A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY

WHITE PAPER SERIES

Administering the Fourth Amendment in the Digital Age

JIM HARPER

NATIONAL CONSTITUTION CENTER

Administering the Fourth Amendment in the Digital Age

By Jim Harper*

Stare decisis is the valued judicial practice of extracting the underlying principle from precedent, the *ratio decidendi*, and applying it to present cases.[1] But what happens to the principle behind a prescient dissent—the *ratio dissensi*, if you will—when a majority's decision later proves wrong? Almost ninety years ago, an understated Supreme Court Justice left crumbs of insight in a dissent that may help solve the riddle of applying the Fourth Amendment, particularly to modern communications and data.[2] His thinking can help construct a more complete, reliable, and truly juridical method for administering the Fourth Amendment. Advocates and courts should look to his prescient *ratio dissensi*.

Pity Justice Butler. Next to contemporaries such as Oliver Wendell Holmes, Jr., Louis D. Brandeis, and Benjamin Cardozo, Pierce Butler occupies second-tier status in history's assessment of Supreme Court justices. A conservative Democrat put forward by a Republican president, Butler was a controversial nominee for the Court. One of his Minnesota home-state senators opposed him, as did progressive lion Robert LaFollette, Sr., a Republican from Wisconsin. The opposite end of the ideological spectrum did Butler no favors: the Ku Klux Klan opposed his nomination because he was a Catholic.

Justice Butler wrote more than 300 opinions in his sixteen years of Supreme Court service, but few stand out today. He is best remembered as one of the "four horsemen" who lost their constitutional stand against President Franklin Delano Roosevelt's expansive "New Deal" programs.[3] But time has vindicated some of Justice Butler's work on the Court, including notable dissents.

Butler alone rejected Oliver Wendell Holmes, Jr.'s now notorious reasoning in *Buck v. Bell*,[4] for example. Allowing forced sterilization of a woman, Holmes wrote coldly for the majority: "Three generations of imbeciles are enough."[5] The Nazis' use of eugenics the next decade cast more than a little pall over the practice, and *Skinner v. Oklahoma* effectively ended forced sterilization in 1942.[6] Score one for the conscience of Justice Butler.

---

* Vice President, The Competitive Enterprise Institute.

[1] Payne v. Tennessee, 501 U.S. 808, 827 (1991) (lauding *stare decisis* because it "promotes the evenhanded, predictable, and consistent development of legal principles, fosters reliance on judicial decisions, and contributes to the actual and perceived integrity of the judicial process.").

[2] Note: *Digital Duplications and the Fourth Amendment*, 129 HARV. L. REV. 1046 (2016) ("It goes without saying that the drafters of the Fourth Amendment did not contemplate its application to the digital era.").

[3] *See* William G. Ross, *The Hughes Court (1930-1941): Evolution and Revolution*, *in* THE UNITED STATES SUPREME COURT: THE PURSUIT OF JUSTICE 246 (Christopher L. Tomlins ed., 2005).

[4] 274 U.S. 200 (1927).

[5] *Id*. at 207.

[6] 316 U.S. 535 (1942).

Likewise, in *Palko v. Connecticut*,[7] Butler alone disagreed with Justice Cardozo's ruling that the Constitution's protection against double jeopardy did not apply to the states. The Court reversed itself on this question three decades later.[8] Score another.

Butler was a legal technician, and his areas of focus were not what generally capture public and scholarly attention. His approach to opinion writing "stressed simplicity and minimalism," according to a history by David R. Stras, now a Minnesota Supreme Court justice himself, "and it was rare indeed when he used rhetorical flourishes to argue a point."[9] So it is not surprising that Justice Butler's dissent in *Olmstead v. United States*[10] has remained obscure behind the fanfare of his brother Louis Brandeis's dissent. But time may yet vindicate Justice Butler's reasoning, especially given its usefulness for applying the Fourth Amendment to the digital world.

Olmstead, of course, was the 1928 case in which the Court found that a Fourth Amendment search had not occurred when government agents wiretapped the telephones of suspected bootleggers. Justice Brandeis, co-author of a *Harvard Law Review* article called "The Right to Privacy" forty years earlier,[11] inveighed against the ruling using powerful and persuasive language. "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness," he wrote:

> They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[12]

Posterity has favored Brandeis's passion. Commentators and scholars today still quote and muse over his formulation of "the right to be let alone."[13] They explore how that notion might be implemented to preserve the values that the Framers held dear.

But Brandeis's words did not found a sustaining rationale for Fourth Amendment protection. The proof is in the eating of the pudding: Modern Fourth Amendment jurisprudence is a muddle, and it is sorely challenged by advances in information technology. This is particularly poignant because Brandeis foresaw the surveillance

---

[7] 302 U.S. 319 (1937).
[8] Benton v. Maryland, 395 U.S. 784 (1969).
[9] David R. Stras, *Pierce Butler: A Supreme Technician*, 62 VAND. L. REV. 695 (March 2009).
[10] 277 U.S. 438 (1928).
[11] Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[12] *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).
[13] *See, e.g.*, M.G. Michael and Katina Michael, *Privacy—"The Times They Are A-Changin,"* IEEE TECH. AND SOC'Y MAG. 31.4 (2012): 20-21; J. Lyn Entrikin, *The Right to be Let Alone: The Kansas Right of Privacy*, UALR Bowen School Research Paper No. 12-05 (Feb. 19, 2013); Justin Conforti, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, And The Ninth Circuit's Misapplication Of The* Ortega *Test In* Quon v. Arch Wireless, 5 SETON HALL CIR. REV. 7 (2012); Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles over the Right to Be Let Alone Online*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 229 (2011-2012).

capabilities enabled by today's information and communications technologies. "Ways may someday be developed," he wrote, "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."[14]

The case that reversed *Olmstead*, of course, was *Katz v. United States*.[15] In *Katz*, thirty-nine years later, Justice Harlan shared his sense of how the Constitution controls government access to private communications in his solo concurrence: "My understanding," he wrote, "is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[16]

Since then, courts have analyzed whether defendants have had a "reasonable expectation of privacy" in information or things. Under Justice Harlan's concurrence, if not the *Katz* majority's rationale, the defeat of a "reasonable expectation of privacy" signals a constitutional search generally requiring a warrant.[17]

That doctrine has not worked. Courts rarely follow the full analysis Justice Harlan's formulation suggests. They rarely inquire into a defendant's "actual (subjective) expectation of privacy," for example, or how it was "exhibited."[18] The second half of the test requires judges to use their own views on privacy as a proxy for objectivity, though they are neither public opinion researchers nor sociologists. Against litigants importuning about privacy, courts after *Katz* have found as often as not that the Fourth Amendment does not protect the security of sensitive and revealing information.

In *Smith v. Maryland*,[19] for example, one of the leading communications privacy cases, the Supreme Court found that placement of a pen register[20] on a suspect's phone line without a warrant did not violate the Fourth Amendment.[21] "[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial," Justice Blackmun wrote.[22] Walking through the influences that would suppress expectations of privacy in phone-dialing, and none that would support it,[23] he said, "[I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[24]

---

[14] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).
[15] 389 U.S. 347 (1967).
[16] *Id*. at 361.
[17] On the warrant requirement, the Court has said, "It is a cardinal rule that . . . law enforcement . . . use search warrants wherever reasonably practicable." Chimel v. California, 395 U.S. 752, 758 (1969) (quoting Trupiano v. United States, 334 U.S. 699, 705 (1948)).
[18] *See* Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015).
[19] 442 U.S. 735 (1979).
[20] *See id.* at 736 n.1 (explaining that a pen register records the telephone numbers one dials but does not transmit conversation).
[21] *Id*. at 736.
[22] *Id.*
[23] *See id.*
[24] *Id*. at 743.

A Court without Justice Brandeis's passion for privacy is evidently quite free to undercut it. So in *United States v. Karo*,[25] government agents had arranged with an informant to surreptitiously install a radio beeper in a container. They used the presence of the beeper in the container over a period of several days to locate it at three different residences and in the driveway of a fourth, to locate the container in a pair of self-service storage facilities, and also to locate it in transit—all the while unable to suffer the inconvenience of getting a warrant.[26] The Court did not examine whether all this warrantless beeper-tracking was reasonable. It gave the once-over to Karo's expectation of privacy and found his (presumed) feelings unreasonable.[27]

More recently, the "reasonable expectation of privacy" test produced a ruling that government agents' examination of a stopped vehicle with a drug-sniffing dog is not a Fourth Amendment search.[28] It is hard to think of a word better than "search" for such highly focused analysis of whether certain particulates exist in the air. Some cases certainly have maintained the protection the people have from inquisitive government agents, but the "right to be let alone" has not fared all that well when privacy and expectations thereof have been the locus of the Court's decision-making.

If Justice Brandeis's passion did not lay the groundwork for sound administration of a strong Fourth Amendment right, perhaps Justice Butler's *Olmstead* dissent could. His challenge to the majority decision eschewed feelings, instead examining the legal status of telephone conversations:

> The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission, the exclusive use of the wire belongs to the persons served by it. Wiretapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence.[29]

The communications belong to the parties between whom they pass.[30] It is a fascinating—and very different—way of thinking about what happened in *Olmstead*. Justice Butler would have protected Olmstead's calls from warrantless wiretapping not because it is part of human essence to have communications remain private, as Justice Brandeis said, but because people's conversations are not the government's to listen to.

---

[25] 468 U.S. 705 (1984).
[26] *Id*. at 708-709.
[27] *Id*. at 713.
[28] Illinois v. Caballes, 543 U.S. 405 (2005).
[29] *Olmstead*, 277 U.S. at 487 (Butler, J., dissenting).
[30] *See* Susan W. Brenner & Barbara A. Frederikson, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 111 (2002) ("[I]nformation contained in computer files clearly belongs to the owner of the files. The ownership of information is similar to the contents of private conversation in which the information belongs to the parties to the conversation.").

Justice Butler's formulation holds the seeds of an alternative way to administer the Fourth Amendment. It is technical and value-free, but it offers the hope of better Fourth Amendment administration because it is more susceptible to sound application than current Fourth Amendment doctrine. Its use would provide consistent and reliable protection for Americans' liberties and a stable rule for law enforcement in a time of technological change.

Courts in Fourth Amendment cases should decline to invoke doctrine that requires them to make broad social pronouncements. Rather, they should apply the text of the Amendment and general legal principles as literally as possible to the facts of cases. That is not always easy, and it requires new and deeper analysis of what it means to "search" and to "seize." It also requires fuller awareness of property and contract rights as they apply to communications and data. But it is a more methodical judicial exercise than applying "reasonable expectations" doctrine, and it would achieve the current Court's goal of preserving "that degree of privacy against government that existed when the Fourth Amendment was adopted."[31] Applying the law to the facts is the better way to administer the Fourth Amendment.

Administering the Fourth Amendment

The first phrase of the Fourth Amendment says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[32] Absent doctrine, courts would analyze its elements as follows:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?

If there was a search or seizure, if it was of protected things, and if it was unreasonable, then the right has been violated. That is how to administer the Fourth Amendment.

Though the Supreme Court is not plain about it, it uses this simple construct for analyzing easy Fourth Amendment cases.[33] In harder cases, such as when communications and data are involved, the concepts of "search" and "seizure" seem harder to apply, and the Court retreats to confusing and malleable "reasonable expectations" doctrine.

---

[31] Kyllo v. United States, 533 U.S. 27, 34 (2001); United States v. Jones, 565 U.S. ___, 950 (2011); *Id*. at 958 (Alito J., concurring in the judgment).

[32] U.S. CONST. amend. IV. There is a second phase to the Fourth Amendment, of course. We focus here on the existence of searching and seizing and their reasonableness when they exist, putting aside questions around the warrant requirement.

[33] *See infra*, notes 44-51.

But the standard—simplistic—mode of interpretation noted above can be used in all Fourth Amendment cases, including those dealing with communications and digital materials. There are direct parallels between protected communications technologies used at the time of the Framing and today's. Applying the words of the Fourth Amendment, background legal principles, and an understanding of technology, it is possible to administer the Fourth Amendment in all cases without artifice.

The exercise begins with identifying seizures—which are government invasions of any property right—and searches—focused sensing that is often signaled by efforts to bring exposure to concealed things. Discerning seizures and searches requires some careful thinking and a modicum of technical knowledge because current doctrine has obscured the concepts and the technological environment is changing. But courts can and should determine in all cases if government agents have seized or searched items protected by the Fourth Amendment, and if they have done so unreasonably.

Seizures and Searches in *Riley*

The Supreme Court's recent decision in *Riley v. California*[34] can model the exercise of spotting seizures and searches, including with respect to digital devices and data. David Riley's encounter with the San Diego police included a large number of seizures and searches: of Riley, Riley's car, his phone, and his data. The legal bases for these seizures and searches shifted, grew, and ultimately found their limit.

The case began on August 22, 2009, when Officer Charles Dunnigan observed Riley driving an Oldsmobile with expired registration tags. Dunnigan pulled Riley over, seizing him and his car.[35] Officer Dunnigan was allowed to do this given his reasonable suspicion that an infraction had occurred.[36] Upon learning that Riley was driving with a suspended driver's license, Officer Dunnigan removed him from the car, continuing the original seizure of Riley with an additional legal basis for doing so: reasonable suspicion of another violation.

Officer Dunnigan was then joined by an Officer Ruggiero, who prepared the car for impoundment consistent with a policy that prevents suspended drivers from returning to, and continuing to operate, their vehicles. No longer seized for the purpose of a brief investigation, the car was now seized in order to prevent additional driving infractions.

Officer Ruggiero began an "impound inventory search" of the car, a procedure the Supreme Court approved as reasonable in *South Dakota v. Opperman*.[37] To be precise, an inventory search of a car is executed through a series of small seizures in addition to, and conceptually distinct from, the seizure of the car as a whole. Officer Ruggiero exercised further dominion over the car by opening the hood, for example, the trunk, and other

[34] 134 S. Ct. 2473 (2014).
[35] Brendlin v. California, 551 U.S. 249, 254-263 (2007).
[36] Terry v. Ohio, 392 U.S. 1, 20-27 (1968).
[37] 428 U.S. 364, 376 (1976).

compartments. Though they were not his, he no doubt took control of items in the car (seized them) by picking them up or moving them to facilitate the inventory.

Officer Ruggiero's search turned up guns in the engine compartment of the car. This gave Officer Dunnigan probable cause to believe Riley had committed another, more serious crime. He placed Riley under arrest, continuing the ongoing seizure of Riley's body under new legal authority.

In the course of placing Riley under arrest, Officer Dunnigan also searched his person, undoubtedly doing so by placing his hands on Riley. The difference between the felt contours of Riley's body and other things under his clothes would reveal weapons or other items that could endanger Officer Dunnigan, as well as evidence Riley might dispose of. This search was distinct from the ongoing seizure of Riley, and its legal basis was different, too. *Chimel v. California* permits searches incident to arrest to aid in the discovery of weapons or of evidence that suspects might destroy.[38]

Consistent with standard practice for a "booking search," which is yet another legal basis for both searching suspects and seizing their property,[39] Officer Dunnigan examined Riley's person and seized his possessions, including his cell phone, so he could safely transport and house his arrestee.

The lower court's description of events is not detailed, but at some point in the process, Officer Dunnigan "looked at Riley's cell phone," and "he noticed all of the entries starting with the letter 'K' were preceded by the letter 'C'," [40] an indication of affiliation with the "Bloods" gang, whose members self-characterize as "Crip Killas." It is possible that these entries were in plain view, displayed by the otherwise untouched phone as Officer Dunnigan seized it. The likelihood is that Dunnigan caused the entries to be displayed by manipulating the phone. This was an additional series of seizures in the form of "use." Those seizures together facilitated a separate, additional search for more information about Riley. Later, at the station, Detective Malinowski, who had come at the request of Officer Dunnigan, "looked through the phone," turning up photos that corroborated other evidence suggesting that Riley was involved in gang activity.

Officer Dunnigan's and Detective Malinowski's searches of the phone have similarities to the inventory search of a car. Both searches were executed through a series of small seizures. Data in a phone obviously does not display itself. Rather, the phone responds to commands issued via taps, touches, and swipes on buttons and screens. Looking through the phone made use of its electronics, the battery, the display technology, and the data, none of which are ordinarily the government's property to use.

[38] 395 U.S. 752, 762-763 (1969).
[39] *See, e.g.*, Illinois v. Lafayette, 462 U.S. 640 (1983).
[40] People v. Riley, 2013 Cal. App. Unpub., LEXIS 1033 at 8 (Cal. 2013).

The power of Officer Dunnigan and Detective Malinowski to use the phone this way is what Riley contested in the Supreme Court.[41]

In *Riley*, as in many Fourth Amendment cases, there were many separate instances of searching and seizing. The imperfect record in the case suggests three substantial seizures and many more minor ones, with six legal justifications among them. The five searches in the case had three legal bases. Courts often lump these activities together, which can be an efficient shorthand. But sometimes, glossing over details results in lost fidelity to both the facts and the protections of the Fourth Amendment.

The most sensible, faithful, and articulate application of the Fourth Amendment's elements starts with seizures and searches. Because seizures so often precede searches in time, or constitute them, the first question to ask is whether a given fact pattern included any seizure.

Was there a seizure?

The Supreme Court has rarely defined "seizure" distinctly from "search."[42] This is in part because small seizures are often the means by which government agents reveal the information they seek. Seizures are constituents of an overall search. Whether or not there is any searching, though, a seizure exists whenever government agents infringe a property right,[43] including the property right people have in their own persons.

We can see what seizure looks like, and how it commonly interacts with search, in a case as familiar as *Terry v. Ohio*.[44] In *Terry*, a plain-clothes police detective observed three men acting strangely and became suspicious that they were "casing" a store for a "stick-up."[45] Stopping them some blocks away and receiving an unsatisfactory answer to his questions, Officer McFadden "grabbed petitioner Terry, spun him around . . . and patted down the outside of his clothing."[46] Doing so revealed a gun.

The government urged the Court to place brief "stop and frisk" incidents like this outside the Fourth Amendment,[47] arguing that police behavior short of a "technical arrest" or a "full blown-search" did not implicate constitutional scrutiny.[48] The Court

---

[41] Detective Malinowski's seizure of data in downloading it from the cell phone was an additional step in the process of investigating Riley, which Riley did not contest articulately. The legal authority to seize data would spring from discovery of it as evidence during a lawful search of the cell phone.
[42] United States v. Jacobsen, 466 U.S. 109, 114 n.5 (1984) ("[T]he concept of a 'seizure' of property is not much discussed in our cases.").
[43] Bright minds will question this broad statement, pointing to the Fifth Amendment's Takings Clause as the rule that generally controls and administers government property invasions. That provision is used more often to challenge civil seizures, and the Fourth Amendment criminal ones, but the two overlap. *See* Severance v. Patterson, 566 F. 3d 490, 501 (5th Cir. 2009); Presley v. City of Charlottesville, 464 F. 3d 480, 487 (4th Cir. 2006).
[44] 392 U.S. 1, 6 (1968).
[45] *Id*. at 6.
[46] *Id.* at 7.
[47] *Id*. at 16 fn. 12.
[48] *Id.*at 19.

rejected the idea that there should be a fuzzy line dividing "stop and frisk" from "search and seizure." It wrote with precision about the seizure, then the search, of Terry: "[T]here can be no question . . . that Officer McFadden 'seized' petitioner and subjected him to a 'search' when he took hold of him and patted down the outer surfaces of his clothing."[49] One following the other, the seizure and search were reasonable and therefore constitutional. Though Justice Douglas dissented from the ruling, he agreed that Terry was "seized" within the meaning of the Fourth Amendment.[50] "I also agree," he wrote, "that frisking petitioner and his companions for guns was a 'search.'"[51]

Often, as in *Terry*, a seizure or seizures, and the search they facilitate, have the same legal justification—or they both lack one. So in *United States v. Jones*,[52] a recent case where government agents attached a GPS device to a vehicle to track its owner, the Court struck down Jones's conviction because "[t]he Government physically occupied private property for the purpose of obtaining information" without a warrant.[53] The invasion of a property right in making use of the car and the searching that use facilitated violated the Fourth Amendment the same way.[54] This was also true of moving pieces of stereo equipment to search for the serial numbers on them in *Arizona v. Hicks*.[55]

Seizures and searches are not the same, and they do not always occur together. In *Soldal v. Cook County*,[56] government agents seized a mobile home—literally helped take it from its owner—making no search of it.[57] In *Kyllo v. United States*,[58] there was a search without a seizure. Government agents used a thermal imager to observe heat emanations from a home, "a 'search' despite the absence of trespass."[59]

At bottom, "seizure" is best administered as any government invasion of a property right. The extent of the seizure is not important,[60] and the question for administering the constitutional right is not whether an otherwise actionable trespass has occurred.[61] Any invasion of a property right is a potential constitutional "trespass"—in

---

[49] *Id*.
[50] *Id*. at 35 (Douglas, J., dissenting).
[51] *Id*.
[52] 132 S. Ct. 945 (2012).
[53] *Id*. at 949.
[54] *See* ACLU v. Clapper, ___ F._d ___ (2nd Cir. 2015) (referring to attachment of the GPS device in Jones as "a technical trespass on the defendant's vehicle.")
[55] 480 U.S. 321 (1987).
[56] 506 U.S. 56 (1992).
[57] *Id*. at 68.
[58] 533 U.S. 27 (2001).
[59] *Id*. at 32.
[60] "[E]very invasion of private property, be it ever so minute, is a trespass," said Charles Pratt, Chief Justice of the Court of Common Pleas in 1765's *Entick v. Carrington*. 19 Howell's St Trials 1029, 1066 (CP 1765). "It is not so much the breaking of his door nor the rummaging of his drawers that constitutes the essence of the offense, but it is the invasion of his indefeasible rights of personal liberty." *Id.*
[61] *See* Laurent Sacharoff, *Constitutional Trespass*, 81 TENN. L. REV. 877 (2014). The Court has been consistently unclear about what it is doing when it administers the seizure concept—sometimes suggesting an overlap between common law trespass and seizure. The confusion is aided by scholarship that conflates property, the right, with trespass, the cause of action. *See* Orin S. Kerr, *The Curious History of Fourth*

the broad sense meaning a "wrong"—which triggers continued analysis to see if it was indeed wrongful.

Modern precision also requires recognizing that seizure exists when government agents violate any incident of property ownership, including not only the right to possess property but also the right to use it. The right to exclude others and to the income of property—the enjoyment of its benefits—are yet more in what law students are taught to be the "bundle of sticks" that comprises property rights.[62]

Blackstone defined property as "that sole and despotic dominion . . . exercise[d] over the external things … in total exclusion of the right of any other."[63] The U.S. Supreme Court, too, has focused on exclusion as the critical property right. In *Loretto v. Teleprompter Manhattan CATV Corp*., the Court called the right to exclude "one of the most treasured strands" of the property rights bundle.[64] *Kaiser Aetna v. United States* called it "one of the most essential sticks."[65]

The Supreme Court's cases have sometimes wandered away from the full correlation between property rights and seizure that sound administration of the Fourth Amendment requires. Casual use of language in a spate of Fourth Amendment cases from the 1980s suggests that only possession—the "possessory" interest in property—is relevant to Fourth Amendment analysis. In *United States v. Place*,[66] for example, the Court discussed the "possessory" interest in luggage.[67] The Court in *United States v. Jacobsen*[68] found a seizure because destruction of powder infringed "possessory interests."[69] And in *United States v. Karo*,[70] noted above, the Court found that installation of a beeper in a canister did not interfere with a "possessory" interest in the canister.[71] *Arizona v. Hicks* found that recording serial numbers from stereo equipment overturned for the purpose was not a seizure because it did not "'meaningfully interfere' with respondent's possessory interest in either the serial numbers of the equipment."[72]

Amendment Seizures, 1 SUP. CT. REV. 67 (2012). This may suggest to some that property has no place in administering a right that makes direct reference to four categories of property.

[62] Legal philosopher Tony Honoré best articulates the bundle of sticks concept. His 1961 essay, "Ownership," described the incidents of ownership common to "mature legal systems." TONY HONORÉ, OXFORD ESSAYS ON JURISPRUDENCE 104-147 (A.G. Guest ed., 1961), *republished in* TONY HONORÉ, MAKING LAW BIND: ESSAYS LEGAL AND PHILOSOPHICAL 161, 162 (1987). "Ownership comprises the right to possess, the right to use, the right to manage, the right to the income of the thing, the right to the capital, the right to security, the rights or incidents of transmissibility and absence of term, the duty to prevent harm, liability to execution, and the incident of residuarity." *Id*. at 165.

[63] 2 WILLIAM BLACKSTONE, COMMENTARIES 2.

[64] 458 U.S. 419, 435 (1982).

[65] 444 U.S. 164, 176 (1979)

[66] 462 U.S. 696 (1983).

[67] *Id*. at 705.

[68] 466 U.S. 109 (1984).

[69] *Id*. at 113.

[70] 468 U.S. 705 (1984).

[71] *Id*. at 712.

[72] 480 U.S. 321, 324 (1987) (citing Maryland v. Macon, 472 U.S. 463, 469 (1985)).

Justice Stevens's *Karo* dissent was correct, if muddy on distinctions among property rights: "Surely such an invasion is an 'interference' with possessory rights; the right to exclude . . . had been infringed."[73] In 1990, Justice Stevens wrote more clearly about seizure of property for the majority in *Horton v. California*:[74] "a seizure deprives the individual of dominion over his or her person or property."[75]

Seizures of Property Rights other than Possession

In the past, it may have been generally sound to treat deprivation of "possessory interests" as coterminous with constitutional seizure. Possession of movables is often the aspect of ownership that is material in Fourth Amendment cases—it certainly has been the easiest to recognize. But at least one court has treated seizure of a future interest as actionable under the Fourth Amendment,[76] and the limitation of seizure to the possessory interest does not translate to information or the information technology context. The interests that the Fourth Amendment protects can be invaded by depriving a person of the right to exclude others from data or by the *use* of information technologies without respect to possession.

The line between possession and use was what Officer Dunnigan crossed in *Riley*. He had properly seized Riley's cell phone incident to arrest,[77] so his possession of the phone was rightful. But Dunnigan also *used* the phone, manipulating its interface and drawing down its battery power, to gather evidence. Using a device to bring stored information out of its natural concealment—by looking through photos on it, for example—does a great deal to threaten the interests that the Fourth Amendment protects. Chief Justice Roberts issued a crisp admonition for such seizure-based searches: "get a warrant."[78]

Use of physical items that is otherwise unremarkable may become constitutionally significant if the use interacts with information technologies. The *Jones* case is an example. The government did not take possession of the defendant's car, but by attaching their GPS device to it, they used the car to transport their location sensor. The government's agents enjoyed the benefits of Jones's vehicle, taking use and enjoyment without the legal right to do so, and they deprived Jones of his right to exclude others from the car. These seizures all underlaid their continuous, four-week search for Jones's location.[79]

---

[73] *Id*. at 729.
[74] 496 U.S. 128 (1990).
[75] *Id*. at 133.
[76] *See* Mathis v. City of Lyon, 633 F.3d 877 (9th Cir. 2011) (addressing seizure of future interest in personal property).
[77] 134 S. Ct. at 2480.
[78] *Id*. at ___; 134 S. Ct. at 2495.
[79] *Jones* repudiates the Seventh Circuit's decision five years earlier in United States v. Garcia, 474 F.3d 994 (2007). In that case, Judge Posner called "untenable" the contention that attaching a tracking device to a car is a seizure. *Id*. at 996.

Detailed attention to property rights also explains seizure of data without reference to the device on which it is held, such as when government agents download or copy a suspect's data. Data and information are properly thought of as property, though they have different proper*ties* than tangible items. Information and data are routinely held, used, and traded consistent with the sticks in the "bundle" conception of property.[80] This is true without reference to intellectual property legislation.

When government agents copy data or information that is otherwise unavailable for their use, they have taken the rights to use and enjoy that data's benefits for the government, and the owner's right to exclude others has been violated.[81] The owner's rights to possess and to use the data are not typically compromised in these cases, of course, because the owner still retains a copy. Government agents invade no property right if communications and data are publicly available, or if they can otherwise lawfully access, copy, and use it.

As with telephones according to Justice Butler's view in *Olmstead*, people use modern communications and Internet facilities under contracts that allocate property rights. Though hardly with perfect clarity,[82] these contracts detail how communications machinery will be used, and they divide up the ownership of information and data. The use of cables and switches is subdivided into nanoseconds and slivers of wavelength rather than minutes on a wire, but the contractual protections for customer privacy are similar—if more explicit and detailed—to what they were in the 1920s.

The *Full Privacy Policy* of Verizon,[83] for example, is a 5,000-word tome, describing in detail the company's policies with regard to data collection, use, sharing, safety, and security. Verizon collects and derives customer-identifiable information subject to these contractual covenants. The communications and the data that result from it are partially the property of Verizon and partially the property of their customers, as defined in the privacy policy.

---

[80] Someone who knows a recipe for cookies, for example, has the right to use it to make those cookies, also enjoying the right to income from the recipe. Excluding others from information is a right that can be very valuable, such as the recipe for Coca-Cola. Knowing another's secrets is an enjoyable exercise of the right to possess information—either because it nurtures an intimate relationship or because it puts a person one-up on another. Secret-keeping and some forms of dishonesty are appropriate exercises of the right to exclude others from information, with valuable social and interpersonal purposes. *See* United States v. Alvarez, __ F.3d __, 2001 WL 941617 (9th Cir. Mar. 21, 2011) (ord. denying reh'g en banc) (Kozinski, C.J., concurring in denial of reh'g en banc) ("Saints may always tell the truth, but for mortals living means lying." E.g.: "We lie to protect our privacy ("No, I don't live around here"); to avoid hurt feelings ("Friday is my study night"); to make others feel better ("Gee you've gotten skinny"); to avoid recriminations ("I only lost $10 at poker"); to prevent grief ("The doc says you're getting better"); to maintain domestic tranquility ("She's just a friend"). . . or to maintain innocence ("There are eight tiny reindeer on the rooftop").")

[81] *See* Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476, 491-96 (2010).

[82] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 142-45 (2014).

[83] *Full Privacy Policy*, VERIZON, http://www22.verizon.com/about/privacy/policy/.

The general rule is that Verizon does not share customer data, and there are exceptions to the general rule. "We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: . . . to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law."[84] This precludes Verizon from making disclosures in other circumstances, such as invalid legal processes. In terms of property, the right to exclude others from personal information belongs to the customer when legal processes are invalid. Government agents accessing their data invade the customer's property right, a seizure.

It has been more than twenty years since the publication of Anne Wells Branscomb's *Who Owns Information?*,[85] but awareness of common law and contract rights in information and data is still underdeveloped, and Fourth Amendment analysis suffers for it. In the areas where it is most important, such as legal services and health care, there is some recognition of information ownership, but contract rights are often interleaved with professional ethics and torts.[86] Government regulations also sometimes undercut contractual information rights.[87] But property rights in information and data are routinely allocated by contract.[88] Contract and property elucidate better than any other framework the sometimes finely subdivided ownership rights that attend to information and data.[89]

In the online world, the "cloud" metaphor probably confuses many by suggesting that there are not specific, identifiable, legally liable, and responsible service providers who facilitate Internet communications and services subject to contractual obligations. There are.[90] Through painstaking common law development, our society is determining

---

[84] *Id*.

[85] ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? (1994).

[86] Though lawyers are trained to think of it in terms of professional ethics, the attorney's duty of confidentiality to clients is based in contract. The Hippocratic Oath is the ethical expression of a contractual duty on health care providers, as the Supreme Court of New York has found, relying on contract liability when addressing unauthorized disclosure of confidential psychological information. *Hammonds v. Aetna Casualty & Surety* is a leading case in the area of unauthorized disclosure of medical information. 243 F.Supp. 793 (N.D. Ohio 1965). ("Any time a doctor undertakes the treatment of a patient, . . . [d]octor and patient enter into a simple contract. As an implied condition of that contract, this Court is of the opinion that the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission.").

[87] *See* Jim Harper, *Understanding Privacy—and the Real Threats to It*, Cato Inst. Pol'y Anal. No. 520, 14-15 (Aug. 4, 2004).

[88] Before the Bank Secrecy Act undercut common law development of information terms in financial services contracts, courts recognized an implied contractual duty not to disclose information about depositors' accounts. *See, e.g.*, *Peterson v. Idaho First National Bank*, 83 Idaho 578, 367 P.2d 284 (1961) (finding that a bank had an implied duty not to disclose any information concerning a depositor's account to third persons unless authorized by law or by the depositor). The Supreme Court did not address the conflict with bank customers' contractual rights when it ratified the Bank Secrecy Act as against constitutional challenges in *California Bankers* and *Miller*.

[89] *See* Carpenter v. United States, 484 U.S. 19, 25 (1987); United States v. Seidlitz, 589 F. 2d 152, 160 (4th Cir. 1978).

[90] *See* Ingrid Burrington, *What People Mean When They Talk About "The Cloud*," THE ATLANTIC (Nov. 4, 2015), http://www.theatlantic.com/technology/archive/2015/11/what-people-mean-when-they-talk-about-the-cloud/413758/.

the role of online statements, "clickwrap" licenses, and the like in articulating the rules under which communications and data are transmitted and stored.[91] Hurrying to establish legal frameworks that common law has not yet supplied, statutes dealing with event data recorders in automobiles do all but call the data they produce the property of the car owner.[92] The better view is that privacy policies and published Terms of Use statements are either explicit contract terms or attempts by the supplying party to establish, augment, or alter implied contract rights that govern the ownership of information, data, and communications.

Terminology used by Congress in federal legislation illustrates the general understanding that data and communications are property. Section 702 of the Telecommunications Act of 1996,[93] for example, says: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers…."[94] Calling this data "Consumer Proprietary Network Information" (CPNI), Congress used the adjective "proprietary" because it conceived of the data and information that telephone companies amass essentially as property.

Doing so nests with communications and data being the subject of contract terms, and it does not exclude the same information being jointly owned by the customer. Indeed, the statute allocates some narrow statutory property rights in CPNI to telecommunications customers. Consumers can require telecommunications providers to disclose copies of their CPNI to them,[95] meaning the information is also theirs to possess and use if they want it. The privacy requirements of the statute can be avoided "with the approval of the customer,"[96] meaning that customers' rights to exclude others from personal information and data are alienable, as property rights are.

Contracts between communications firms and their customers contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass, and much of the data about communications usage does, too. When government agents seize communications and data that are the property of telecommunications firms or their customers, this should trigger further Fourth Amendment analysis. Credit Justice Butler's *ratio dissensi* in *Olmstead*.

---

[91] *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP.1 (2009).
[92] *See, e.g.,* Calif. Veh. Code § 9951.
[93] Pub. L. 104-104 (Feb. 8, 1996).
[94] 47 U.S.C. §222(a). The statute defines "Customer Proprietary Network Information" ("CPNI"), as "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and…information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer." 47 U.S.C. §222(f)(1).
[95] 47 U.S.C. §222(c)(2).
[96] 47 U.S.C. §222(c)(1).

Whether property is tangible or intangible, seizures occur whenever government agents invade a property right. Seizure includes not just taking possession, but taking away the right to exclude or taking the rights to use and enjoy property for oneself, including by operating digital devices or copying and using data. Courts administering the Fourth Amendment should recognize all the property rights that can be seized.

There are some nuances to this simple rule, of course. The Fourth Amendment limits its own application to persons, houses, papers, and effects. In the main, this means that it protects a smaller universe of things than property rights or common law trespass does.[97] The inclusion of "persons,"[98] on the other hand, extends the Fourth Amendment's seizure protection to self-ownership. This is beyond what trespass law usually protects and what most people today think of as property, despite the intellectual endowments given by Locke and Madison.[99]

And, of course, the existence of seizure does not end the analysis; seizures may be reasonable. That question arises later in the process of applying the Fourth Amendment's elements. If there was a seizure, it may stand for further analysis on its own. Often, though, seizures facilitate a search. The existence of a search is the next element of the Fourth Amendment analysis.

Was there a search?

Seizing and searching are distinct activities, and the distinction matters in some cases. While "seizure" is based in legal conclusions about property rights, there is no common law of "search." Natural language must guide whether looking (or other sensing) is so focused or directed that it crosses a threshold into the "search" category.

The word "search" suggests intentionality on the part of the actor, a purpose of finding something.[100] Advocates and courts should examine the actions of government agents and often literally ask them whether they meant to find something in particular. If they did, there was likely a search, later to be determined reasonable or unreasonable.

Sensing often rises to the level of searching in a way that is relatively easy to recognize. That is when government agents seek to bring information or things out of concealment. Picking up others' things, for example, entering private property, and manipulating others' persons, objects, devices, or data—these activities typically aim to expose something that was concealed. They signal directedness and focus that goes beyond casual and undirected looking, smelling, tasting, or feeling.

---

[97] The relationship of trespass to the Fourth Amendment was much discussed in *Jones*, 132 S. Ct. 945.
[98] 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.").
[99] *See* JOHN LOCKE, SECOND TREATISE OF GOVERNMENT § 27 ("every Man has a Property in his own Person"); THE PAPERS OF JAMES MADISON, *Property,* 14:266-68 ("[A man] has a property very dear to him in the safety and liberty of his person.").
[100] *See infra*, notes 134-35.

Because of their role in exposing concealed things, seizures make searches easy to recognize. But exposure can also be produced by the use of high-tech or specialized devices and observation techniques. In some cases, government agents may look so intently for something already exposed that the effort is a "search." But most often the objective fact that they try to deprive something of concealment can guide the 'search' for "search."

Concealment Subject to Search Produces Exposure

Familiar though they are, the concepts of "concealment" and "exposure," are not often examined in constitutional or legal terms. *New York v. Class*[101] is a search case that helps explore their contours, and it illustrates how "concealment" and "exposure" can help administer the "search" question.

In *Class*, New York City police officers Lawrence Meyer and William McNamee pulled over Benigno Class for speeding and driving with a cracked windshield. While Officer Meyer talked to Class, who had exited the vehicle, Officer McNamee went to the car and opened its door—a small seizure—to look for its Vehicle Identification Number (VIN). Not finding it there, he reached into the interior of Class's car to move some papers—another small seizure—that were covering the area of the dashboard where the VIN was located. Doing so, he espied a gun under the seat, which led to Class's being charged with criminal possession of a weapon.[102] His small, seizure-based search was a success.

The Court ruled the opposite way, citing the lacking "expectation of privacy" in Vehicle Identification Numbers.[103] Rather than methodically analyzing the seizure question, the search question, and then reasonableness, the Court pronounced VINs non-private and re-interpreted activities focused on discovering particular concealed information as non-search.

Class illustrates how the "reasonable expectation of privacy" test turns an objective, essentially factual question—the existence or non-existence of a search—inside out. Doing so, the Court produced a wrong result.[104]

Kyllo v. United States,[105] decided in 2001, is a wonderfully instructive search case because it involved no seizure at all. It allows us to observe search in the abstract and see how concealment subjected to search produces exposure. *Kyllo* does not involve the familiar operation of light, of course, but radiation in a non-visible part of the electromagnetic spectrum.

---

[101] 475 U.S. 106 (1981).
[102] *Id*. at 108.
[103] *Id*. at 111-14.
[104] A better way to reach the same result would have been for the Court to recognize the search, but find it reasonable for many of the same reasons around motor vehicle administration the Court found it not a search. That result seems unlikely, though, because Officers Meyer and McNamee had no suspicion of crime for which the VIN was relevant. *Id.* at 108.
[105] 533 U.S. 27 (2001).

In the case, agents of the U.S. Department of the Interior suspected that Danny Lee Kyllo was growing marijuana using high-intensity lamps in his home on Rhododendron Drive in Florence, Oregon.[106] From a public area, they aimed an Agema thermovision 210 thermal imager at his triplex. The imager displayed significantly more heat over the roof of the garage and on a side wall of Kyllo's home than elsewhere on the premises. Using this and other information, the agents obtained a warrant, searched the home, and found the drugs they suspected.

Prior to the government agents' actions, Kyllo's domestic activities and his possessions were concealed. The opaque and impervious walls of his home physically prevented others from seeing, hearing, or smelling—and certainly from tasting—what occurred or existed within. Temperature differences among the home's roof and exterior walls were invisible, disabling outsiders from drawing inferences about Kyllo's domestic life. Kyllo's property rights meant that others could not approach the house closely enough to peer in windows, sniff at side doors, or touch it to measure its exterior temperatures. Nor could they enter into the house.[107] But by using their thermal imager and making imperceptible radiation perceptible, the Interior Department's agents undercut the concealment Kyllo had given to activities going on within his domicile. They exposed that there was a source of unusual heat inside, which allowed them to draw inferences about its cause.[108]

The Supreme Court found the use of thermal imaging on a home without a warrant to be a Fourth Amendment violation. "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," the Court held, "the surveillance is a 'search' and is presumptively unreasonable without a warrant."[109]

There's a lot packed into that sentence, including the conclusion that this particular search was unreasonable. That question comes later in a methodical analysis. But in *Kyllo* concealed, imperceptible, and "unknowable" information was exposed through a search.

The Supreme Court has developed simple and administrable rules for the treatment of "exposure" under the Fourth Amendment. The majority in *Katz*, for example, said, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[110] If law enforcers can see,

---

[106] *Id*. at 29.
[107] Doing either would have violated his property right to exclude others.
[108] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 553 ("For the holding in *Kyllo* to make sense, it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search. What made the conduct in *Kyllo* a search was not the existence of the radiation signal in the air, but the output of the thermal image machine and what it exposed to human observation.").
[109] *Id*. at 40.
[110] *Katz*, 389 U.S. at 351.

hear, smell, or feel something, they are entitled to take cognizance of it. This is the "plain view" doctrine, which the Court expanded on in *Horton v. California*.[111]

A parallel "plain concealment" doctrine would bring simplicity and symmetry to the question of whether things are available for government perusal. The rule should be that information one conceals from the general public is also concealed from government agents. When government agents seek to expose concealed things by defeating or eluding physical or human laws, it is a search.[112] This is not the exclusive signal of directed or focused sensing. Search can also exist if government agents intensely examine exposed things. But manufactured exposure is a strong signal of searching.

The Supreme Court is having mixed success with placing topical investigatory techniques and evidentiary materials, such as drug-sniffing dogs and DNA, within the concealment-versus-exposure rubric. Doing so with more precision would improve Fourth Amendment administration.

Sensitive to the 'searching' examination given by drug-sniffing dogs, for example, the Court has focused on the seizures that often attend the use of this investigatory tool. In *Florida v. Jardines*, for example, the Court found that bringing a drug-sniffing dog to the front door of a home exceeded the scope of the traditional license that property owners offer to uninvited guests.[113] "One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy," the Court said.[114] In *Rodriguez v. United States*,[115] like *Illinois v. Caballes* before it,[116] the Court examined how long a suspect was seized so a dog could sniff around him for drugs.

These cases elide the central aspect of a drug-sniffing dog examination, which is to search for drugs.[117] They discover concentrations of particulates that suggest the presence of otherwise imperceptible, and thus concealed, illegal drugs. Drug-sniffing dogs are analogous to thermal imagers in that they take physical phenomena that are imperceptible to humans and make them perceptible. Trained dogs are cuddly chromatographs. The question when they do give exposure to something in or on a person, house, or effect is whether such a search was reasonable.

The Court has easily recognized that DNA analysis is a search, but it has somewhat muddled the concepts. The Court in *Maryland v. King* treated the buccal swab involved in gathering DNA as a "search."[118] In fact, taking a sample of cheek cells is a seizure of that tissue, and the analysis of DNA in it to discern the identifying alleles was a

---

[111] 496 U.S. 128 (1990).
[112] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 ("a search occurs when information from or about the data is exposed to possible human observation").
[113] 133 S. Ct. 1409, 1416 (2013).
[114] *Id*. at 1417.
[115] 575 U.S. ___ (2015).
[116] 543 U.S. 405 (2005).
[117] *But see Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring) ("[A] drug-detection dog is a specialized device for discovering objects not in plain view (or plain smell).").
[118] 133 S. Ct. 1958, 1969 (2013).

search of that seized material. This kind of precision was not important in *King*, but it will be needed when a challenge to government agents' DNA analysis of abandoned tissue arises.[119] It is almost certainly not a seizure to collect abandoned hair, saliva, or semen, but analyzing that bit of a person exposes concealed information. It is highly directed, technically enhanced observation: a search. Treating it as not searched because the bodily material is not seized would be an error.

The next step in the constitutional analysis is to find whether it is a constitutionally protected item, which may be a difficult question because such DNA is both abandoned and always a part of a person's body. DNA analysis of material collected in a rape kit or from under the fingernails of a murder victim would likely be reasonable because the bodily material from which DNA is analyzed is itself direct evidence from the crime scene. Analysis of abandoned DNA collected from a suspect's drinking glass should probably require a warrant because the analysis is performed to confirm an investigatory theory. When development of the technology allows it, mass scale DNA analysis should probably be found flatly unreasonable, as suspicion lacks and any warrant permitting it would be a general warrant to search the material sloughed off the body of any person that had been in the collection area.

Real cases should flesh out the rules, but DNA and the information it contains are naturally concealed. Whether seized, as in *King*, or collected without seizure, DNA analysis is a search that exposes a human's molecular makeup.

Communications and Concealment

The special problem of communications is a little challenging to fit within the concealment-versus-exposure rubric, but careful analysis shows that it fits well. The Supreme Court has used concealment since early in our nation's legal history to administer the Fourth Amendment's application to communications. The constitutional protection of postal mail and its basis in concealment show how to administer constitutional protection of telephone and Internet communications today.

When establishing their "constitutional post," America's revolutionaries were acutely aware of the importance of postal privacy. Many of their communications, after all, had dealt with subject matter that the British Crown and Loyalists would have regarded as treasonous.[120] So it is not surprising that Congress's first comprehensive postal statute in 1792 wrote the confidentiality of sealed correspondence into law, with heavy fines for opening or delaying mail.[121]

---

[119] *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006).
[120] *See* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 564, 563–64 (2007).
[121] *Id*. at 566-57. In relevant part, the 1792 law says: "[I]f any person, employed in any of the departments of the general post-office, shall unlawfully detain, delay, or open, any letter, packet, bag or mail of letters, with which he shall be entrusted, or which shall have come to his possession, and which are intended to be conveyed by post . . . , every such offender, being thereof duly convicted, shall, for every such offence, be

In 1878, *Ex Parte Jackson*[122] established the protected status of mail under the Fourth Amendment. The Court made an important distinction: it accorded constitutional protection to mailed content if senders had initially concealed the information in their mailed items. Protection did not obtain for unsealed mail like newspapers and pamphlets: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[123] Letters and packages enclosing their contents in opaque materials had the same security as letters kept in the home. Mailed matter left open had no physical security and thus no constitutional security. The arrangement of postal mail to conceal gave its contents protection backed by the Fourth Amendment.

In *Olmstead*, the Court failed to adapt that rule to a new technology. Telephone communications are much like written letters, except that they reduce words to electric (today, digital) signals rather than printing on paper. Crucially, these signals pass along telephone lines invisibly and inaudibly to any human. They are concealed. Accessing them requires an invasion of the private property of the phone company and its customers, as well as a search of the electrical signal to draw its meaning out of concealment.

In *Olmstead*, Chief Justice William Howard Taft described how the government tapped the defendants' phones: "Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office" of the conspiracy.[124] These wires carried signals to a device the government controlled, which reproduced the sound of voices otherwise unheard all along the wire. Government agents took the conversations down to use as evidence. But later in his opinion, Taft ignored these facts, justifying his legal conclusions by saying: "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only."[125] Chief Justice Taft was wrong. The wire and signals both were seized and the signals searched.

As Justice Butler pointed out in his dissent, "the exclusive use of the wire belong[ed] to the persons served by it."[126] The government's agents' use of the wire invaded Olmstead's right to exclude others. Collecting the signals, which "belong[ed] to the parties between whom they pass[ed],"[127] was a seizure of those signals. Converting the signals to the sounds they represented was a use of Olmstead's property that government agents were not entitled to make, a further seizure. These efforts gave exposure to formerly concealed information, a search. All told, the government's activity was a seizure-based search.

---

fined not exceeding three hundred dollars, or imprisoned not exceeding six months, or both, according to the circumstances and aggravations of the offence." Act of Feb. 20, 1792, § 16, 1 Stat. 232, 236.

[122] 96 U.S. 727 (1878).

[123] *Jackson*, 96 U.S. at 733.

[124] *Olmstead*, 277 U.S. at 457.

[125] *Id*. at 464.

[126] *Id*. at 487 (Butler, J., dissenting).

[127] *Id*.

The *Katz* case, which reversed *Olmstead*, is the progenitor of "reasonable expectation of privacy" doctrine, but the majority ruling in *Katz* centered on concealment and exposure. While Justice Harlan opined about privacy expectations in his solo concurrence, Justice Potter Stewart's majority opinion rested on the physical protection that Katz had given to his oral communications by going into a phone booth. Stewart's preface is what people remember:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[128]

The paragraphs that followed discussed the import of Katz going into a phone booth made of glass that concealed the sound of his voice.[129] Against the argument that Katz's body was in public for all to see, the Court wrote: "[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear."[130] The government's use of a secreted listening and recording device to enhance ordinary perception overcame the physical concealment Katz had given to his voice. Gathering the sound waves seized something of Katz's. Exposing the concealed conversation was a Fourth Amendment search.

As in *Ex Parte Jackson*, the rationale of the *Katz* majority was that people who generally conceal information on or about their persons, houses, papers, and effects have concealed it from the government. Other than in certain narrow cases, such as exigency, the government cannot overcome this concealment via seizure or search except after getting a warrant.

This rationale applies the same way to Internet communications, which operate similarly to mail and telephones. Rather than words or sounds converted to writing or analog electrical signals, Internet communications and data are converted into digital formats. As letters and telephone calls do in their media environments, Internet communications pass invisibly and inaudibly along privately owned and apportioned wires, switches, and fiber-optic cables. The communications are concealed from observation by physics and law.[131]

All this comports with common meanings of words, both today and at the time of the Framing. *Black's Law Dictionary* says that "conceal" means "hide, secrete, or withhold from the knowledge of others . . . withhold from utterance or declaration . . . cover or keep from sight … hide or withdraw from observation, or prevent discovery

---

[128] *Katz*, 389 U.S. at 351 (citations omitted).
[129] *Id*. at 352.
[130] *Id*.
[131] *See* Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, CATO SUP. CT. REV. 219 (2011-2012).

of."[132] *Black's* defines the verb "to expose" as "[t]o show publicly; to display; to offer to the public view, as, to 'expose' goods to sale, to 'expose' a tariff or schedule of rates, to 'expose' misconduct of public or quasi-public figures."[133] Webster's 1828 dictionary defined "to expose" first as "[t]o lay open; to set to public view; to disclose; to uncover or draw from concealment; as, to expose the secret artifices of a court; to expose a plan or design."[134]

Search sits between concealment and exposure: "'Search' consists of looking for or seeking out that which is otherwise concealed from view," says *Black's*.[135] In *Kyllo*, the Court said, "When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief.'"[136] Communications and data, just like other things, can be seized, and they are searched when their contents are brought out of concealment into exposure.

Exposed Things Can Be Searched

In natural language, there can be examinations of already exposed things that rise to the level of "search"—"to search the wood for a thief," for example. (Woods are not an object of the Fourth Amendment's protections, of course, but that is relevant later in the analysis.) Efforts to expose concealed things are not the only signal of searching. Sensing with a "purpose of finding something" is the gravamen of "search." It may not be signaled by the manufacture of physical exposure, instead coming down to government agents' subjective purpose.

The use of certain devices or technologies to enhance perception of exposed things may signal when sensing activities cross over from casual looking to directed searching. Ordinary enhancements to sensing do not make for "search." Wearing ordinary corrective lenses or hearing aids, for example, probably does not make looking or listening into searching. The Court has held that using a flashlight to illuminate an exposed area is not a "search."[137]

But the use of highly powerful or exotic visual, audio, or other collection or analysis tools may exhibit that intensity or directedness that converts looking to searching. Recall that a factor in the *Kyllo* decision was the use of a device "not in

[132] BLACK'S LAW DICTIONARY at 288.
[133] *Id*. at 579.
[134] N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed. 1989).
[135] BLACK'S LAW DICTIONARY at 1349.
[136] N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed. 1989) (quoted in *Kyllo*, 533 U.S. at 32 n.1).
[137] In *United States v. Lee*, 274 U.S. 559 (1927), for example, government agents on a Coast Guard ship used a searchlight to apprehend cases of liquor onboard a boat during Prohibition. *Id*. at 561. This common enhancement to sensing Justice Brandeis deemed "no search." *Id*. at 563. More recently, in *Texas v. Brown*, 460 U.S. 730 (1983), the Court held that shining a flashlight into a stopped car did not violate the Constitution because "the use of artificial means to illuminate a darkened area simply does not constitute a search." *Id*. at 740.

general public use."[138] The case is better administered using the generalization that bringing things out of concealment signals searching, but using a high-tech gizmo suggests directedness and intensity that pushes sensing over the line into searching.

One example of exotic technology used on exposed things is facial recognition. Our faces are exposed to the public every day, of course. Facial recognition can be done on photographs that were taken voluntarily or with the acquiescence of the subject,[139] so collecting the appearance of the face is typically not a seizure. There is no right to exclude others from such imagery per se. Gathering a facial image (in the visible spectrum) does not give exposure to concealed things, so collection of a facial image is not a search on that basis. That does not foreclose the question whether exposed facial images once collected might be searched.

Facial recognition systems work by converting the features of the face to a matrix of spatial relationships among its features, of colors, and textures. The distances between the eyes, width of the nose, color of the skin, and so on become elements in what is essentially a biometric signature. When the facial signature is collected, there may be no investigation underway, which may seem to imply that there is no Fourth Amendment search—just some inert administrative process. But the conversion of a face image to a facial recognition signature has only one purpose: to find something later.

Searching has two conceptual parts, which generally occur in a particular order. First, the specific thing to be searched for is identified. Next, the field in which it may be found is examined. Searching a forest, for instance, involves identifying the person, instrumentality, or evidence to be found, then marching through the area with eyes peeled for that thing. Facial recognition reverses these processes. It collects the material to be canvassed—facial signatures—then at any later time canvasses the earlier-collected facial signature data for a match. The fact that the steps in the process are reversed should not change the conclusion that facial recognition is a search technology and the use of it is a search. Conversion of a facial image to a facial signature that can be scanned for matches is a search of the face itself to render data that make the face amenable to being the object of a later search. It is enough of a step in the process of searching that it is best recognized as a search occurring at the time the processing is done. Facial recognition is an example of exposed things being searched because of the "purpose of finding something." There is no other purpose to facial recognition technology.

The fact that facial scanning is a search should not bias the question whether or not it is reasonable. It would seem unreasonable to collect and scan facial images of everyone appearing in a given public place, because none of them are suspicious by dint merely of being there. It may be reasonable to run facial scans during the issuance of drivers' licenses to thwart identity fraud, or it may not be. The mass of facial images collected for that purpose will be attractive for searching in pursuit of criminal suspects forever after the initial collection. Recurring searches of these facial signatures would

[138] *Kyllo*, 533 U.S. at 40.
[139] Conditioning a driver's license on "facial image capture," REAL ID Act of 2005 § 202(d)(3), is an arguable seizure.

wisely be regulated by the warrant requirement, though courts should determine this in actual cases.

The recent popularity of unmanned aerial flying vehicles, or drones, has raised the question of how their use by government agents might interact with the Fourth Amendment. Posit a fact situation analogous to *Jones*, but without attachment of a GPS device to a car. Rather, government agents sic a tiny cadre of drones to follow a car and note its whereabouts for weeks on end. Or imagine a drone flown above public property at an angle high enough to observe goings-on in a fenced backyard or through open windows. High-orbit, high-resolution cameras and monitoring software today allow extremely detailed observation and tracking of numerous people and things across vast expanses for long periods of time. In these cases, there may be no property invasion/seizure or exposure of concealed things to signal directedness and search. But the use of outré technologies and techniques may signal a "purpose of finding something" that is a search, even if the thing is unconcealed.

California v. Ciraolo,[140] decided in 1985, is one of very few Fourth Amendment cases where there is no invasion of a property right and arguably no exposure of a concealed thing to clearly signal the intensity of focus that makes for a "search." In the case, Santa Clara police received an anonymous tip that marijuana was growing in Ciraolo's backyard.[141] Unable to see over the high fences around the constitutionally protected "curtilage" of his home,[142] officers flew a private plane over it to confirm the presence of marijuana plants.[143] Based on the anonymous tip and their observations, they obtained a search warrant, searched the home, seized the plants, and charged Ciraolo.

The Supreme Court examined the directed aerial inspection under the "reasonable expectation of privacy" test. The high fences around the house did not necessarily manifest a subjective expectation of privacy, it turned out. Ciraolo had "merely a hope that no one would observe his gardening pursuits."[144] As to the objective reasonableness of expecting privacy in one's backyard, the Court noted that the officers were in public navigable airspace, the observations were non-intrusive, and the marijuana plants were easily discernable. Declining to say so explicitly, the Court concluded that this highly directed observation of Ciraolo's yard was not a search.[145] In *Florida v. Riley*,[146] the Court extended this precedent to observations taken from a helicopter at 400 feet.[147]

Aerial observation from a high enough height does not invade any property right, so it is not a seizure, and, absent the use of outré technology, it does not bring exposure to otherwise concealed things. The clearest cues to "search" do not exist. Still, scrambling a plane, flying it over a particular house, and looking down at it in hopes of espying

[140] 476 U.S. 207 (1986).
[141] *Id*. at 209.
[142] *Id*. at 212.
[143] *Id*. at 209.
[144] *Id*. at 212.
[145] *Id*. at 213-214.
[146] 488 U.S. 445 (1989).
[147] *Id*. at 450-51.

anticipated items seems to have a "purpose of finding something." Testimony in such cases may reveal a non-search explanation for this behavior, but it probably is searching in the ordinary sense of the term. *Ciraolo* and *Riley* seem wrongly decided.

As a precedent for drone- and satellite-based observation, *Ciraolo* would ratify aerial observation of all people, houses, and things exposed to the sky without limit. This would undercut the Fourth Amendment's grant of security to people in their persons, houses, papers, and effects whenever they were uncovered. In "reasonable expectation of privacy" cases like *Ciraolo*, courts can too easily reason backward from found drugs to lacking expectations of privacy.

Search, Seizure, and Privacy

Inquiring about privacy expectations, subjective or objective, is a poor way to administer the Fourth Amendment relative to the methodical, text-based analysis suggested here. But "privacy" has been discussed in the Court's Fourth Amendment decisionmaking for decades. The relationship between privacy and concealment shows that shifting to sounder Fourth Amendment administration would not be a departure from precedent, and it would help achieve the Court's aims with respect to the Fourth Amendment's protections. The Supreme Court has recently stated as a goal that it will "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[148]

Protecting privacy requires understanding what privacy is, as well as the role of concealment in protecting it. The strongest sense of the word "privacy," and the one relevant to Fourth Amendment administration, is enjoyment of control over personal information. People maintain privacy by exercising control over personal information as they see fit.

In 1967, the year that the Supreme Court decided *Katz*, scholar Alan Westin characterized privacy in his seminal book, *Privacy and Freedom*, as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[149] A tighter, more legalistic definition of privacy is: "[T]he subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[150] Given control over information about themselves, people will define and protect their privacy as they see fit.

Whether or not the Fourth Amendment requires it, giving individuals the same level of control over personal information today as they had at the time of the Framing is at least a meaningful and judicially administrable goal. One simply has to examine how people controlled information in the past and see that their ability to do so is maintained in the present.

---

[148] Kyllo v. United States, 533 U.S. 27, 34; *Jones*, 565 U.S. at 950; *Id*. at 958 (Alito, J., concurring).
[149] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).
[150] Harper, *Understanding Privacy, supra* note 87.

In the late eighteenth century, people controlled information about themselves by arranging things in the world around them. Retreating into one's home and drawing the blinds, for example, caused what happened inside to be private. Lowering one's voice to a level others could not hear made a conversation private. Draping the body with clothing made the details of its shapes, textures, and colors private. These methods use the physical properties of things to block sound waves, photons, and similar phenomena.

A list of all privacy-protecting decisions and behaviors would be very long, and it would not be helpful for crafting lasting privacy-protecting rules. But abstracting the nature of privacy protection can: People protect privacy through concealment, literally by preventing others from perceiving things.

The concepts should be familiar by now: Perception of something comes from being able to collect its representation in physical media. Photons reaching eyeballs make a thing visible to a person. Sound waves reaching eardrums make a thing audible to a person. Particulates reaching a person's nostrils or tongue make a thing perceptible by scent or taste. The surface of an object touched or pressed upon by skin can reveal its density, hardness, size, and weight. When a person's brain collects these data, he or she perceives the things in the world. The observer draws inferences about things, and about the people who own and control them.

When photons, sounds waves, particulate remnants, and surfaces that reveal things are not available, such things are concealed, and the drawing of inferences about people is blocked. This, again, is how people protect privacy. They did it this way in the late-eighteenth century, and they do it this way today.

It is not enough, of course, for people to withdraw into their homes, lower their voices, or get dressed. When people enter their homes, they do so relying on the aggregate of rights that prevent others from entering or accessing their homes to discover what goes on within. They rely on property rights, as Danny Lee Kyllo did. When people put on clothes to prevent photons from revealing the appearance of sensitive areas, they do so relying on protection against wrongful physical contact that might strip the body of its wrappings. They rely on the law of battery, as Terry did in Ohio.

Sometimes people do rely almost entirely on physics to protect privacy, such as in *Katz*, by lowering and shrouding their voices in public places. And sometimes they rely heavily on law, such as when they share information with a fiduciary or service provider bound to confidentiality by contract or regulation. Most of the time, people protect privacy using natural laws and human laws together to conceal.[151]

When government agents seek to expose concealed things, threatening privacy or rendering it asunder, that is searching. But reasoning backward from privacy expectations is not a sound way to administer the Fourth Amendment. The question of privacy expectations produces maladministration of the Fourth Amendment. Courts are not at

[151] Harper, *supra* note131.

their strengths examining why people erect physical barriers, what they think about them, or what others should think of their thinking. The Supreme Court has not historically relied on privacy and privacy expectations. Most cases rely on concealment and exposure. The very decision that founded the sideways "reasonable expectation of privacy" doctrine itself, *Katz v. United States*, was a concealment/exposure case.

The Court uses the "reasonable expectation of privacy" test less and less often. Invited to reason forward systematically and sensibly, courts are well equipped to judge where various activities lie on the continuum from casual, non-search looking and sensing to directed, relatively intense "searching." Courts can recognize "concealment" and "exposure." They can apply the common meaning of the word "search" to familiar human activity. They can do these things better than they can determine what are "reasonable expectations of privacy."

It is a low-consequence exercise, the "search" determination, because finding a "search" doesn't end the inquiry. The constitutional import of a search or seizure turns on later questions such as whether the search was of a constitutionally protected item and whether or not the search was reasonable.

Some care is required to fastidiously identify seizures and searches, of course. The former is any invasion of a property right, and the latter is intense sensing, often signaled by effort to remove concealment from something and give it exposure. Or it is sensing so directed as to exhibit a "purpose of finding something."

The house, the body, the gun, and the paper can be seized and searched. The wire, the communication, and the data can, too. They are all potential subjects of seizure and search regulated by the Fourth Amendment. If a seizure or search exists, though, this only raises the next question, which is whether the seizure or search was of someone's person, his or her papers, house, or effects.

Was the seizure or search of a thing the Fourth Amendment protects?

When there has been a seizure or search, the next question is whether it was of a constitutionally protected item—a person, house, paper, or effect. Perhaps absorbed by confusing Fourth Amendment doctrine, the Supreme Court has rarely made explicit what the contours of these concepts are. But they are mostly familiar and commonsensical.

Terry and many similar cases assume that the human body and its appurtenances are the Fourth Amendment "person." Taking possession of persons (to say nothing of using them) is a power the Fourth Amendment denies government agents in the absence of the requisite level of suspicion and typically a warrant.

Oliver v. United States[152] makes clear that the Fourth Amendment's protection for houses does not bar government agents' entry onto open fields, even when the owner has

[152] 466 U.S. 170 (1984).

posted a "no trespassing" sign at the property line.[153] Nothing since the Fourth Amendment was adopted has made places far away from a house constitutionally a "house." The dynamics of concealment, exposure, and security that existed when people departed their homes at the time of the Framing are the same today. Government agents who invade uninhabited private lands should be liable for trespass, perhaps, but they do not violate the Fourth Amendment.

Professor Andrew Guthrie Ferguson finds, though, that each of the items singled out for protection in the Fourth Amendment has been given "a more expansive reading than the pre-technological (pre-industrial) world of the Founders."[154] An example is the development of "curtilage" doctrine.

The concept of "papers" requires updating in light of changed information and communication technologies. It was not papers as a form-factor for cellulose that the Framers sought to protect, but the common medium for storage and communication of information.[155]

The federal trial court system has recognized, as it must, that digital representations of information are equivalent to paper documents for purposes of both filing and discovery.[156] The subject matter held in digital documents and communications is at least as extensive and intimate as what was held on paper records at the Framing, and probably much more so.[157] The storage of documents on media other than paper changes nothing about their Fourth Amendment significance. The same information about each American's life that once resided on paper and similar media in attics, garages, workshops, master bedrooms, sewing rooms, and desk drawers,[158] now resides, digitized, in cell phones and similar electronic devices.

Courts should explicitly recognize digital representations of information as constitutional "papers and effects" whose security against unreasonable seizure is protected by the Fourth Amendment. (To those for whom literalism is at a premium, the

---

[153] *Id*. at 176-77. The trial court's ruling in that case shows how "reasonable expectation of privacy" doctrine pulls courts away from the text of the Fourth Amendment. Applying the doctrine, it found that Oliver had a reasonable expectation that a field a mile from his home would remain private because he "had done all that could be expected of him to assert his privacy in the area of farm that was searched." *Id*. at 173.

[154] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805, 854 (2016).

[155] *See* United States v. Seljan, 547 F.3d 993, 1014-17 (9th Cir. 2008) (Kozinski, J., dissenting), *cert. denied*, 129 S. Ct. 1368 (2009) ("What makes papers special—and the reason why they are listed alongside houses, persons and effects—is the ideas they embody, ideas that can only be seized by reading the words on the page.").

[156] *See* Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee 2, 18-22 (May 27, 2005), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV5-2005.pdf.

[157] *See* Mary Czerwinski et al., *Digital Memories in an Era of Ubiquitous Computing and Abundant Storage, Communications of the ACM*, at 45 (Jan. 2006), http://research.microsoft.com/pubs/79673/CACMJan2006DigitalMemories.pdf.

[158] *Cf. Chimel*, 395 U.S. at 754.

word "effects" has far less connotation of tangible objects than "papers," and the two can be used interchangeably.[159]) The coverage of the Fourth Amendment must extend to these media if the Court is to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[160]

At least one lower court has found constitutional protection for email clearly enough to rely on its premise that email represents a paper or effect. In *United States v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit wrote: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail."[161]

Many cases explore the category of "effects," though often tacitly. A car is an effect.[162] A cell phone is an effect.[163] So are containers[164] and packages, both when held by a person and entrusted to private carriers.[165]

The Court did not say so explicitly in *Katz*, but it treated the sound of Katz's voice, suitably shrouded, as a constitutionally protected item. Not reduced to a tangible medium of expression, it is hard to treat it as a constitutional "paper." But sound is a natural information conveyance equivalent to made items like paper and other tangible things. The best understanding of *Katz* consistent with the text of the Fourth Amendment is that a whisper or shrouded oral communication is an "effect" or what might be called "personal curtilage."[166] When people's digital items produce personal data, that data may be part of a "virtual curtilage."[167]

The Fourth Amendment uses the possessive pronoun "their," which places boundaries around the items in which a person may assert a right against unreasonable seizure or search. Resorting to "positive law" analysis solves most problems in this area. If police arriving at a doorway are rebuffed by a sole occupant with apparent authority to permit or deny ingress, the apartment is "his" or "hers," as the case may be, and the

[159] During the framing of the Fourth Amendment, the Committee of Eleven changed Madison's language protecting "persons, houses, papers, and other property," to "persons, houses, papers, and effects," arguably broadening the scope of the items protected. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1301 (2016).
[160] *Kyllo*, 533 U.S. at 34.
[161] 631 F.3d 266, 285-86 (6th Cir. 2010).
[162] *Jones*, 132 S. Ct. at 953; Cady v. Dombrowski, 413 U.S. 433, 439 (1973); Brinegar v. United States, 338 U.S. 160, 182 (1949).
[163] *Riley*, 134 S. Ct. at 2485.
[164] Florida v. Jimeno, 500 U.S. 248 (1980).
[165] Walter v. United States, 447 U.S. 649, 654 (1980), Ex Parte Jackson, 96 U.S. 727, 733 (1877); United States v. Jacobsen, 466 U.S. 109, 114 (1984).
[166] Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283 (2014).
[167] *See* Ferguson, *supra* note 154.

police may not enter without permission or probable cause and a warrant.[168] A bailee's car is "his" for Fourth Amendment purposes.[169]

Whatever the case, if a constitutionally protected item was searched or seized, the final question is whether that was reasonable. In "reasonable expectation of privacy" doctrine, the analysis is collapsed: A search is almost always unreasonable without a warrant. But the more methodical analysis allows for such a thing as a reasonable search or seizure.

Was the seizure or search reasonable?

When constitutionally protected items have been seized or searched, the Fourth Amendment calls for examining the reasonableness of government agents' actions in doing so. This is where the judging should occur.

The question does not go to the reasonableness of privacy expectations, of course, but to the reasonableness of government agents' actions. And it has less to do with the ordinary sensibilities of decent people, as modern usage would suggest. According to Professor Laura Donohue, the word "unreasonable" in antecedents to the Fourth Amendment and the amendment itself "conveyed a particular meaning: namely, against reason, or against the reason of the common law."[170] "That which was consistent with the common law was reasonable and, therefore, legal. That which was inconsistent was unreasonable and, ipso facto, illegal."[171]

The boundaries laid out by "positive law" are excellent guides to what is reasonable.[172] Common law, statutes, and regulations delimit what people can and cannot do in general—ordinary people and government agents alike. Searching or seizing that falls within these bounds would almost always be constitutionally reasonable. But a seizure or search that would be a civil or criminal wrong under ordinary circumstances must occur only after the second-thought and third-party review provided by the warrant application process. The *Olmstead* Court would have done well to heed the Washington state law that made it a misdemeanor to intercept messages sent by telegraph or telephone.[173]

To serve well, the reasonableness analysis must allow for reasonable seizure and reasonable search. Imagine a law enforcement officer walking down the street. She trips

---

[168] *See* United States v. Matlock, 415 U.S. 164 (1974).
[169] *Jones*, 132 S. Ct. at 949 n. 2.
[170] Donohue, *supra* note 159, at 1270.
[171] *Id*. at 1270-71.
[172] *See* William Baude & James Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016). Baude and Stern treat "positive law" as defining the contours of search, but it may better delimit reasonableness. *But see* Kiel Brennan-Marquez and Andrew Tutt, *Offensive Searches*, ___ HAR . CIV. RIGHTS-CIV. LIBERTIES L. REV. ___, ___ (forthcoming) (arguing that the Court has repeatedly rejected positive law).
[173] REMINGTON COMPILED STAT., § 2656-18 (1922); *see Olmstead*, 277 U.S. at 480 (Brandeis, J., dissenting).

on a crack in the sidewalk and reaches out to steady herself on a nearby automobile, leaving a noticeable smudge. For an instant, she converted the car to her purposes, in a small but real seizure of another's private property.[174]

An instinct in such a case may be to say, "that was no seizure." But recall the government's argument in *Terry* to exclude "stop and frisk" from Fourth Amendment examination, which the Court rejected. The better way to think of steadying oneself on a car is as an entirely reasonable seizure. It creates no action for trespass and it doesn't violate any statute or regulation, nor does the practice in context invade the security of people's cars. Were the officer to have converted the car to her purposes in a different way—attaching a GPS device to it, for example, so as to track its movements—this creepy behavior, recognized as illegal stalking in many states,[175] is not reasonable without a warrant supported by probable cause.

The same goes for reasonable searching. Say our law enforcement officer is at the beach. Espying odd behavior—maybe an incipient fist-fight—off in the direction of the wharf, she raises her binoculars to her eyes and looks at what is happening there.[176] That kind of directed looking may qualify as a search, but the existence of something "odd" and her use of a relatively ordinary technology place the search well within the bounds of reasonableness. In a second scenario, where a government agent sets up on a bluff and uses a military-grade instrument to read over a beachgoer's shoulder, that seems to be unreasonable searching. It is an arguable invasion of the intrusion on seclusion branch of the common law privacy right.

Allowing for reasonable seizures and searches could invite all the outcome-determinativeness that people rightly deplore in "reasonable expectation" cases, but courts should be better able to resist outcome-determinacy using this analysis. "Reasonable expectation" doctrine asks if it was reasonable to expect privacy in the thing found. When the thing found is illegal drugs or guns, the answer is almost always "no." But in this analysis, the focus is as it should be, on the actions of government agents. Courts will better analyze the abstract behavior without reference to what it turns up. They should be cautioned against reasoning backward, of course, and it will be fairly obvious when they do.

There is no replacing the need for judging in close Fourth Amendment cases. But examining the reasonableness of seizures and searches is the better way to administer the Fourth Amendment than the untethered guesstimation called for by the "reasonable expectation of privacy" test. Courts should use the ordinary meanings of the words in the Fourth Amendment and employ relatively familiar and settled property, contract, and tort concepts, as well as statute and regulation. They should strike balances based on the facts in individual cases rather than by making sweeping pronouncements about privacy.

---

[174] The question whether a seizure occurred is objective and has no relation to the intention of the actor.
[175] *See* Ashley N. B. Beagle, *Modern Stalking Laws: A Survey of State Anti-Stalking Statutes Considering Modern Mediums and Constitutional Challenges*, 14 CHAP. L. REV. 457 (Winter 2011).
[176] In contrast to seizure, searching is subjective. It turns on the actor's purpose of finding something.

To recap, the methodology required for sound administration of the Fourth Amendment asks:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?

A recent Tenth Circuit opinion written by Judge Neil Gorsuch exhibits how that methodology can sharpen a court's reasoning.

United States v. Ackerman[177] dealt with the Fourth Amendment's application to an email that AOL had forwarded to the National Center for Missing and Exploited Children's (NCMEC) "CyberTipline" and opened by that group. Having found that NCMEC was a state actor, Judge Gorsuch began his consideration of the Fourth Amendment issues by applying key elements of its text: "No one in this appeal disputes that an email is a 'paper' or 'effect' for Fourth Amendment purposes . . . . The undisputed facts show, too, that NCMEC opened Mr. Ackerman's email, found four attachments, and proceeded to view each of them. And that sort of rummaging through private papers or effects would seem pretty obviously a 'search.'"[178]

In addition to a "reasonable expectations" analysis, Judge Gorsuch considered reasonableness in light of longstanding common law concepts. Opening and examining private correspondence "seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment," he wrote. "Of course, the framers were concerned with the protection of physical rather than virtual correspondence. But a more obvious analogy from principle to new technology is hard to imagine."[179]

Opening an email is a search of it. An email is a "paper" or "effect." Searching it without a warrant is unreasonable according to common law principles. Courts may benefit from this straightforward mode of Fourth Amendment reasoning for years to come.

Conclusion

In part, the failure of courts to administer the Fourth Amendment well can be laid at the door of the general legal environment, which does not yet comprehend communications and data very well. Our entry into the Information Age demands a new, higher respect for data, information, and communications as common law property. The Fourth Amendment and society generally will benefit from legal development in this area, which would parallel legal advances of the past.

[177] 831 F.3d 1292 (10th Cir. 2016).
[178] *Id*. at 1304 (citations omitted).
[179] *Id*. at 1307-08 (citations omitted).

In feudal times, prior to the development of trade and commerce, personal property was not well recognized by the law. It was treated something like communications and data are treated now. William Blackstone, writing in his famous *Commentaries on the Laws of England*, remarked that ordinary possessions were "not esteemed of so high a nature, nor paid so much regard to by the law, as things that are in their nature more permanent and immoveable, as lands, and houses, and the profits issuing thereout." But when changes in technology and society allowed people to travel and engage in commerce with increasingly valuable movable goods, that necessitated expanded legal recognition for personalty "in a light nearly, if not quite, equal to" realty.[180]

Benjamin Constant described in his classic speech, *The Liberty of the Ancients Compared with the Moderns*,[181] how important rights in personal property were to the development of liberty. Feudal times allowed for hereditary rule and hereditary subservience because an owner of land could grant only the right to use property, or "usufruct," to his subjects—not ownership. Property rights in movables emancipated the peon by allowing him to acquire wealth that was portable and, through wealth, a measure of independence.[182]

By the time of the American Founding, of course, "papers" and "effects" were well-established articles of property. They were used commonly enough and recognized as high-enough in value that the Framers of the Bill of Rights wrote their protection into the Fourth Amendment. The protection of these things as property helped form a nation conceived in liberty.

Today, we are seeing a rise of commerce in information and communications that parallels the growth of commerce in personalty hundreds of years ago. But the legal environment around information remains in a feudal era. Information goods have a low status, and the law is blasé about confiscation of communications and data in ways that are increasingly alarming to those who recognize the value of their data. With the growth of commerce in information, recognition of communications and information as a form of property would rebalance the relationship between the individual and the state.

Justice Butler laid the groundwork for establishing clearer Fourth Amendment rights with respect to information in his *Olmstead* dissent. Under contract with telephone companies, callers have the legal right to exclude others from their calls. The communications themselves belong to the parties between whom they pass.

When courts administer the Fourth Amendment, they should do so methodically, by examining whether there have been searches, which are invasions of any property

---

[180] 2 WILLIAM BLACKSTONE, COMMENTARIES ch. 24. *See also* ERIC JONES, THE EUROPEAN MIRACLE (3d. ed. 2003) (examining theories that might explain how personal property rights took hold).
[181] Benjamin Constant, *The Liberty of the Ancients Compared with the Moderns, in* CONSTANT: POLITICAL WRITINGS 307 (Biancamaria Fontana ed., 2010).
[182] "Commerce confers a new quality on property, circulation. Without circulation, property is merely a usufruct; political authority can always affect usufruct, because it can prevent its enjoyment; but circulation creates an invisible and invincible obstacle to the actions of social power." *Id.* at 324-25.

right, and searches, which are signaled by bringing exposure to concealed things or acting with a "purpose of finding something." If a seizure or search exists, the next step in the analysis is to determine whether it is of something that is protected by the Fourth Amendment: a person, house, paper, or effect. And if it is, the final question is whether the search or seizure was reasonable.

Crucially, this model puts courts in their familiar role of applying the law to the facts in cases that come before them. It does not require courts to make broad pronouncements about social mores, such as what are "reasonable expectations of privacy." This way of administering the Fourth Amendment would focus the analysis in Fourth Amendment on the reasonableness of government action rather than the reasonableness of private defendants' privacy preferences. And it would help the U.S. Supreme Court preserve the degree of privacy people enjoyed at the time of the Framing.

Modest Justice Pierce Butler is owed a revival, and perhaps a place in history next to Holmes, Cardozo, and Brandeis. He bequeathed us some very helpful *ratio dissensi*.