often under the plain view rule.[51] In fact, this seemed like a reasonable application of *Berger* and *Katz*. Intangible property was seized when reproduced, subject to many exceptions. Unfortunately, the Supreme Court upset this logical approach, perhaps inadvertently, in a few subsequent cases.

E. The (Inadvertent?) Return to the Physical Interpretation of Seizure

¶26 The Supreme Court is to blame for the confusing turn in the law that has led to opinions like *Thomas* and *Gorshkov*. In *United States v. Jacobsen*, the Court was faced with a claim of seizure of physical, not intangible, property: a "trace amount" of white powder which turned out to be cocaine.[52] The Court held that by field testing the trace amount, the DEA agents "seized" the powder, but the seizure was held reasonable when balanced against law enforcement interests and the "de minimis" impact on the defendant's interest in his property was considered.[53] To support this sensible holding, the Court for the first time relied on the "meaningful interference with an individual's possessory interests in . . . property" test.[54] Still, the *Jacobsen* Court could not have anticipated how this test would later be used to restrict intangible seizure, because the case dealt only with physical evidence.[55]

¶27 Nevertheless, *Jacobsen* is the source of the river, so to speak, the statement of the rule that has been cited repeatedly for the holding, *contra Berger* and *Katz*, that seizure protects against only physical dispossession. While *Jacobsen* talked only about that which was sufficient to be seizure, the rule has come to stand for what is necessary for seizure.[56]

¶28 The Supreme Court's first step down the road from *Jacobsen* to a test that precludes seizure of intangible property was *United States v. Karo*.[57] In *Karo*, police placed an electronic tracking device into a container owned by defendant, an act the majority of the Court held not to be a seizure, citing the *Jacobsen* test.[58] The Court held that "[a]lthough the can may have contained an unknown and

---

[50] In addition to the cases cited above, see Davis v. Mississippi, 394 U.S. 721, 724-28 (1969) (finding an unlawful seizure of fingerprints where police had obtained them during an improper detention); United States v. Johnson, 452 F.2d 1363, 1371 (D.C. Cir. 1971) (suggesting, before remanding, that "the photographic seizure of [the defendant's] person during an involuntary detention may run afoul of the Fourth Amendment's proscription against unreasonable searches and seizures."). *See also* United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986) (construing Rule 41, holding that a "surreptitious entry" warrant authorized a seizure of intangible property, namely, "information regarding the 'status of the suspected clandestine methamphetamine laboratory'"); State v. Murray, 527 P.2d 1303, 1308 (Wash. 1974) ("The serial numbers were not within the plain view of the officers, and their being obtained by the tilting of the Sony television constituted a warrantless seizure of those numbers."). *But see* United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980) (holding that making a photocopy is not a seizure).

[51] *See, e.g.*, United States v. Marbury, 732 F.2d 390 (5th Cir. 1984) (finding the copying of identification numbers of equipment was not an unlawful seizure under the plain view doctrine or, alternatively, under the "open fields" doctrine); Sovereign News Co. v. United States, 690 F.2d 569 (6th Cir. 1982) (analyzing note-taking by officers as a "seizure" but ultimately finding no unlawful seizure under the plain view doctrine); United States v. Espinoza, 641 F.2d 153, 166 (4th Cir. 1981) (suggesting that photographing the scene of an executed search warrant might be a seizure, but ruling "the plain view doctrine justified" the photographs); United States v. Wolfe, 375 F. Supp. 949, 957 (E.D. Pa. 1974) (analyzing the copying of a federal probation report as a seizure, but concluding no unlawful seizure occurred because the plain view doctrine applied or, alternatively, because the report could be considered an item "reasonably related to the purposes of the search" to which the search warrant could lawfully be extended).

[52] 466 U.S. 109, 125 (1984).

[53] *Id.*

[54] *Id.* at 113. In a much earlier case, the Court held that "a seizure contemplates a forcible dispossession of the owner." Hale v. Henkel, 201 U.S. 43, 76 (1906).

[55] LeClair v. Hart, 800 F.2d 692, 695 (7th Cir. 1986) ("The Court [in *Jacobsen*] was discussing a package containing drugs, a tangible physical item, and thus the Court had no occasion to discuss the definition of seizures in the context of intangible property.").

[56] *Jacobsen* was cited in *Maryland v. Macon* for the proposition that undercover agents do not seize magazines that they buy from the proprietor of an adult bookstore. 472 U.S. 463, 469 (1985). Again, this was a case about tangible property, so the "meaningful interference" test still had no particular bearing on intangible property.

[57] 468 U.S. 705 (1984).

[58] *Id.* at 712.

unwanted foreign object, it cannot be said that anyone's possessory interest was interfered with in a meaningful way."[59]

¶29 The shift in regarding the "meaningful interference" test as not simply sufficient but necessary was finally completed in *Arizona v. Hicks*, where the Court concluded that copying serial numbers from the bottom of a stereo was not a seizure, but suppressed the serial numbers anyway by holding that the police unlawfully "searched" the equipment by moving it to reveal the serial numbers.[60]

¶30 Because the Court found an unconstitutional search and upheld the lower court's decision to suppress the serial numbers as the fruit of the search, anything said in *Hicks* about copying and seizure is dicta. But in this dicta, the Court erred by concluding that copying serial numbers was not a seizure. In the majority opinion, Justice Scalia singled out search as the principal protector of privacy within the Fourth Amendment and relegated seizure to a more crabbed role, protecting only possessory property interests. *Hicks* seems at odds with *Berger* and *Katz*, yet the Court never cites those cases in coming to this conclusion and makes no attempt to explain the discrepancy.

¶31 In light of *Hicks*, in particular, lower courts have retreated from their position in the late 1970s and early 1980s of finding the seizure of intangible property.[61] In addition to *Thomas* and *Gorshkov*, courts have found all of the following acts not to be a seizure: photographing the scene of the execution of a search warrant;[62] photocopying several file cabinets worth of documents;[63] and copying the VIN from a car.[64]

III. THE GAP IN FOURTH AMENDMENT PROTECTION: TECHNOLOGIES OF REPRODUCTION

A. The Masking Effect of Search

¶32 That the *Olmsteadian* Seizure Clause persists four decades after *Katz* and eight decades after *Olmstead* is not entirely surprising. In nearly every case in which intangible property has been "seized," something first had to have been searched,[65] and the reasonable expectation of privacy test

---

[59] *Id.* The Court also held that monitoring a beeper while it is inside a private residence requires a warrant. *Id.* at 718.

[60] 480 U.S. 321, 324 (1987).

[61] A few courts have continued to adhere to the rule that intangible data can be seized. *See, e.g.*, United States v. Meriwether, 917 F.2d 955, 958 (6th Cir. 1990) ("The agent in the instant case, by seizing and examining the contents of the pager, was acting in conformity with the warrant."); Smith v. State, 713 N.E.2d 338, 344 (Ind. App. 1999) ("[W]e conclude that the Fourth Amendment affords protection from the unreasonable search and seizure of the computer memory of a cellular phone to retrieve its electronic contents."). *Meriwether* and *Berger* were cited in *United States v. David*, 756 F. Supp. 1385, 1389 (D. Nev. 1991), for the proposition that "[t]he Courts have . . . recognized that information, i.e., *intangible* items, may be seized within the meaning of the *Fourth Amendment*."

[62] *See* United States v. Mancari, 463 F.3d 590, 596 (7th Cir. 2006) ("Nor did the photographing of the money [at the scene of the executed warrant] by police constitute an unreasonable seizure."); Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) ("[T]he 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."). Interestingly, the *Bills* court keeps the door open to the possibility that photographing the scene of a warrant's execution may constitute a seizure. First, as an alternative to the "no meaningful interference" holding, the court notes that "[b]ecause the police officers in this case were properly on the Bills' premises, they could record by photography scenes presented to their plain view." *Id.* It should have been unnecessary to talk about the plain view test if nothing had been seized. Additionally, the court hinted that a third party, Meisling, who had been invited along on the search and who took photographs of property possibly stolen from his employer, *might* have been improperly seizing. *Id.* The court declined to reach this question, however, because Meisling had previously settled the section 1983 lawsuit brought against him. *Id.* at 701, 707-08.

[63] *Cf.* United States v. Chapman, 559 F.2d 402, 407-08 (5th Cir. 1977) (holding no obligation to return photocopies of materials to former defendant after indictment dismissed).

[64] McDonald v. State, 119 S.W.3d 41 (Ark. 2003).

[65] The Seventh Circuit has observed that

> seizures made in the course of investigations by police or other law enforcement officers are almost always, as in the plain view cases, the culmination of searches. The police search in order to seize, and it is the search *and ensuing seizure* that the Fourth Amendment by its reference to "searches and seizures" seeks to regulate.

Soldal v. County of Cook, 942 F.2d 1073, 1079 (7th Cir. 1991) (en banc), *rev'd*, 506 U.S. 56 (1992). The Supreme Court, in reversing the Seventh Circuit, singled out the passage from which this quote is drawn by saying, "[w]e have difficulty with this passage." Soldal v. Cook County, 506 U.S. 56, 68 (1992). What seemed to trouble the Supreme Court, however, wasn't the empirical observation that searches and seizures "almost always" happen together, but rather the further part of the quote (omitted above) suggesting that seizures are unprotected when unaccompanied by search. *Id.* at 68-69.

for search has tended to resolve these cases in ways that have been unobjectionable to most observers. Courts have rarely had to grapple with the true effects of the crabbed Seizure Clause because search has been enlisted to lead courts to unobjectionable results. With intangible property, search and seizure often go hand-in-hand because of three facts about the world:

¶33 First, as *Hicks* exemplifies, we live in what I call an *atoms-before-bits* world. Historically, the government has had to deprive a person of physical property (even if momentarily) before it could make a copy of his intangible property. In *Hicks*, the serial numbers were visible only after the stereo equipment was moved.[66] Similarly, in order to copy the bits from a hard drive, the government must open the physical case of the computer containing the hard drive.[67]

¶34 Second, a lot of intangible property is held by third-party intermediaries. Google keeps my calendar and RSS feed reader settings, my employer stores my e-mail messages, and Amazon keeps a record of my past purchases. Intangible data tend not to be left lying around in publicly available spaces, and third parties serve as gatekeepers between the data and the police.[68] These gatekeepers serve as a brake on unchecked police access to data, although some fear that they are merely a speed bump.[69]

¶35 Third, people use code to express expectations of "virtual" privacy when they go online. For example, even in purely virtual settings, the borders of private "spaces" are delineated by virtual walls and doors, such as passwords and computer dialog boxes.[70] You can't access my inbox unless you know my login name and password.[71] The reasonable expectation of privacy test recognizes these virtual doors and walls, treating them like their physical equivalents.[72] Similarly, people delete files, expressing their desire to make data inaccessible to others. The rules for search are flexible enough to apply in these situations, and the police can't bypass these virtual constraints without complying with the Fourth Amendment.

¶36 For these three reasons, until recently, the police have not been able to collect intangible data without first intruding physically or virtually on expectations of privacy. When they have done that, they have searched, subjecting their acts to constitutional scrutiny. In this way, the Search Clause has served as a mask, obscuring the negative effect of the cramped way in which seizure has been construed.

---

[66] Arizona v. Hicks, 480 U.S. 321 (1987) (holding the copying of serial numbers not to be a seizure but suppressing the serial numbers because they were revealed after a "search" involving the lifting of the stereo equipment).

[67] *Cf.* United States v. Simons, 206 F.3d 392, 398-401 (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).

[68] *See* Eric Lichtblau, James Risen & Scott Shane, *Wider Spying Fuels Aid Plan for Telecom Industry*, N.Y. TIMES, Dec. 16, 2007, § 1, at 11 ("The federal government's reliance on private industry has been driven by changes in technology. Two decades ago, telephone calls and other communications traveled mostly through the air, relayed along microwave towers or bounced off satellites. The N.S.A. could vacuum up phone, fax and data traffic merely by erecting its own satellite dishes. But the fiber optics revolution has sent more and more international communications by land and undersea cable, forcing the agency to seek company cooperation to get access.")

[69] This is because third-party intermediaries tend to make it easy for the police to access data, and to do so without the subscriber's knowledge. This is the lesson of the Thomas case. Because UPS possessed the box that was "inadvertently broken open," the FBI could investigate without ever needing to notify the defendant. United States v. Thomas, 613 F.2d 787, 789 (10th Cir. 1980); *see also* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 518-21 (2005) (discussing the third-party doctrine).

[70] *See* United States v. Andrus, 483 F.3d 711, 723 (10th Cir. 2007) (McKay, J., dissenting) (describing "outward signs of . . . protection" that indicate security used on computers, such as password prompts at boot, log-in, and re-activation from a screen-saver).

[71] Until recently, virtual doors could be opened simply by knowing some fact stored in my brain or written down on a piece of paper in my office. New technology sometimes requires also having some physical thing belonging to me, like a keychain displaying a highly accurate, frequently changing six-digit number, or my fingerprint or retina pattern.

[72] Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) ("[P]assword-protected files are analogous to the locked footlocker inside the bedroom.").

B. Why the Search Clause is Not Enough

¶37 There are significant problems with relying on search to do all of the work in protecting privacy when it comes to our intangible property. First, the word "search" often inadequately describes the government's invasions. Atoms-before-bits cases like *Hicks* seem strangely counter-intuitive; the Fourth Amendment protects what we really cared about—our information—only because it happens to be encased in a physical box we care very little about.[73] Cases like *Hicks* reach the right result but only by focusing on issues of relatively marginal importance, leading to hyper-technical rulings.

¶38 Second, comparing virtual doors and walls to their physical counterparts raises problems typical with reasoning by analogy.[74] Software is contingent and constructed, and it can be used to create an infinite variety of "doors," many of which differ in fundamental ways from physical doors. Analogy's problems do not lead inexorably to unfair results, but they cause unpredictability. Given the infinite variability of the many aspects of physical walls and doors that can be compared, courts can often pick or chose analogies to support any result. Everybody—the police in the field as well as the people trying to protect their intangible data from government invasion—is left unsure how a court will rule on the propriety of any particular police act. Third, this counter-intuitiveness and unpredictability make the test very difficult to apply.

C. Naked Seizure: How New Technology Enables Seizure Without Search

¶39 Counter-intuitiveness, unpredictability, and difficulty in application should be enough to warrant a closer look at the current approach to intangible seizure, but there is another, more important problem looming. Profound shifts in technology will end the happy confluence of search and seizure. Because of these shifts, the police will much more frequently grab intangible data without having to handle atoms, pass through virtual walls, or deal with intermediaries. I call these kinds of acts "naked seizures." From the *Hicks* dictum and its progeny, we know that courts will not consider these acts to be seizures, and they may not find them to be searches, either, justifiably concluding that during naked seizures the police do not intrude on a reasonable expectation of privacy. Instead, these invasive acts might fall completely outside the Fourth Amendment.

¶40 Although search has proved the bulwark protecting us from rampant acts of naked seizure, developments in technology are putting pressure on this bulwark. In dissent in *Olmstead*, Justice Brandeis predicted that "[w]ays may some day 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."[75] Today, as explored in this Subpart, electronic secret drawers are everywhere.

¶41 Furthermore, the police have adapted well to new forms of secret drawers, using tools that can duplicate the data stored on electronic devices. These police practices are both profoundly useful and invasive, because more devices store larger quantities of information about an expanding variety of transactions. As the police continue in this manner, accessing and copying intangible information unhindered by the protections of the trio of attributes—atoms-before-bits, virtual doors, and intermediaries—that have always coupled search and seizure, the harmful effects of the misguided rule from *Hicks* will be felt. Consider how each of the protective trio has diminished in recent years.

1. Ignoring Physical Barriers

¶42 First, physical constraints are disappearing, with the police able to access intangible data at a distance and without breaching physical barriers. No longer will they need to lift record players to

---

[73] *See* William C. Heffernan, *Property, Privacy, and the Fourth Amendment*, 60 BROOK. L. REV. 633, 643 (1994) ("What is critical to informational privacy, then, is not the presence of a physical 'shell' that contains facts about someone's life, but an individual's control over the dissemination of the facts themselves.").

[74] *See generally* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

[75] Olmstead v. United States, 277 U.S. 438, 474 (Brandeis, J., dissenting).

read serial numbers; the devices themselves will report their serial number through the air when asked.[76]

¶43 Consider the amazing recent developments in wireless networking. In most cities, ubiquitous WiFi networks allow users to transmit data over the Internet using radio waves. With specialized but inexpensive equipment, WiFi signals can be intercepted. Although WiFi can be encrypted, some forms of WiFi encryption are notoriously insecure.[77]

¶44 Another wireless protocol, Bluetooth, allows people to share information between devices (and sometimes with the Internet) but at closer ranges than does WiFi.[78] Although Bluetooth is also not quite as flexible as WiFi, it is used to transmit communications that most citizens (and the police) would consider very revealing and private.[79] Like WiFi, Bluetooth security has been criticized and attacked,[80] and there have been reports of so-called Bluetooth sniffing,[81] techniques which the police could use to download a target's address book or calendar from half-a-block away.

2. Bypassing Third Parties

¶45 Second, although third-party intermediaries are still important (and arguably increasingly important given the expansion of online services which encourage people to store more data online), many Internet communications can be monitored without the assistance of third-party gatekeepers. Consider packet sniffers. Packet sniffers are wiretaps for computer networks, computer programs that collect any electronic communications that flow through the place on the network where the sniffer is running.[82] If the sniffer is located at a point in the network through which the communications of many other computers flow—imagine a major network switch—the sniffer will capture everything: e-mail messages, instant messages, web page requests, and YouTube videos crossing that switch.

¶46 The revelation of the NSA's massive wiretapping program[83]—which almost certainly involves the use of powerful packet sniffers—has confirmed many conspiracy theories.[84] Even before the program was revealed, academics had analyzed hypothetically the legality of massive governmental network monitoring, but they focused almost exclusively on the Fourth Amendment's search prong,[85] while ignoring the seizure prong. Is it a Fourth Amendment seizure for the government to collect information indiscriminately and on a massive scale? Does it matter if a human being—the

---

[76] Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605, 1622 (2007) (describing RFID technology and noting that "RFID's major improvement over existing auto-identification technologies is its ability to read information about items at a distance and through barriers").

[77] In particular, the Wired Equivalent Privacy or WEP protocol has been repeatedly cracked. *See* Nancy Cam-Winget et al., *Security Flaws in 802.11 Data Link Protocols*, 46 COMM. ACM, May 2003, 35, 36 ("The . . . attack is devastating to WEP. Once the WEP key is discovered, all security is lost.").

[78] Bluetooth comes in three classes of allowable power, with the range varying from one meter to 100 meters, depending on the power class. Joshua Wright, *Dispelling Common Bluetooth Misconceptions*, SANS TECH. INST., Sept. 19, 2007, http://www.sans.edu/resources/securitylab/bluetooth.php (listing power classes and "intended range").

[79] For example, many telephones transmit voice conversations to wireless Bluetooth headsets (the kind seen with increasing frequency clipped to the ears of businesspeople). Similarly, many telephones and PDAs use Bluetooth to transmit e-mail, address book, and calendar information.

[80] Wright, *supra* note 78 (citing studies about the weaknesses in Bluetooth's E0 encryption protocol).

[81] Annalee Newitz, *They've Got Your Number* ..., WIRED, Dec. 2004 (describing Bluetooth attacks on cellphones), *available at* http://www.wired.com/wired/archive/ 12.12/phreakers_pr.html.

[82] A fundamental computer networking technology is Ethernet. *See* IEEE STANDARD 802.3-2005 (IEEE Standards Ass'n, 2005), *available at* http://standards.ieee.org/ getieee802/802.3.html. On an ethernet, multiple computers share a communications path, such as a network cable. This allows for efficient resource allocation and simpler hardware, but it has the side-effect of letting every computer listen in to the conversations of every other computer using the shared cable.

[83] Eric Lichtblau & James Risen, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[84] *See* Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), Eur. Parl. Doc. (COM A5-0264/2001) 11, *available at* http://www.fas.org/irp/program/process/rapport_ echelon_en.pdf (describing ECHELON as "a global system for intercepting communications, operat[ed] by . . . the USA, the UK, Canada, Australia and New Zealand").

[85] *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38 (2005); *see also* Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

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?

¶47 Wireless networks can also be monitored without third-party assistance. With simple, relatively inexpensive tools, the police can intercept a suspect's communications while sitting in a car outside his home or in a booth next to him in a café.

3. Circumventing Virtual Constraints

¶48 Finally, the extra layers of virtual privacy that people use are sometimes easy to circumvent. Tools can get at data directly from storage, ignoring any passwords that may have been in place[86] and recovering so-called "deleted" files.

¶49 Consider the power of computer forensics. The first step in the analysis of a computer's hard drive is the bit-by-bit image copy.[87] Unlike the copies of files that ordinary users make, a bit-by-bit copy is a thorough, detailed reproduction of every piece of data stored on a computer's hard drive, performed using specialized hardware and software tools.[88] An image copy allows the police to preserve hidden pools of data that most ordinary users do not realize exist.[89] For example, the police can often recover deleted files.

¶50 In addition, computer forensics tools can defeat virtual privacy by bypassing login names and passwords. For example, in *United States v. Andrus*, agents used computer forensics tools to trawl through the contents of a computer.[90] Although the defendant had set up his computer to require a username and password, the agents were oblivious to this fact, having not configured their tool to recognize the presence of passwords, and viewing files that were intended to be inaccessible without a password.[91]

¶51 Not only can the police flout expressions of virtual privacy when searching stored data, they can do so while monitoring communications flowing across networks. Packet sniffers are typically used like vacuum cleaners: they indiscriminately suck up everything in their path, even communications that the user could not send or receive without entering a password first.

D. The Constitutionality of Collect Now, Analyze Later

¶52 New technologies allow the police to surveil at a distance, evading virtual constraints and bypassing third-party intermediaries. We might not worry about these technologies if we thought courts would regulate them as searches under the Fourth Amendment, hoping that the famous malleability of the reasonable expectation of privacy test would expand to cover these situations, striking the right balance between protecting privacy and allowing police investigations. In other words, we would hope that the test's vague contours and expansive language would protect us from undue government intrusion into intangible property, as it has in the past.

¶53 At first blush, one might assume that courts would find invasions of privacy in the types of cases described, because intuitively, they seem invasive and intrusive. Why should it matter whether the police lift a record player or interrogate it wirelessly, when the expectation of privacy invaded seems indistinguishable? But once intangible property loses the trio of protections described in Part II, the government can try to end-run the search cases by *sealing* what they have collected. Does a packet

---

[86] *See, e.g.*, United States v. Andrus, 483 F.3d 711, 719 n.5 (10th Cir. 2007) (McKay, J., dissenting) ("The difficulty with seeing a 'lock' on computer data is exacerbated by the forensic software sometimes used by law enforcement to conduct computer searches. The software . . . allows user profiles and password protection to be bypassed."); United States v. Buckner, 473 F.3d 551, 553 (4th Cir. 2007) (stating that the government's forensic software "would not necessarily detect user passwords" on password-protected computer files).

[87] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 557 (2006).

[88] *Id.*

[89] The list of hidden pools is a mouthful of technical jargon: deleted files, swap space, slack space (further divided into file slack and RAM slack), and cache.

[90] United States v. Andrus, 483 F.3d 711, 713-14 (10th Cir. 2007).

[91] *Id.*

sniffer conduct a search when it is programmed to seal its information away from police review? What if the image of a hard drive is stored on media that is immediately locked inside a cabinet at police headquarters? The reasonable expectation of privacy test turns, as a threshold matter, on an *intrusion* or *invasion*,[92] and the government has a reasonable argument that when it seals the collected data, it stops short of invading or intruding on the data owner's privacy. As long as none of the collected information is reviewed immediately, and as long as review requires an additional, tamper-evident step, the police can claim that they have not yet conducted 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.[93]

¶54 If courts examine copy-then-seal police investigations as violations of the Search Clause, they will often be faced with frustrating, metaphysical inquiries: if a bit falls in a packet sniffer, has it been searched? Consider the following hypothetical: The police ask a suspect whether they can search his computer, and he consents. They haul the computer to the lab and create an image copy before doing anything else. What happens if the suspect withdraws consent *after* the image copy has been made? The police would have no choice but to return the *physical* hardware in their possession; retention after withdrawn consent might be an unlawful seizure in violation of the Fourth Amendment.[94] They would also be absolutely barred from continuing to examine the contents of the original.

¶55 But what about the image copy? Would the prohibition on continued seizure and search apply, or would the lawfully-made image no longer be protected by the Fourth Amendment? Once the suspect regains possession of his computer, after all, he would no longer be physically deprived of anything, so the *Hicks* dictum would suggest no seizure. Nor would his reasonable expectation of privacy be intruded upon—meaning no search—by the bare, naked act of retention, because the image was made with his consent. Perhaps the police would be prohibited from opening the files and folders on the image, because those might be considered closed containers that could not be searched without a warrant.[95] But they would have a very good argument that they could store the image of the hard drive until they next obtained probable cause and a warrant to search.

¶56 Next consider what happens to the thousands of hard drives the FBI examines each year with search warrants. In each case, the warrant provides probable cause to open the folders and files on the drive, but for an ostensibly limited—in time and scope—purpose. Almost always, the FBI first takes a bit-by-bit image to help preserve the integrity of the original drive. What is the legal status of the image when the case is closed, following conviction, acquittal, or a decision not to prosecute, and once the original hard drive is returned? Presumably, under *Hicks*, keeping the data is not a continuing seizure, since the owner has had his physical property returned. There is no dispossession. Can the police lock the hard drive away on the off-chance that they learn that the owner of the data may have committed another crime? Can the police, in essence, create a snapshot of all of the personal data of every person who has ever fallen under this level of scrutiny?

¶57 The FBI might want to keep all of this data in case their owners commit future crimes, but even if their owners avoid future scrutiny, the data might still be useful for data mining. "Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns

---

[92] Katz v. United States, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring)

[93] Kerr, *supra* note 87, at 557 ("Once again, what matters is exposure to human observation.").

[94] *Cf.* Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding standing in case alleging FISA violations because of the "government's continued retention of derivative materials collected by covert surveillance"). 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.*, United States v. Grosenheider, 200 F.3d 321, 330 n.10 (5th Cir. 2000); United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998). *See generally* U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations n.2 (2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm [hereinafter DOJ Search and Seizure Manual].

[95] *See* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that the contents of closed files are not in plain view to agents with a warrant to search a computer).

and relationships in large data sets."[96] It has become an increasingly prominent part of efforts to detect and track potential terrorists.[97] Many legal scholars have criticized government data mining, some pointing out that experts are doubtful that data mining can lead to terrorists.[98] Others have criticized the "false positives" inevitable in data mining that lead to invasions of privacy or worse for those wrongly identified as potential terrorists.[99] But regardless of its efficacy, there can be no doubt that the government has faith in data mining, and the idea of indexing and searching hard drive images full of gigabytes of information about the most intimate details of the lives of suspects must be appealing to some in law enforcement. Under *Katz* the initial creation of the image copy with a warrant would not have been a search, and under *Hicks* the subsequent retention of the copy for future data mining would not be a seizure.

¶58 The same kind of analysis would possibly apply to the use of the other technologies described in this Part when the police seal what they collect. If they directly collect a suspect's WiFi traffic, interrogate his PDA via Bluetooth, or set up packet sniffers to capture his network traffic, but seal what they collect, courts reasonably could hold that the Fourth Amendment simply does not apply. The police have not obtained anything tangible, so they have not performed a seizure, and they have locked things away, so they have not performed a search. In the meantime, our ability to protect our intangible information from the scrutiny of the police will have diminished significantly.

IV. TWENTY-FIRST CENTURY SEIZURE

¶59 In *Hicks*, the Court was wrong about seizure, and the cases which follow its dictum have incorrectly concluded that the Seizure Clause does not apply to copies of intangible data. The test from *Hicks*—meaningful interference with a possessory interest—should be replaced or expanded to encompass other Fourth Amendment interests. There are two possible doctrinal approaches for expanding the rule, each of which leads to a slightly different articulation of the new test but to similar ends. Although these two tests would bring within the Fourth Amendment many activities that might not be considered seizures under the *Hicks/Jacobsen* test, each would still be subject to the many exceptions to the Fourth Amendment's warrant requirement.[100] For this reason, as I will discuss below, application of the new test is not likely to change the outcome of many prior cases, although it may have a profound effect on future police practices.

A. Dominion and Control

¶60 Meaningful interference with a possessory interest should be seen as sufficient but not necessary for seizure. In fact, *Jacobsen* itself articulated another definition of seizure: dominion and control by the police of property.[101] While the meaningful interference conception of seizure focuses on the deprivation to the property owner, the dominion and control class focuses on the usurpation by the state of the property.[102] With physical property, these competing emphases are two sides of the same coin: by exerting dominion and control, the police meaningfully interfere with the owner's possessory interest. This is not so with nonrivalrous property, over which the police can exert dominion and

---

[96] Jeffrey W. Seifert, Cong. Research Serv., Data Mining and Homeland Security: An Overview 1 (2007), *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf.

[97] *Id.* at 5.

[98] *See, e.g.*, Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 773 (2006) (quoting Bruce Schneier as saying that there are "trillions of connections between people and events — things that the data mining system will have to 'look at'—and very few plots. This rarity makes even accurate identification systems useless.").

[99] *Id.* at 774; *see also* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 378 (2006).

[100] *See* California v. Acevedo, 500 U.S. 565, 584 (Scalia, J., concurring) (listing exceptions to the warrant requirement).

[101] United States v. Jacobsen, 466 U.S. 109, 120 n.18 (1984) ("[T]he decision by governmental authorities to exert dominion and control over the package for their own purposes clearly constituted a 'seizure,' though not necessarily an unreasonable one.").

[102] *See* United States v. Karo, 468 U.S. 705, 730 (1984) (Stevens, J., concurring in part and dissenting in part) (finding a seizure by government agents who "usurped a part of a citizen's property," thereby asserting dominion and control).

control with no interference to traditional possessory interests. Since *Jacobsen*, Justice Stevens, in particular, has tried to remind the Court on several occasions of the dominion and control prong.[103] As has been described throughout this Article, the police can exercise dominion and control without treading at all on the traditional rights of possession in intangible property. To state it more specifically, the seizure of intangible property occurs whenever the police take dominion and control over intangible property.

B. Intangible "Dispossession" and the Right to Delete[104]

¶61 Another way to encompass the proper view of the seizure of intangible property which preserves the formulation but not the meaning of the *Jacobsen* test is to recast the "meaningful interference with a possessory interest" phrase in light of what "dispossession" means with intangible property. To do so, 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 obsolete and unhelpful.

¶62 To restate this as a test, does the government's copying of intangible property produce negative effects on par with the effects of physical dispossession? For example, 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. By analogy, does the government's copy of some intangible property prevent the owner from altering, destroying, or otherwise changing the state of his property?

¶63 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.[105] This right is tied to the rights of dominion and control. Although the right to destroy may seem culturally or economically unsavory, it is protected because without the extreme ability to change, delete, or destroy, virtually nothing will be left of the rights of dominion and control.[106]

¶64 Furthermore, the 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.

---

[103] In *Karo*, Justice Stevens, writing for three justices in partial dissent, said:

> [B]y attaching a monitoring device to respondents' property, the agents usurped a part of a citizen's property-in this case a part of respondents' exclusionary rights in their tangible personal property. By attaching the beeper and using the container to conceal it, the Government in the most fundamental sense was asserting "dominion and control" over the property-the power to use the property for its own purposes. And "assert[ing] dominion and control" is a "seizure" in the most basic sense of the term.

Id. (quoting *Jacobsen*, 466 U.S. at 120); *see also* Hudson v. Palmer, 468 U.S. 517, 544 (1984) (Stevens, J., concurring in part and dissenting in part) ("There can be no doubt that the complaint adequately alleges a 'seizure' within the meaning of the Fourth Amendment. Palmer was completely deprived of his possessory interests in his property; by taking and destroying it, Hudson was asserting 'dominion and control' over it; hence his conduct 'did constitute a seizure' . . . ") (quoting *Jacobsen*, 466 U.S. at 120); Segura v. United States, 468 U.S. 796, 822-23 (1984) (Stevens, J., dissenting) ("There can be no doubt here that petitioners' possessory interests . . . were subject to meaningful governmental interference. The agents not only excluded petitioners from access to their own apartment . . . but they also exercised complete dominion and control over the apartment and its contents.").

[104] Parts of this Subpart are adapted from an essay I authored, where I began to develop this idea. *See* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2006).

[105] Lior Jacob Strahilevitz, *The Right To Destroy*, 114 YALE L.J. 781, 794 (2005).

[106] *See id.* at 794-95 (describing the right to destroy as an extreme version of the rights to exclude, use, and control subsequent alienation).

¶65 A 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.[107] It also explains pre-*Hicks* cases which had found copying intangible information to be seizure.[108]

¶66 An echo of this test was heard in *Karo*, albeit in a dissenting opinion. Justice Stevens, with Justices Brennan and Marshall, would have held that attaching an electronic tracking device to defendant's property *was* a seizure.[109] In support of this conclusion, Justice Stevens argued for a broader understanding of "meaningful interference":

> The owner of property, of course, has a right to exclude from it all the world, including the Government, and a concomitant right to use it exclusively for his own purposes. When the Government attaches an electronic monitoring device to that property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use. Surely such an invasion is an "interference" with possessory rights; the right to exclude, which attached as soon as the can respondents purchased was delivered, had been infringed. That interference is also "meaningful"; the character of the property is profoundly different when infected with an electronic bug than when it is entirely germ free.[110]

¶67 A similar reasoning underlies the constitutional right to delete.[111] When the police use a packet sniffer, use a hard-drive imager, or keep data subject to withdrawn consent, 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.

C. Intangible Seizure in Practice: The Many Exceptions to the Warrant Requirement

¶68 If either of these proposed tests were adopted, it would upset the logic of hundreds of prior cases. Nevertheless, it probably would change the holding of very few, if any of them. Seizure is only unconstitutional under the Fourth Amendment if unreasonable.[112] Two exceptions, in particular, allow warrantless seizure in a much broader range of cases than is allowed for search: the plain view and the probable cause/"operational necessities" exceptions.

---

[107] *See* Ayeni v. Mottola, 35 F.3d 680, 688 (2d Cir. 1994), *abrogated on other grounds by* Wilson v. Layne, 526 U.S. 603 (1999).

[108] *See* Part II.B; LeClair v. Hart, 800 F.2d 692, 695-96 (7th Cir. 1986) ("Even if the Court can be said to have somehow linked seizures to property interests, it is well established that '[t]he right to exclude others is generally "one of the most essential sticks in the bundle of rights that are commonly characterized as property."'" (quoting Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1011 (1984) (quoting Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979)))).

[109] United States v. Karo, 468 U.S. 705, 729 (1984) (Stevens, J., dissenting)

[110] *Id.* (footnote omitted).

[111] Recently, the Fourth Circuit sounded a similar theme in a case involving a section 1983 suit against the City of Charlottesville alleging that the city had published a map showing a public trail running across the plaintiff's yard, causing a Fourth Amendment seizure of her property. Presley v. City of Charlottesville, 464 F.3d 480 (4th Cir. 2006). The Fourth Circuit reversed the district court's dismissal of the action, concluding that she properly stated a Fourth Amendment claim of seizure. In explaining its reasoning, the court said:

> Presley has alleged an "interference with" her "possessory interests" that is clearly "meaningful"; indeed, this interference has assertedly been disruptive, stressful, and invasive. Her complaint states that she has been deprived of the use of part of her property due to the regular presence of a veritable army of trespassers who freely and regularly traverse her yard, littering, making noise, damaging her land, and occasionally even camping overnight. This constant physical occupation certainly constitutes a "meaningful interference" with Presley's "possessory interests" in her property.

Id. at 487.

[112] *See, e.g.*, Soldal v. Cook County, 506 U.S. 56, 61-62 (1992) ("Whether the Amendment was in fact violated is, of course, a different question that requires determining if the seizure was reasonable.").

¶69 Under the plain view exception, the police may seize anything in plain view if the item's "incriminating character" is "immediately apparent," and if the police are lawfully present at the place from which the item is viewed.[113] This exception would likely apply often to the seizure of intangible property. For example, photographing the scene of the execution of a search warrant may be permissible as a plain view seizure. The orthodox plain view rule permits the seizure of things that are obviously evidence of a crime,[114] but the police are given latitude to seize more if "operational necessities" require.[115] Courts are likely to hold that seizure-by-photography meets such operational necessities, for example as a reasonable safeguard taken to protect the police against future claims of impropriety.[116]

¶70 Another, related exception allows the police to seize containers temporarily without a warrant if the police have probable cause to believe they contain evidence of a crime. The Supreme Court summarized the rule in *United States v. Place* as follows:

> Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.[117]

¶71 Several cases have applied this rule in the context of things like computers which contain intangible information.[118] Nothing in the reasoning of these cases suggests the rule should not apply to intangible information, considered separately from the physical container which contains it.

D. What a Difference a Verb Makes

¶72 I am not proposing a unified theory of the Fourth Amendment, in part because I am unconvinced that such a thing can ever be found.[119] I am suggesting, however, that we pay too much attention to one verb—search—in the Amendment and too little on the other verb—seizure. Search literally connotes the exploration for things, while seizure connotes dominion over a thing. That the founders listed both verbs in the Bill of Rights suggests it was too difficult to reduce the evil that they sought to avoid (or in reverse, the freedom that they sought to preserve) to one verb. Modern constitutional theorists have forgotten this, trying to cram ill-fitting analyses into search and the reasonable expectation of privacy test, even when the match is poor.

---

[113] Coolidge v. New Hampshire, 403 U.S. 443, 465-66 (1971). "It is well established that under certain circumstances the police may seize evidence in plain view without a warrant." *Id.* at 465.

[114] *Id.*

[115] Arizona v. Hicks, 480 U.S. 321, 327 (1987).

[116] *Cf.* Illinois v. Lafayette, 462 U.S. 640, 646 (1980) (holding that police may perform an inventory search upon booking of arrestee to help monitor against theft, defend against false claims of theft, protect the arrestees and the police, and verify the arrestee's identity).

[117] United States v. Place, 462 U.S. 696, 701 (1983).

[118] The Department of Justice's manual on searching and seizing computers summarizes the doctrine as it applies specifically to computers as follows:

> 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). The Fourth Amendment permits agents to seize a computer temporarily so long as they have probable cause to believe that it contains evidence of a crime, the agents seek a warrant expeditiously, and the duration of the warrantless seizure is not "unreasonable" given the totality of the circumstances. See United States v. Place, 462 U.S. 696, 701 (1983); United States v. Martin, 157 F.3d 46, 54 (2d Cir. 1998); United States v. Licata, 761 F.2d 537, 540-42 (9th Cir. 1985).

DOJ Search and Seizure Manual, *supra* note 94.

[119] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. (forthcoming 2007) (manuscript at 4, *available at* http://ssrn.com/abstract=976296) (explaining "why the Supreme Court has not and cannot adopt a single test for what makes an expectation of privacy 'reasonable'"). *But see* Morgan Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 556 (1996) (suggesting to integrate a single "vibrant and effective theory of the Fourth Amendment").

¶73 Being armed with a second verb allows us to clear away a few vexing constitutional puzzles, little conundrums that are discussed by others to demonstrate how imperfect and complex the reasonable expectation test can be. In fact, off-loading some of these hard cases onto seizure may even help rehabilitate the reputation of the reasonable expectation of privacy test, by bringing within the Fourth Amendment some police activities that are hard to analyze as a search.

¶74 Most of these examples revolve around the seize-now, search-later paradigm described in Part II. For example, consider again the NSA wiretapping program. The NSA is probably storing thousands of e-mail messages and voice conversations for later analysis. Imagine, counter-factually, that the NSA seals every communication immediately after collection and seeks judicial approval to open the seal every time they have probable cause about a particular message or particular speaker. How would this program fare under constitutional scrutiny, at least under the Fourth Amendment standards for criminal investigations?[120] Under the reasonable expectation of privacy test, the initial collection and storage may not be a search, but under *Berger* and *Katz* and the tests I have presented earlier in this section—dominion and control and an invasion of the right to delete—this collection is a seizure, and post-hoc judicial authorization cannot cure the Fourth Amendment violation.

¶75 Consider a more difficult example, government data mining. It is conceivable that an aggressive Department of Justice would conclude that data mining implicates the Fourth Amendment only if the amount of information it "exposes" to the analyst is above some threshold of specificity. Any less specificity, DOJ might argue, and the "reasonable expectation of privacy" has not been implicated. For example, the data mining algorithm could spit out a yes/no response: "no" means the algorithm found nothing suspicious, and "yes" means that some target matched the terrorist profile. With a yes, the analyst will seek a warrant, and with a no, the analyst will move on to the next test, but under neither circumstance will an expectation of privacy have been breached. This is the type of hard question the reasonable expectation of privacy test so often raises.

¶76 But the intangible seizure test will focus on an earlier event, the collection of the data itself. Under what circumstances were the databases compiled? Did they involve the government's warrantless, suspicion-less assertion of dominion and control over a private party's data? Did they involve the government's direct collection of communications or transactional information from a network? If so, the Fourth Amendment violation accrues in the collection, even before there is any use.

¶77 Consider one final example. Orin Kerr has speculated that courts might hold that making a mirror image of a hard drive is not a search.[121] He worries that during the time after an image is made and before it is analyzed, or "exposed," the Fourth Amendment does not apply, citing *Arizona v. Hicks*.[122]

¶78 Under the doctrine of intangible seizure presented in this Part, there is little doubt that making a hard drive image is a seizure. It involves the government's dominion and control over massive amounts of property, most of which is irrelevant to the government agent's suspicion. Furthermore, by making an image, the government deprives the hard drive's owner of the right to delete. The content on the hard drive is frozen in time when the image is made. The owner of the content has no future opportunity to explain, contextualize, delete, or complete the information on the government's image. Thus, the image of a hard drive is a government seizure that must be justified by a warrant or under some exception to the Fourth Amendment's warrant requirement.

---

[120] The program may be constitutional under a "national security" exception to the Fourth Amendment. The Supreme Court has left open the question of whether such an exception exists for foreign intelligence surveillance. United States v. U.S. District Court, 407 U.S. 297, 308 (1972) ("[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country.").

[121] Kerr, *supra* note 87, at 560.

[122] *Id.* at 558.

V. DOES THE FOURTH AMENDMENT PROTECT PRIVACY, PROPERTY, LIBERTY, OR SECURITY?

¶79 The Fourth Amendment protects privacy, we are often reminded. At least since *Boyd*, judges and scholars have contested this claim, arguing that the Fourth Amendment is better seen as a protector of some other value, perhaps property,[123] liberty,[124] or security.[125] Theorists who choose only one of these three are accused of advancing an unhelpful "unitary" approach to the Amendment.[126] Many have argued that the Fourth Amendment protects more than one of these values.[127]

¶80 I side with those who embrace a multi-dimensional Fourth Amendment. Cases like *Olmstead* remind us why the Fourth Amendment protects more than just property interests, while cases like *Hicks* and its progeny suggest that it is not enough to rely on privacy alone. Not only does a single-minded attention to privacy tend to under-protect our interests in intangible property, it may also be to blame for the confusion and uncertainty surrounding the reasonable expectation of privacy test. Perhaps the time has come to acknowledge that the Fourth Amendment, the product of a number of various values and concerns, is ill-served by focusing on only one of privacy, property, liberty, or security.

¶81 The question, of course, is how should one select between the menu of possible value choices, and more specifically, how should courts be guided in applying the Amendment? If the Fourth Amendment was really intended to champion so many disparate values, what mode of constitutional interpretation should guide courts in deciding how to resolve any particular controversy? In my future work, I plan to more comprehensively tackle this question, but at present, I aim for a more modest contribution.

¶82 Just as it is unhelpful to try to single out one value as the driving force behind Fourth Amendment protection, it is also unhelpful to find particular unitary values underlying any one of the three separate protections in the Amendment: freedom from unreasonable search, seizure of the person, and seizure of property.[128] *Katz* and its progeny have for the most part avoided the unitary value trap, finding both privacy and property conceptions of the Fourth Amendment within the definition of search, but the cases construing seizure of property are mired in property rhetoric and rationale. This is a mistake.

¶83 The seizure of personal property has been the neglected step-child of Supreme Court Fourth Amendment jurisprudence.[129] Physical property seizure often coincides with search[130] or with the seizure of a person,[131] and the Court has relied on the constitutional regulation of those other types of acts to protect against the most egregious examples of personal property seizure.

---

[123] Soldal v. Cook County, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the [Fourth] Amendment protects property as well as privacy."); Kerr, *supra* note 17 at 807.

[124] Heffernan, *supra* note 73, at 648; William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1060-1068.

[125] Thomas K. Clancy, *What does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307 (1998).

[126] Heffernan, *supra* note 73, at 648 ("[O]ne must conclude that an interest in privacy-as-personal-solitude is at most an occasional adjunct to the interest central to all seizures of the person--the interest in physical liberty. This point alone makes Posner's unitary analysis of the Fourth Amendment unacceptable." (footnote omitted)).

[127] Boyd v. United States, 116 U.S. 616, 630 (1886) ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense . . . ."); Heffernan, *supra* note 73, at 654 ("Soldal posits three independently cognizable interests protected by the Fourth Amendment--privacy, liberty and property.").

[128] The seizure of the person is often associated with liberty. *See* Tennessee v. Garner, 471 U.S. 1, 7 (1985) ("Whenever an officer restrains the freedom of a person to walk away, he has seized that person.").

[129] *See* U.S. v. Jacobsen, 466 U.S. 109, 114 n.5 (1984) ("[T]he concept of a 'seizure' of property [as opposed to the seizure of a person] is not much discussed in our cases . . . .").

[130] *See* Arizona v. Hicks, 480 U.S. 321 (1987).

[131] *See* United States v. Chadwick, 433 U.S. 1, 15 (1977).

¶84 Property seizure should also be seen as a government act which implicates privacy—not just property. This was the obvious message of *Berger* and *Katz*. Sometimes the government intrudes on Fourth Amendment-protected privacy by collecting and retaining information about us, regardless of whether it views or uses the information. In those circumstances, relying on search and the reasonable expectation of privacy test is a frustrating, unpredictable endeavor. Faced with this challenge, courts are likely to elevate form over substance by rewarding law enforcement gamesmanship.

¶85 It is strange that although *Katz* meant to bring privacy and property together as cohabitant values in the Fourth Amendment, courts still separate the two from one another in seizure cases. Even Justice Stevens, who was lauded in the last Part for attempting to revive the "dominion and control" test, has made this mistake. In a concurring opinion, he said:

> Although our Fourth Amendment cases sometimes refer indiscriminately to searches and seizures, there are important differences between the two that are relevant to the plain view doctrine. The Amendment protects two different interests of the citizen-the interest in retaining possession of property and the interest in maintaining personal privacy. A seizure threatens the former, a search the latter.[132]

¶86 Quotes like this replicate the *Olmsteadian* mistake. Technology has a tendency to complexify the relationship between two important Fourth Amendment values—privacy and property. At the time of the Founding, the two were basically coextensive: protecting property meant protecting privacy and vice versa.[133] William Heffernan has remarked:

> To Camden (Entick's author) and to the framers of the Fourth Amendment, informational privacy was indeed a matter of embeddedness--that is, to eighteenth-century minds, one enjoyed privacy by exerting control over tangible objects such as one's house or one's papers. The words of the Fourth Amendment reflect this understanding. They refer only to tangible objects--persons, houses, papers, and effects--that to eighteenth-as well as twentieth-century minds have a central bearing on a person's existence as a distinct individual.[134]

The Court in *Olmstead* faced a changing world of technology where privacy could be breached without treading on property, and its formalistic opinion failed to recognize that the Founders wrote a constitutional provision meant to protect both. In *Katz*, the Court remedied this misconstruction, by acknowledging that the two values go hand in hand, and it tried to apply this corrective to both constitutional verbs, search and seizure.

¶87 Somewhere along the way, the project of *Katz* stalled, and cases like *Jacobsen* and *Hicks* loaded all of the constitutional focus on one verb—search—while diminishing the dual protection of property

---

[132] Texas v. Brown, 460 U.S. 730, 747 (1983) (Stevens, J., concurring).

[133] William Heffernan traces the relationship between property and privacy back to Lord Camden's discussion in *Entick v. Harrington*. Heffernan, *supra* note 73, at 633-34 (quoting 19 Howell's State Trials 1029 (1765)). Lord Camden declared that "though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass . . . ." *Id.* (quoting 19 Howell's State Trials at 1066).

[134] *Id.* at 644. In a similar vein, Sherry Colb has said:

> In the late eighteenth century, someone who cared deeply about privacy could secure its effective protection by writing an amendment that guaranteed the people a robust right of security in their houses, papers, and effects. Such an amendment would automatically cover privacy interests as well. In a world where privacy and property were so intimately linked, it would have seemed unnecessary to craft a separate protection for privacy per se, particularly when the Fourth Amendment includes a right of security in one's "person"--an extension beyond contemporary notions of property that might have seemed adequate to cover any unusual invasions of privacy that failed to trespass upon real property or personal effects. The right to be secure against unreasonable searches and seizures, in historical context, thus necessarily encompassed privacy.
>
> As the world changed, however, and invasions of privacy without invasions of property became possible and increasingly likely, Fourth Amendment doctrine had to adapt.

Sherry F. Colb, *A World Without Privacy: Why Property Does not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 MICH. L. REV. 889, 895 (2004).

and privacy found in the other verb—seizure. For two decades, this move has been given scant attention, because every seizure was also a search.

¶88 But technology is complexifying things again. The value of collecting without analysis has increased with reduced costs of storage and computation. "Save now, analyze later," is a powerful tool in the investigators arsenal. Viewed only as a violation of property rights, this is a contingent, complex debate that turns on ideas about the right to delete[135] and incomplete analogies to intellectual property. But once the reinvigorated Seizure Clause is understood to protect privacy as well as property, the constitutional doctrine can be brought in line with the technological reality.

¶89 There are other constitutional values to be found in the reinvigorated Seizure Clause. As discussed above, the Fourth Amendment isn't about only privacy and property. Seizure of intangible property also implicates *security* interests, meaning the Fourth Amendment's promise that we will be secure from government coercion and unreasonable exercises of power.[136] In particular, by returning to the "dominion and control" conception of seizure, we shift the emphasis away from both privacy and property and focus instead on the government's exercise of control over a copy of our property.

VI. CONCLUSION

¶90 We are reminded that whenever a court focuses too much on any one Fourth Amendment value, they usually end up drawing conclusions that they some day retract. In *Olmstead*, the mistake was to privilege property over privacy. With intangible property, an overattention on property will likely lead us to miss damaging effects on other interests like liberty and privacy. In every Fourth Amendment context, courts and scholars should pause when privileging one interest and excluding others. Undoubtedly, this is not the last time new technology will upset our past understandings. The next time this happens, courts will be well-advised to remember that *Katz* was about freeing the analysis from formalistic understandings of exactly what the Fourth Amendment protects.

---

[135] Ohm, *supra* note 104.

[136] "The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV. (emphasis added); *see also* Clancy, *supra* note 125.