From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies

Ric Simmons

Follow this and additional works at: https://repository.uchastings.edu/hastings_law_journal

Recommended Citation
Ric Simmons, From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies, 53 HASTINGS L.J. 1303 (2002).
Available at: https://repository.uchastings.edu/hastings_law_journal/vol53/iss6/2

This Article is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Law Journal by an authorized editor of UC Hastings Scholarship Repository.
From *Katz* to *Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies

*by*

RIC SIMMONS*

**Introduction**

In the late 1960's, the Supreme Court engineered a paradigm shift in Fourth Amendment law: instead of focusing solely on property interests in determining whether or not a "search" had occurred, the Court broadened the scope of the Amendment's protection to include any activity in which an individual has a "reasonable expectation of privacy." In *United States v. Katz*, which set out this new test, the Court cited numerous reasons for this shift.

---

* Acting Assistant Professor of Law, New York University School of Law. I would like to thank Peggy Davis, Karin Ciano, Kris Franklin, Justine Daniels, Amanda Wood, and the Lawyering Program at New York University School of Law for their feedback and support.

1. In the twisted parlance of Fourth Amendment jurisprudence, the key question is whether or not a "search" has taken place. Once there is a "search," it is presumptively "unreasonable" unless the government obtained a warrant or one of the numerous exceptions applies. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 32 (2001) ("One might think that the new validating public rationale would be that examining the portion of a house that is in plain public view, while it is a 'search' despite the absence of trespass, is not an 'unreasonable' one under the Fourth Amendment. But in fact we have held that visual observation is no 'search' at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.") (citations omitted). This article will generally use the word "search" in this narrower, technical sense—that is, meaning any government surveillance, observation, or examination pursuant to an investigation which implicates the Fourth Amendment. Generally, the article will use the term "surveillance" to describe government investigatory actions which have not been found to be a "search."


First, the Court noted that the location of a person's activity should not be the primary factor in determining whether or not the activity deserves Fourth Amendment protection: in modern society, many activities that formerly might have been able to take place in the privacy of our homes now take place in semi-public areas—thus the famous (if ultimately unhelpful) declaration that the Fourth Amendment "protects people, not places." 4 Second, the Court was beginning to realize that in an age where pure information was becoming more valuable as a commodity, the Fourth Amendment must protect private speech and conversations as well as more tangible possessions. 5 But primarily, the Court was acknowledging the fact that given the new technologies available in government investigations, a consideration of how the government agents (or their devices) carried out surveillance was no longer a meaningful factor. 6

4. Id. at 351. Justice Stewart further noted that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id. at 351-52. He later intimated that modern life involves engaging in private activities in many places outside the home: "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment." Id. at 352 (footnotes omitted). This shift in the nature of twentieth-century life was recognized by some members of the Court as far back as 1942, when Justice Murphy wrote that "[w]ith the passing of the years since 1787, marked changes have ensued in the ways of conducting business and personal affairs. Many transactions of a business or personal character that in the eighteenth century were conducted at home are now carried on in business offices away from the home." Goldman v. United States, 316 U.S. 129, 138 (1942) (Murphy, J., dissenting). As one commentator noted, social and economic changes mandated this shift in perspective:

In the eighteenth and nineteenth centuries, limitations upon police invasions of property interests offered adequate protection for a predominantly rural population whose lives and aspirations were largely confined within the physical limits of their property. That was no longer true of a twentieth-century population whose endeavors are rarely contiguous with its property holdings. Few [modern] Americans work on their own property or out of their homes. Minimal participation in modern life requires extensive contacts which take us beyond the four corners of our property.


5. This dramatic shift in Fourth Amendment law—holding that the Amendment protects intangible words as tangible items—occurred in two landmark 1967 cases: Berger, 388 U.S. at 51 ("[T]hat a conversation passing over a telephone wire cannot be said to come within the Fourth Amendment's enumeration of 'persons, houses, papers, and effects' ha[s] been negated by our subsequent cases as hereinafter noted.") and Katz, 389 U.S. at 353 ("[W]e have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any technical trespass under... local property law.") (citations omitted). Although both cases claimed that they were merely restating settled law, no court had held this to be true before Katz and Berger.

6. See, e.g., Katz, 389 U.S. at 353 ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and
For example, previous rulings had held that electronic eavesdropping with a "slap-mike" (which touched the outer surface of an adjoining wall but did not penetrate that wall) was permissible, while eavesdropping on the same conversation with a "spike-mike" (which penetrated through the adjoining wall to make contact with a sound-conducting element on the defendant's property) was not permissible. As investigative technology improved—resulting in, for example, parabolic microphones that could eavesdrop on a conversation from across the street—it became more and more clear that an inquiry as to the method in which law enforcement agents conducted the surveillance would do little to protect Fourth Amendment rights.

Increasingly over the past thirty years, however, this last aspect of the Katz test has been watered down or ignored. Subsequent courts have narrowly interpreted the Katz decision as merely a repudiation of the "trespass doctrine" of the previous forty years, which held that government surveillance was a "search" if and only if the law enforcement agents (or their devices) trespassed on the property interests of the defendant. This overly narrow interpretation is a result of the vague language of the test itself, which leads courts that are struggling to define the test to view Katz through the prism of the long history of "trespass doctrine" cases that came before it. Applying this narrow interpretation of Katz gives too little guidance to courts, and as they refine the test, results in a number of decisions (and, more ominously for future cases, a line of reasoning) that are inconsistent with the original broad intent of the Katz test. At the same time, further advances in technologies—both those used by criminals and those used by government investigators—have continued to alter the landscape of the real world, making adherence to the original intent behind the test even more critical.

As noted above, Katz actually stands for more than a mere repudiation of the trespass doctrine; rather than merely holding that the location of law enforcement agents (or their devices) is irrelevant, Katz stands for the broader proposition that the method used by the law enforcement agents is irrelevant. In adopting the language

7. See Goldman, 316 U.S. at 134-35 (finding no Fourth Amendment violation if "trespass did not aid materially in the use of the dictaphone" attached to a wall adjoining defendant's office).
8. See United States v. Silverman, 365 U.S. 505, 509 (1961) (finding that electronic eavesdropping that was accomplished by means of a "physical intrusion" of a spike-mike into defendant's wall was unconstitutional).
9. See, e.g., Olmstead v. United States, 277 U.S. 438 (1928), and other cases cited infra Part I.A.
"legitimate expectation of privacy," *Katz* was presenting a test that focused solely on the activity or information that was being monitored, without regard for how it might have been observed or acquired by the government.

This Article argues that courts should apply the *Katz* test as it was originally intended: a test which considers only the result of the search—the type of information that was acquired; and disregards altogether the method of the search—the action or conduct of the agent conducting the search. Although such a test would directly contradict a few subsequent cases that have interpreted the *Katz* standard, it is entirely consistent with the paradigm shift that the Court engineered in *Katz*. This argument is supported by a close textual reading of Justice Harlan's concurring opinion in *Katz* (which set out the "reasonable expectations" test) and is also consistent with much of the reasoning in case law from the hundred years prior to *Katz*. Furthermore, application of a purely "results-based" test is all the more necessary given the advances in technology that have occurred since that landmark case was decided over thirty years ago. Specifically, in the fields of computer crime (which did not exist at all thirty years ago), sense-enhancing technology (which existed in much cruder form), and binary or content-discriminating searches (which are soon to become a prominent and valuable tool for law enforcement), a continued adherence to a test that considers the method of search used by the government will result in the same inconsistencies that the Court observed in the electronic eavesdropping field, in which the constitutionality of a surveillance absurdly turned on whether the microphone "trespassed" into the defendant's wall. Perhaps more ominously, using the method of search as a factor in determining constitutionality will inevitably result—indeed, has already resulted—in a gradual weakening of Fourth Amendment protections as investigative technologies become more sophisticated.

Part I of this Article will analyze the "reasonable expectation of privacy" test set out in the *Katz* case by briefly tracing the history behind the test and then examining how the Court has applied the test since *Katz*. Part II will justify a "results-based" interpretation of the *Katz* test and place it in the context of the evolving case law on the subject. Part III will examine three specific methods of investigation: computer-assisted investigations (whether of

---

10. Most significantly, a reevaluation of *Katz* will require rejecting the rationale (though not necessarily the rule) of *Smith v. Maryland*, 442 U.S. 735 (1979), regarding the protection accorded to information "given" to third parties (see infra note 144-56 and accompanying text); and the rationale (and probably the rule) of *Bond v. United States*, 529 U.S. 334 (2000), on the relevance of the physical invasiveness of a search (see infra notes 61-67 and accompanying text).
cybercrime or more traditional crimes), sense-enhancing technology, and binary or content-discriminating searches, and demonstrate the ways in which improper applications of the Katz standard have resulted in holdings that are inconsistent with Katz's original purpose—and incompatible with technology in today's world.

I. The Katz Test: What Is a "Reasonable Expectation of Privacy?"

A. Pre-Katz: Where the Test Came From

In the landmark case of Katz v. United States,\(^\text{11}\) the Supreme Court reversed nearly a century of Fourth Amendment jurisprudence by declaring that property interests were no longer the controlling factor in determining whether or not a search has occurred.\(^\text{12}\) The majority opinion itself, however, did little to explain what would replace the old test;\(^\text{13}\) instead, Justice Harlan's concurrence has become the standard to which courts now turn: whether an alleged search violates an individual's "reasonable expectation of privacy."

\(^\text{11}\) 389 U.S. 347 (1967)
\(^\text{12}\) "It is true that the absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry, for that Amendment was thought to limit only searches and seizures of tangible property. But 'the premise that property interests control the right of the Government to search and seize property has been discredited.'"\(^\text{14}\) Id. at 352-53 (citations and footnotes omitted).
\(^\text{13}\) In deciding the case, Justice Stewart's majority opinion described very specific requirements with which the government must comply in order to legitimize electronic surveillance: for example, obtaining a warrant from a magistrate that met the requirements set out in two prior cases, Osborn v. United States, 385 U.S. 323 (1966), and Berger v. New York, 388 U.S. 41 (1967).\(^\text{15}\) Id. at 355-56. This guidance, however, was only helpful in what the government must be required to do once it is determined that a search has occurred. As far as determining whether or not a search has occurred in the first place, Justice Stewart provides little guidance, aside from noting that "[t]he government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."\(^\text{16}\) Id. at 353 (emphasis added). Harlan's concurrence picked up this language and fleshed out a more detailed test which could be applied in future cases. Some commentators have theorized that Stewart was intentionally vague about the new test in order to ensure a majority for a case that was radically altering Fourth Amendment law. See, e.g., Lewis R. Katz, supra note 4, at 559 ("Justice Stewart could express the Court's sense of principle in a remarkably facile way without forcing the other members of the Court to commit to specifics. In Katz he led the majority to reject property as the sole measure of fourth amendment protection without committing them to a privacy test for all future cases").
\(^\text{14}\) "My understanding of the rule that has emerged from prior decisions 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.'"\(^\text{17}\) Katz, 389 U.S. at 361 (Harlan, J., concurring).
As is usually the case with new legal standards, even those that represent seismic shifts in the law such as the one \textit{Katz} heralded, this new test was not constructed from scratch. The term “reasonable” comes from the language of the Fourth Amendment itself,\textsuperscript{15} and thus it is unsurprising that many previous Fourth Amendment cases turned on whether or not the defendant could reasonably believe that his or her conduct was considered private. In 1928, the Supreme Court considered its first wiretapping case in \textit{Olmstead v. United States},\textsuperscript{16} and a reader of the opinion could be forgiven for believing that the Court was in fact applying the \textit{Katz} test some forty years before it was officially set out:

The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.\textsuperscript{17}

In other words, according to the majority in \textit{Olmstead}, someone who uses a “telephone instrument” to knowingly project his or her voice across the outside world into another’s home has waived his or her right to privacy in the content of the communication. As we shall see, this argument is a recurring theme in Fourth Amendment jurisprudence in the realm of technology. For example, over sixty years after \textit{Olmstead} the Court was forced to consider whether a knowing release of heat waves out of a house into the outside world represented an implicit waiver of the right to keep the heat patterns inside your house confidential.\textsuperscript{18}

But more significant is the fact that the \textit{Olmstead} Court implied a “reasonable expectations of privacy” test—or perhaps a less formal precursor thereof—and then found that individuals did \textit{not} have a reasonable expectation of privacy in the content of their phone calls. This is primarily because, as noted above, the Court’s conception of what is reasonably private was tied very closely to notions of property

\begin{footnotesize}
\begin{enumerate}
\item The Fourth Amendment reads:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by an Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

\textit{U.S. Const.} amend. IV.
\item 277 U.S. 438 (1928).
\item \textit{Id.} at 466.
\item \textit{See} \textit{Kyllo v. United States}, 533 U.S. 27, 43-44, 121 (2001) (Stevens, J., dissenting) ("Heat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building.")
\end{enumerate}
\end{footnotesize}
rights—note the determinative last sentence: “those who intercepted the projected voices were not in the house of either party to the conversation.” Thus, in determining what degree of privacy was “reasonable,” the Olmstead Court looked first and foremost at the location of the government observers, and since their method of search did not involve a trespass into an area considered to be private, the search they conducted with the wiretap was permissible.

In this way, Olmstead saw this early “reasonable expectations” test give birth to the “property rights” test. The concept that society’s reasonable expectations are best determined by examining property rights was not self-evident; Olmstead represented only a five-member majority, with Justice Brandeis and even the usually strict-constructionist Holmes writing strong dissents.9 Furthermore, six years later, Congress demonstrated its disagreement with Olmstead’s conclusion that people should have no “reasonable expectation” of privacy in their telephone conversations by passing the Federal Communications Act of 1934, which prohibited intercepting and disclosing any information passing over telephone lines.20

Unfortunately, in subsequent cases the Supreme Court allowed the “property rights” offspring to devour its “reasonable expectations” parent whole. This may have been inevitable: a “property rights” test was far easier to apply than an amorphous “reasonableness” standard, and seemed to comport well with the Fourth Amendment’s language describing a person’s “houses, papers, and effects” as being protected from unreasonable searches.21 Thus, in its next major Fourth Amendment case involving technology, the Court had little patience for a defendant who attempted to rely on society’s expectations of privacy. In Goldman v. United States,22 federal agents placed a dictaphone against the wall of an adjoining office to listen to the defendant’s conversations on the other side. Even though the device could pick up conversations that were not projected to the outside world through telephone wires, the Court held that Olmstead’s property-rights test controlled, primarily due to administrative simplicity in applying such a bright-line rule:23

---

9. Olmstead, 277 U.S. at 469-485. Both Holmes and Brandeis seemed most concerned that the government, though not trespassing when conducting the wiretap, was in fact violating state law. Id.


21. U.S. CONST. amend. IV.

22. 316 U.S. 129 (1942).

23. In the facts of Goldman, the conversation that was overheard by the government with the dictaphone was, in fact, a telephone conversation, but the opinion makes clear that this fact had no bearing on the admissibility of the search. In fact, the Court rejected
[Defendants argue that] the *Olmstead* case dealt with the tapping of telephone wires, and the court adverted to the fact that, in using a telephone, the speaker projects his voice beyond the confines of his home or office and, therefore, assumes the risk that his message may be intercepted. It is urged that where, as in the present case, one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone's use of a delicate detector in the next room. We think, however, the distinction is too nice for practical application of the Constitutional guarantee, and no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the *Olmstead* case.\(^{24}\)

To modern minds, this reasoning strikes us as wrong for a number of reasons; foremost among them being that it supports a holding which denies Fourth Amendment protection to any conversation in our offices and potentially even our homes. The almost casual rejection of the "reasonableness" test from *Olmstead* also seems improper: if the *Olmstead* holding were based on a theory—however misguided—that we have no reasonable expectation of privacy in conversations which we "release" to the public by sending them out on wires into the world, how could it support eavesdropping on a private conversation in an office? But perhaps a deeper explanation as to why this reasoning offends modern sensibilities is its ultimate reliance on the government's conduct—the last line compares the activities of the government agents in *Olmstead* with those in *Goldman* and finds them comparable, and on this basis the Court finds no "logical or reasonable distinction" between the two cases. This focus on the activity of the government actor rather than on the nature of the information received seems outdated in modern times, when information is frequently the most valuable commodity a person possesses, and when government agents can intercept or acquire private information with minimally intrusive technologies—thus achieving a very intimate invasion of privacy with relatively non-offensive activity.

---

the defendant's argument that his conversation was protected by the Federal Communications Act that effectively overruled *Olmstead*'s wiretapping holding:

[w]ords spoken in a room in the presence of another into a telephone receiver do not constitute a communication by wire within the meaning of the [Act]. . . . The listening in the next room to the words of [defendant] as he talked into the telephone receiver was no more the interception of a wire communication, within the meaning of the Act, than would have been the overhearing of the conversation by one sitting in the same room.

*Id.* at 133-34.

24. *Id.* at 135.
This triumph of formalism over realism reached its peak in *United States v. Silverman*, in which the Court ruled that essentially the identical kind of eavesdropping that was approved in *Goldman* was unconstitutional if the microphone that was used did not merely rest on the outside of an adjoining wall, but actually penetrated through the wall a few inches to make contact with the property of the defendant. As in *Goldman*, the only relevant factor considered by the Court in *Silverman* was the method of search used by the government: "This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard."

Of course, the Court had essentially held this to be permissible eighteen years earlier in *Goldman*, but their formalist test looked only to *where* the government was and *what* it was doing rather than the functional result of the search.

But all of this changed after *Katz*—or at least, it began to change. In *Katz*, FBI agents attached an electronic listening device to the outside of a public telephone booth—an action that could not possibly offend anyone's property rights. In the words of the majority opinion, *Katz* rejected the formalist "trespass" doctrine, and shifted the focus of the Fourth Amendment inquiry from "places" to "people." Given this language—and the sparseness of other guidance in the majority opinion—some courts have held that what *Katz* was rejecting was an emphasis on the location of the law enforcement officer (or the officer's device) in determining the constitutionality of a search.

But Harlan's standard-setting concurrence implies that *Katz* was not really about rejecting the "place-based" analysis; in fact, Harlan quickly pointed out that although the Fourth Amendment protects "people, not places," the protection it affords to people generally

---

26. Id. at 512.
27. Id. at 511-12. In order to further emphasize that the action taken by the government was the primary factor in determining that an unreasonable search occurred, the Court then declared that its opinion was "based upon the reality of an actual intrusion into a constitutionally protected area." Id. at 512.
29. Id. at 353 ("[T]he 'trespass' doctrine [of *Olmstead* and *Goldman*] can no longer be regarded as controlling.").
30. Id. at 351 ("[T]he Fourth Amendment protects people, not places.").
31. See, e.g., *Rakas* v. *Illinois*, 439 U.S. 128, 144 n.12 (1978) ("Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest. These ideas were rejected both in *Jones* and in *Katz*.") (internal citations omitted).
"requires reference to a 'place.'" This phrase sits somewhat awkwardly alongside the majority opinion and makes it more difficult to give meaning to the vague "reasonable expectations of privacy" test.

Harlan's concurrence, if examined closely, resolves this ambiguity. In it he attempts to focus future courts squarely—if not solely—on the location or information sought to be protected and the actions taken by the defendant to protect that location or information. The few sentences in which he defines the contours of what "reasonable expectation of privacy" means describe only the actions taken by the person being observed or the information being acquired, not the methods used by the government. Harlan describes activities in a person's home as deserving protection, while "objects, activities, or statements" that are exposed to the "'plain view' of outsiders" are not protected. Harlan states that the "critical fact" in deciding 

\textit{Katz} was the action taken by the defendant in shutting the phone booth door behind himself and paying for a phone call—a dramatic reversal from \textit{Goldman} and \textit{Silverman}, whose only criteria were the actions taken by the government agents. And he concludes his analysis by noting that the old standard of focusing on the "physical penetration" of the defendant's premises was "bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."

\section*{B. Post-\textit{Katz}: Does the Method of Search Matter?}

In the end, both the majority opinion and Harlan's explanation of the phrase "reasonable expectation of privacy" were sufficiently meager that the task inevitably fell to future courts to define the phrase more fully. Although many courts properly refused to consider the method of surveillance used by law enforcement, others have continued to consider the method as a factor, even though Harlan's concurrence implies that it was this consideration—and not a "place-based analysis,"—which was the true evil that \textit{Katz} had set out to dispel.

Very early on it became clear that the "subjective" prong of the test—that is, whether or not defendants believed that they had an expectation of privacy—was meaningless, for two reasons. First, the defendants would almost never have been carrying out the illicit activity or keeping the incriminating evidence in the first place if they

\footnotesize{32. \textit{Katz}, 389 U.S. at 361 (Harlan, J., concurring).}

\footnotesize{33. \textit{Id.}}

\footnotesize{34. \textit{Id.}}

\footnotesize{35. \textit{Id.} at 362.}
did not believe that they were doing so in private. But more importantly, a defendant's subjective expectation of what is and is not private can too easily be manipulated by the government itself, as noted by Justice Marshall: "[L]aw enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such situations." The majority in Smith v. Maryland acknowledged this problem in a footnote, saying there may be circumstances—such as a refugee from a totalitarian country erroneously assuming the police were monitoring all of his phone conversations—in which "an individual's expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms." The Court stated that if such a conflict did occur between a person's subjective expectations and well-recognized Fourth Amendment doctrine, "those subjective expectations obviously could play no meaningful role in ascertaining what the scope of the Fourth Amendment was." In other words, if the subjective prong and the objective prong of the test conflict, the objective prong will control—which means, of course, that the subjective prong might as well not exist. Harlan himself seemed to recognize this a few years later, when he wrote that in applying the test courts must "transcend the search for subjective expectation" and instead focus on the "desirability of saddling [those expectations] upon society."

36. See, e.g., United States v. Nerber, 222 F.3d 597, 603 (9th Cir. 2000) ("In addition to closing the door [and] drawing the blinds . . . defendants ingested cocaine and brandished weapons in a way they clearly would not have done had they thought outsiders might see them."). In many cases the Court concedes that the defendant had a subjective expectation of privacy, but merely mentions this fact in a cursory fashion before proceeding to the objective prong of the test. See, e.g., California v. Greenwood:

   It may well be that respondents did not expect that the contents of their garbage bags would become known to the police or other members of the public. An expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable.

486 U.S. 35, 39-40 (1988). A notable exception is the case of Smith v. Maryland, 442 U.S. 735, 743 (1979) ("Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.")

38. 442 U.S. 735.
39. Id. at 740 n.5.
40. Id.
Thus, in applying the *Katz* test a court’s sole purpose is to determine what expectations of privacy society deems to be reasonable. In interpreting this language from *Katz*, the Supreme Court has informed us that merely relying on existing Fourth Amendment cases would result in a useless tautology: "[l]egitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." This continued emphasis on property law again demonstrates that, notwithstanding the famous "people, not places" language in the majority opinion, many courts properly reject the idea that *Katz* supplanted a "place-based" analysis, since the location of the search and the defendant’s relationship to that location are still a significant factor in determining whether or not the search was valid. These courts focus on the nature of the place, object, or activity being searched, essentially ignoring the method of search used by the government.

Indeed, numerous Supreme Court cases follow a purely “results-based” *Katz* test. In *Oliver v. United States*, the Court identified three factors as part of the *Katz* test: “the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.” The Court then applied these standards and concluded that society had no “reasonable expectation of privacy” in marijuana that was growing on an open field on a defendant’s property. Although the dissent objected to the rather egregious actions by the government agents in *Oliver*—walking around a locked gate with a “No Trespassing” sign attached to it, an action which would clearly expose a private party to criminal liability—the majority decided that the government activity itself was irrelevant. Instead, the Court held that “[t]here is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields.” The Court further noted that the fields could easily be seen by airplanes flying overhead,
implying that the fact that the government chose a different method of investigation in this case was immaterial.48

In California v. Greenwood,49 the Court applied the language from Oliver to conclude that “society as a whole possesses no such understanding [of privacy] with regard to garbage left for collection at the side of the street.”50 As in Oliver, the dissent focused—at least in part—on the action by the government agent: “Every week for two months, and at least once more a month later, the Laguna Beach police clawed through [defendant’s] trash....”51 The dissent later argued that “[m]ost of us... would be incensed to discover a meddler—whether a neighbor, a reporter, or a detective—scrutinizing our sealed trash containers to discover some detail of our personal lives.”52 But the majority instead focused on the items being searched as well as the actions taken by the defendants: “[D]eposit[ing] their garbage in an area particularly suited for public inspection and, in a manner of speaking,... for the express purpose of having strangers take it, respondents could have no reasonable expectation of privacy in the inculpatory items that they discarded.”53

Unfortunately, the case law is far from consistent in applying a test that considers only the result of the surveillance. Throughout various applications of the Katz test, the method of surveillance continues to survive as a factor in determining whether or not a defendant had a reasonable expectation of privacy. A recent American Bar Association task force isolated seven factors that courts apply in determining whether or not a physical surveillance is a search, and four of the seven related directly to the method used by the government: the degree of physical intrusion of the search, the availability of the technology used to the public, the extent to which the technology used enhances the natural senses, and the extent to which surveillance is unnecessarily intrusive.54

Specific examples from the case law include the “flyover” cases, in which the Court has held that observing or taking pictures of

48. Id.
50. Id. at 43-44.
51. Id. at 45 (Brennan, J., dissenting).
52. Id. at 51 (Brennan, J., dissenting).
53. Id. at 40-41 (internal quotations and citations omitted).
54. See Christopher Slobogin, Technology-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards, 10 HARV. J. L. & TECH. 383, 390-398 (1997). The other three factors, which are consistent with the language and spirit of the Katz test, were the nature of the place observed, the steps taken by the defendant to enhance privacy, and the nature of the object or activity observed. Id. The task force criticizes five of these seven standards, concluding that only the nature of the place observed and the amount of unnecessary intrusion are “central to any analysis of physical surveillance technology.” Id. at 398.
activities or items from an airplane does not constitute a "search"—regardless of the area being observed—since there is no "physical entry" onto the defendant's property.\textsuperscript{55} For example, in \textit{California v. Ciraolo},\textsuperscript{56} the Court held that observations from an airplane are not a "search" since they are made in a "physically nonintrusive" manner. Later, in \textit{Florida v. Riley},\textsuperscript{57} a plurality held that government agents observing the defendant's property from a helicopter 400 feet above the ground was not a search, noting that "[w]e would have a different case if flying at that altitude had been contrary to law or regulation,"\textsuperscript{58} and declared that it was "of obvious importance that the helicopter in this case was \textit{not} violating the law."\textsuperscript{59}

Until quite recently, a methods-based test was also applied to searches involving so-called "sense-enhancing" technologies, such as heat detectors or telescopic lenses on cameras, although the \textit{Kyllo} case, discussed below, now calls that into question.\textsuperscript{60}

\begin{itemize}
  \item 476 U.S. 207 (1986).
  \item \textit{Id.} at 451.
  \item \textit{Id.} Justice O'Connor's concurrence refers back to \textit{Katz} and appropriately argues that the correct inquiry centered on the amount of privacy society was prepared to give to the location in question, not the method used to observe the location:
  \begin{itemize}
    \item In determining whether [defendant] had a reasonable expectation of privacy from aerial observation, the relevant inquiry . . . is not whether the helicopter was where it had a right to be under FAA regulations. Rather, consistent with \textit{Katz}, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that [defendant]'s expectation of privacy was not "one that society is prepared to recognize as 'reasonable'."
  \end{itemize}
  \item \textit{Id.} at 454 (O'Connor, J., concurring) (quoting from \textit{Katz}) (citation omitted). The dissent agrees with O'Connor on this point, claiming that the plurality "reads almost as if \textit{Katz} had never been decided." \textit{Id.} at 456 (Brennan, J., dissenting) (citation omitted). The dissent disagrees with O'Connor only on the "empirical matter" of whether the public actually did fly over defendant's property at such a low altitude often enough to render defendant's expectation of privacy unreasonable. \textit{Id.} at 464-65. The distinction between developing a new technology that allows the government to search intimate areas in a less physically invasive manner (such as a thermal imager or a parabolic microphone) and a technology becoming widely accepted in society so as to alter what is a reasonable expectation of privacy (such as observations with flashlights or from high-flying aircraft) is a subtle but immensely significant one; \textit{see infra} notes, 129-42 and accompanying text.
  \item As explained by the American Bar Association report, \textit{supra} note 54, some courts have tried to distinguish between "devices that 'improve' the human senses [like binoculars, flashlights, and telephoto lenses] and devices that 'replace' them [such as heat-sensing technology or x-ray machines]." Courts as a rule will be more likely to accept a search made with a "sense-improving" technology than a "sense-replacing" technology. \textit{Compare} United States v. Whaley, 779 F.2d 585 (11th Cir. 1986) (use of binoculars not a search) and \textit{Texas v. Brown}, 460 U.S. 730 (1983) (use of flashlight not a search) \textit{with} United States v. Thomas, 757 F.2d 1359 (2d. Cir. 1985) (trained dog is a search) and United States v. Knotts, 460 U.S. 276 (1983) (electronic tracer would be a search if it
Two recent Supreme Court decisions highlight the growing tension in Fourth Amendment jurisprudence on this question. In *Bond v. United States*, the Court focused on the method of search employed by the government to conclude that a government agent squeezing a piece of luggage in an overhead compartment constituted a "search" under the Fourth Amendment. More recently, in *Kyllo v. United States*, the Court held that the use of a thermal imager to detect patterns of heat emanating from a home also constituted a "search" even though the method of search was non-invasive.

In *Bond*, the defendant was travelling on a bus which passed through a border patrol checkpoint, and a federal customs agent boarded the bus to check the immigration status of its passengers. After ensuring that the passengers were all legally in the country, the agent walked up to the front of the bus from the back, squeezing the soft luggage that the passengers had stored in the overhead rack. When the agent squeezed defendant's bag, he felt a hard, "brick-like" object; he then asked and received defendant's permission to open the bag and found a large brick of methamphetamine. The government argued that the defendant had exposed the contents of his bag to the public—or at least the way those contents felt—since he used a soft-sided bag and left it in an area where it would routinely (and foreseeably) be manipulated by other passengers. The Supreme Court disagreed, and distinguished the case from the "flyover" cases in which the defendants were found to have exposed the contents of their field to the public, solely on the basis of the method of search used by the government official: "[p]hysically invasive inspection is simply more intrusive than purely visual inspection." The dissent pointed out that this rationale would lead to "a constitutional jurisprudence of 'squeezes'," noting that the distinction between everyday handling and jostling of a piece of luggage and an "exploratory" manipulation of the bag was overly fine.

conveys information beyond what could be observed with the naked eye). As I argue below, the distinction between sense-improving and sense-replacing is a false dichotomy, and engaging in such a scientifically meaningless categorization is precisely the kind of fruitless exercise that is the natural result of focusing on the method of search. *See infra* notes 177-88, and accompanying text.

63. *Bond*, 529 U.S. at 335-36.
64. *Id* at 337.
65. *Id*.
66. *Id* at 342 (Breyer, J., dissenting).
67. As the dissent notes, everyday manipulation of baggage and "exploratory" manipulation of baggage differ quite clearly based on the *intent* of the individual doing the manipulating, but the Court had recently decided that the state of mind or intention of the
The *Bond* case also provides a good example of the semantic cheats that courts sometimes engage in when interpreting the *Katz* test; in this case using the word "intrusive" to mean (rather like Humpty Dumpty) what they want it to mean at different times. In fact the word has two quite different meanings in the context of the Fourth Amendment: (a) physical invasiveness or (b) degree of prying into private affairs. Under a results-based test, the second definition is a critical aspect of whether a surveillance is a search, while the first should be irrelevant. In the original *Katz* concurrence, there is no ambiguity: Justice Harlan was careful to specify that "physical intrusiveness" should no longer be the controlling factor in determining whether or not a search had occurred. Unfortunately subsequent courts have not been as careful to distinguish between physical intrusiveness and privacy intrusiveness.

*United States v. Nerber* provides a good example of this confusion. In considering the validity of covert video surveillance of the defendants in a hotel room after government informants left the room, the Ninth Circuit considered the "severity of the intrusion" to be critical. The court cited *Katz* for this proposition (which, being a case of electronic bugging, had no issue of physical invasiveness and thus obviously meant "intrusive" in the sense of invading privacy). The court then went on to cite *Bond* and *United States v. Place,* two cases in which the Court used "intrusive" in the sense of "physically invasive." *Nerber* then cited two video surveillance cases from other circuits, one of which compares video surveillance to the airplane surveillance in *Ciraolo,* which it described as "minimally-intrusive" and declared "[h]ere, unlike in *Ciraolo,* the government's intrusion is not minimal. It is not a one-time overhead flight or a glance over the government agent had no relevance in determining whether or not a search occurred. *Id.* at 342 (Breyer, J., dissenting) (citing Whren v. United States, 517 U.S. 806, 813 (1996)).

68. As noted infra notes 101-05, physical invasiveness can become relevant under the prohibition against seizures—that is, if a test is so invasive that it requires a suspect to stop and wait, or blood to be taken, etc.—then it may be an unconstitutional seizure. But that has nothing to do with whether or not a "search" has occurred.

69. *United States v. Katz,* 389 U.S. 347, 353 (1967) ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.") (emphasis added).

70. 222 F.3d 597 (9th Cir. 2000).

71. *Id.* at 601 ("[T]he legitimacy of a citizen's expectation of privacy in a particular place may be affected by the nature of the intrusion that occurs.").

72. Specifically the *Nerber* court quoted the portion of *Bond* which held that "[p]hysical inspection is simply more intrusive than purely visual inspection." *Id.* at 602 (citing *Bond v. United States,* 529 U.S. 334, 337 (2000)).

73. 462 U.S. 696 (1983) (in which the Supreme Court held that a dog sniffing luggage is not a “search” because it is "much less intrusive than a typical search").
fence by a passer-by"—again switching gears by citing cases which used the term "intrusive" in the privacy-invasive sense. The Nerber court concluded that "[t]he sweeping, indiscriminate manner in which video surveillance can intrude upon us, regardless of where we are, dictates that its use be approved only in limited circumstances." How the physical invasiveness factors that were considered in Bond and Place contributed to this conclusion—aside from the fact that they more or less by coincidence used the same term as the highly relevant video surveillance and flyover precedents—remains a mystery.

Of course, there is more at work than mere semantic sloppiness, especially given the Court's recent unambiguous re-affirmance of the "physical invasiveness" factor in Bond. But overall, the tendency of courts to use the term "intrusive" to apply to both physical invasiveness and degree of prying into private affairs helps to explain why the former has survived so tenaciously as a factor in the Katz test.

If Bond represents the most recent incarnation of the "methods-based" test, Kyllo v. United States, decided one year later, is perhaps the strongest affirmation so far of the "results-based" test. In Kyllo, government agents suspected the defendant was using high-intensity heat lamps to grow marijuana in his home. In order to confirm their suspicion, they conducted a warrantless scan of the house using a thermal imager, a device which detects infrared radiation. The heat patterns detected by the imager provided further evidence that the defendant was using heat lamps, and the agents then acquired a warrant, searched the home, and found marijuana.

On the first round of appeals, the Ninth Circuit remanded the case for the District Court to determine the "intrusiveness of the thermal imaging device." As noted above, "intrusive" can mean either physical invasiveness or revealing of intimate information. The Ninth Circuit made it clear that they meant "intrusive" in the latter sense, since they were asking for a hearing to determine the "quality and the degree of detail of information that [the device] can glean." Thus, the trial court was instructed to focus on the results of the surveillance, to determine "whether, on the one extreme, this device

74. United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir, 1987) (quoted by Nerber, 222 F.3d at 602).
75. Nerber, 222 F.3d at 603 (emphasis added).
76. See supra notes 63-67 and accompanying text.
78. Id. See also United States v. Kyllo, 37 F.3d 526, 530 (9th Cir. 1994) ("We must have some factual basis for gauging the intrusiveness of the thermal imaging device . . . .")
79. See infra notes 68-76 and accompanying text.
80. Kyllo, 37 F.3d at 530.
can detect sexual activity in the bedroom, as Kyllo's expert suggests, or, at the other extreme, whether it can only detect hot spots where heat is escaping from a structure.\footnote{81}

The trial court responded by measuring the device's "intrusiveness" in both senses of the word: it reported that on the one hand, it "emits no rays or beams" and "cannot penetrate walls or windows;" and on the other, it "did not show any people or activity within the walls of the structure" and "no intimate details of the home were observed."\footnote{82} Unsurprisingly, the Ninth Circuit ignored the findings on physical invasiveness of the device (the method of the surveillance) and decided the case based only on the result of the search: the imager "did not expose any intimate details of Kyllo's life," but only "amorphous 'hot spots' on the roof and exterior wall," and the defendant had no reasonable expectation of privacy in such information.\footnote{83}

The Supreme Court reversed, but maintained (for the most part) the Ninth Circuit's focus on the type of information acquired. The Court first focused on the place being observed—the interior of the home—and noted that "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that \textit{exists}, and that is acknowledged to be \textit{reasonable}."\footnote{84} The Court then set out a results-based test for sense-enhancing technologies: if the use of the technology obtains information "that could not otherwise have been obtained without physical intrusion into a constitutionally protected area," a search has occurred.\footnote{85} Unfortunately, the Court also included a poorly phrased methods-based caveat to the test, adding "at least where (as here) the technology in question is not in general public use."\footnote{86}

\begin{footnotesize}
\begin{itemize}
\item \footnote{81}{\textit{Id.} at 530-31. The Ninth Circuit was thus not concerned with \textit{how} the thermal imager functioned, but simply what information it revealed; it needed details on "the device's ability to detect the shapes of heat-emitting objects inside a home." \textit{Id.}}
\item \footnote{82}{\textit{Kyllo}, 533 U.S. at 30.}
\item \footnote{83}{United States v. Kyllo, 190 F.3d 1041, 1047 (1999). The Court also noted, somewhat dubiously, that the defendant had not even shown a \textit{subjective} expectation of privacy (thus reviving the nearly-defunct first prong of the \textit{Katz} test), since he made no attempt to conceal the heat escaping from his home. \textit{Id.} at 1046. Thus, the Ninth Circuit's analysis of the subjective prong, like its analysis of the objective prong, was independent of the method of search used, focusing instead on the actions taken by the defendant to keep the information private.}
\item \footnote{84}{\textit{Id.} at 34 (emphasis in the original).}
\item \footnote{85}{\textit{Id.} (internal quotations and citation omitted).}
\item \footnote{86}{\textit{Id.} The dissent made the most headway in criticizing the majority's "not in general public use" caveat—noting that "the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available." \textit{Id.} at 47 (Stevens, J., dissenting). The dissent also questions how a court is supposed to determine whether or not a certain technology is in "general public use," noting that around 10,000 thermal imagers have been produced and that they are "readily available to the public." \textit{Id.} at n.5}
\end{itemize}
\end{footnotesize}
The four justices who dissented in *Kyllo* focused almost exclusively on the method of the search, declaring that there is "a distinction of constitutional magnitude between 'through-the-wall surveillance' and "off-the-wall" surveillance." The majority refuted this distinction by pointing out that "a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house," and stated that the Court had "rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth."

Thus, *Kyllo* interpreted the *Katz* test somewhat differently than the *Bond* opinion did just one term earlier, laying bare a growing dissonance in Fourth Amendment jurisprudence, and forcing courts to struggle with an increasingly significant question: to what extent should the method of investigation or surveillance used by the government—and specifically, its degree of invasiveness—be considered in evaluating whether a "search" has occurred?

II. Reviving *Katz* by Disregarding the Method of Search

A. Why the Method Should Not Matter

As noted above, this Article proposes a simple answer to this question: the method of surveillance should be irrelevant, and the

(Stevens, J., dissenting). Although the caveat may have been poorly worded, it is in fact a necessary element of the *Katz* test, since without it the Fourth Amendment would not be flexible enough to keep pace with legitimate changes in societal expectations of privacy brought on by technological changes. *See infra* Part II.C.

87. *Id.* at 41 (Stevens, J., dissenting). The dissent was also concerned with the type of information that was acquired, but it referred to the method of search in order to determine the confidentiality that the specific kind of information deserved. According to the dissent, "through-the-wall" technology "gives the observer or listener direct access to information in a private area," while "off-the-wall" technology only reveals "inferences in the public domain." *Id.* Later, the dissent argues that the thermal imager "did not penetrate the walls of the petitioner's home" and though it picked up "details of the home that were exposed to the public, it did not obtain any information regarding the interior of the home" *Id.* at 44 (Stevens, J., dissenting) (internal quotations and citations omitted). Of course, the imager did reveal information regarding the interior of the home—namely, that there were unusual amounts of heat being generated in certain areas—and the details that were revealed were only "exposed to the public" because the dissent effectively defined "exposed to the public" as any information that is detectable by "off-the-wall" technologies. Thus again we see the dissent using the method of the search to determine whether or not the information acquired was deserving of protection. *See also id.* at 42 ("[T]his case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home.").

88. *Id.* at 35.
results of the surveillance are all that should matter in determining whether an individual's reasonable expectation of privacy has been infringed. Thus, in applying the *Katz* test, courts should look only to the characteristics of the item or information being observed—it's location, its nature, and/or the actions taken by the defendant to conceal it.

The inconsistencies created by considering the method of search only multiply as technologies become more sophisticated and courts struggle to find the correct analogy for any given surveillance method employed by the government. In some cases, courts are forced to choose between equally plausible analogies in order to determine how the Fourth Amendment applies: is thermal imaging analogous to watching snow melt off a roof or is it more like using binoculars? Or perhaps it is most analogous to using a dog to detect the odor of illegal contraband? Is reading the content of an e-mail analogous to wiretapping a phone, or is it analogous to accessing a stored voicemail? Or perhaps reading the content of an e-mail is comparable to reading the content of regular mail? And frequently courts must stack analogy on top of analogy: if reading the content of an e-mail is analogous to wiretapping a phone, we need another analogy to determine whether the founders would think wiretapping violates the Fourth Amendment—is wiretapping a phone the equivalent of standing outside a window and listening to a private conversation, or is it more like standing inside the room listening to the conversation? These inquiries become less and less relevant.

---


90. See *Commonwealth v. Gindlesperger*, 743 A.2d 898, 907 (Pa. 1999) (Castille, J. dissenting) (arguing that thermal imaging is analogous to the use of binoculars because it merely "enhances that which can lawfully be observed." )

91. See, e.g., *Commonwealth v. Gindlesperger*, 706 A.2d 1216, 1220 (Pa. Super. 1997) (noting that the lower court analogized the thermal imager to police contraband and that the "dog sniff theory in relation to thermal imagers ha[s] been accepted by some courts and rejected by others."

92. See U.S. v. Maxwell, 45 MJ. 406, 417 (1996) ("[T]he technology used to communicate via e-mail is extraordinarily analogous to a telephone conversation. Indeed, e-mail is transmitted from one computer to another via telephone communication, either hard line or satellite.").

93. See, e.g., *id* at 417-18.

E-mail transmissions are not unlike other forms of modern communication. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause.

*Id.* at 417-18 (citations omitted). See also *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("E-mail is almost equivalent to sending a letter via the mails").
(and more and more metaphorical) as we move further into the realm of cyber-investigations and the use of devices that detect information that is invisible to the human ear or eye. The only relevant consideration is the result of the surveillance: what information does the government acquire as a result of making the observations?

This proposal might at first seem counter-intuitive, since the very thing that we are describing—a "search"—naturally leads one to think about the verb itself, i.e., the action or conduct of the government official. But in using the Fourth Amendment to strike a balance between individual privacy and a government's legitimate need to investigate a crime, we are not trying to prevent or restrict certain kinds of government conduct per se, but rather to keep certain items, locations, and/or pieces of information beyond the reach of government officials, regardless of the manner in which they are able to observe them.

It may also seem natural to consider the nature of the government's conduct because certain actions by the government seem so much more invasive and egregious than others: a full body frisk, for example, seems to be more objectionable than walking through a metal detector. Intuition would suggest that a meaningful

94. Sometimes courts are even forced to analogize in the other direction—for example, a recent district court judge proposed applying wiretapping standards to the interception of standard mail, since the two methods of surveillance have "certain similarities." "The search of [defendant's] mail represents, like a wiretap, the continuous interception of a stream of communication. The interception of numerous pieces of mail, like the interception of numerous communications on a wiretap, represents a series of seizures supported by a single showing of probable cause." United States v. Heatley, 1998 WL 691201, at *7 (S.D.N.Y. 1998).

Even less sophisticated technologies require courts that focus on the method to use strained analogies: a canine sniff, for example, has been held to be "far more analogous to an electronic 'bug' than to a flashlight," since a flashlight merely "augments" or enhances perception, while a canine sniff and an electronic bug "replaces" natural human perception. See Jones v. Latexo Indep. Sch. Dist., 499 F. Supp. 223, 233 (E.D. Tex. 1980); see also State v. Riley, 88 Ohio App. 3d 468, 474 (1993). This false dichotomy between "sense-enhancing" and "sense-replacing" searches will be discussed infra notes 177-88 and accompanying text.

95. That is, beyond their reach unless a neutral magistrate has issued a warrant allowing the government to seek such information, or unless one of the exceptions to the warrant requirement applies.

96. See, e.g., Camara v. Mun. Court, 387 U.S. 523, 528 (1967) ("The basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.").

97. Compare Terry v. Ohio, 392 U.S. 1, 17 (1968) ("[A body frisk] is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and is not to be undertaken lightly.") with United States v. Albarado, 495 F.2d 799, 806 (2nd Cir. 1974) (arguing that magnetometer in airport involves "minimal invasion of privacy" because it involves none of the "indignities involved in fingerprinting, paring
test would have to distinguish between an invasive method, with all the inconvenience, discomfort, and even embarrassment it might cause, and a non-invasive method, in which an individual might not even know that he or she is being searched.

There are three responses to this intuitive argument. First, we need to distinguish between surveillances that infringe on property rights and those that infringe on bodily integrity. The first category—a surveillance that infringes on a person's property right—was unequivocally rejected in *Katz*. Even the courts that have interpreted *Katz* narrowly agree that the case repudiated the prior "trespass doctrine" which looked to invasion of property rights, thus instructing courts to disregard any invasion of property rights that might occur during the course of the surveillance. As noted above, this was a long-overdue acknowledgment that certain kinds of quite objectionable surveillance, such as listening to everything that is being said in a private home or on a private telephone line, could now be accomplished without infringing on anyone's property right. Unfortunately, even this aspect of *Katz* is occasionally lost in the subsequent Supreme Court case law, as we saw in the flyover cases above.

A close reconsideration of these arguments once again affirms the superfluous nature of the "property rights intrusion" factor: when the government observes our backyard, do we really care if they are doing it undetectably and legally from a satellite miles in the air or blatantly and illegally from a helicopter hovering ten feet above us? The fundamental—indeed, the only—concern is with the information that the government acquires and the location they are monitoring, not the action they took to acquire the information.

The second response to the intuitive objection deals with infringements on bodily integrity; a narrow reading of *Katz* would not require courts to disregard this factor. And it is true that government actions which infringe on our bodily integrity are more troublesome than those which infringe on property rights; certainly a regime in which the government had the right to physically infringe on our person as long as they only sought publicly available information is

of a person's fingernails, or a frisk") (citations omitted). Even though a frisk involves greater physical intrusion by the government agent, circuit courts have unanimously looked to the result and not the method and held that the use of a magnetometer is no less a "search" than a full body frisk. See, e.g., Albarado, 495 F.2d at 803 ("Even the unintrusive magnetometer walk-through is a search in that it searches for and discloses metal items within areas most intimate to the person where there is a normal expectation of privacy"); United States v. Epperson, 454 F.2d 769, 770 (4th Cir. 1972) ("[A] government officer, without permission, discerned metal on Epperson's person. That he did so electronically rather than by patting down his outer clothing or 'frisking' may make the search more tolerable and less offensive—but it is still a search.").

98. *See supra* notes 55-59 and accompanying text.
objectionable. For example, society would not likely accept law enforcement officers routinely and without cause forcing individuals on the street to stand against a wall while comparing their faces to hundreds of photographs of known suspects. On the other hand, it would probably be reasonable for a government agent to merely take a picture of the individual (while s/he was in a public place) and then compare that picture with other pictures. There is no real difference in the information that is acquired, merely in the method in which it is done; yet one is highly objectionable, and the other much less so.

The Supreme Court answered this objection, albeit indirectly, in *Terry v. Ohio*, although one which could be constitutional under certain circumstances. The Court was careful to note that not only were the defendants “searched” in this case—i.e., the police officer took actions in order to acquire information about what they may have been carrying—but they were also “seized”—i.e., the officer used force to prevent their physical bodies from moving freely. In *Terry,*

99. A modern version of this technique is becoming more and more common: using facial recognition technology to compare hundreds of faces in a crowd to pictures of known criminals. See Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy,* 9 S. CAL. INTERDISC. L.J. 295, 297 (1999). Originally developed by the military for national security purposes, facial recognition technology has found its way into many aspects of law enforcement, from the Central Intelligence Agency and the Immigration and Naturalization Service (who use it to identify individuals entering the country) to the West Virginia Department of Motor Vehicles (who use it as part of their fraud prevention program). *Id.* at 297-98. Like other biometric technologies, face recognition works by scanning the face, converting it into digital code that will function as the basis of comparison, and then storing that data for future reference. See Robyn Moo-Young, Note, “Eyeing” the Future: Surviving the Criticisms of Biometric Authentication, 5 N.C. BANKING INST. 421, 424, 426-29, 438 (2001). Because the codes are usually based either on the spatial relationships between features (i.e., the distance between the nose and the lips) or the subject’s bone structure, the system can take into account changes in appearance (such as those that occur due to aging or weight gain). *Id.* at 437-38; Milligan, *supra,* at 304-306. The spreading use of this new technology has raised concerns about excessive use of government power, but under the analysis proposed in this article, facial recognition technology is no different from an officer comparing a photograph of a known criminal to the faces of people the officer passes in the street. Both methods involve comparing a face while in a public place with pictures of known criminals; one method is merely more efficient than the other. Since the content of information received by the officer is identical in the two cases, the Fourth Amendment analysis under *Katz* should also be identical.

100. 392 U.S. 1 (1968).
101. *Id.* at 30-31. Namely, if the officer reasonably believes there is criminal activity afoot and the person with whom the officer is dealing may be armed and dangerous, and the frisk is necessary to protect the officer’s safety during the investigation. *Id.*

102. See *id.* at 20. (“In this case there can be no question, then, that Officer McFadden ‘seized’ petitioner and subjected him to a ‘search’ when he took hold of him and patted down the outer surface of his clothing.”).
there was both a search and a seizure (though both were ultimately deemed legal). If a police officer instead walked behind the defendant and scanned him unobtrusively with an X-ray device that could see through clothing, the defendant would have been searched but not seized. Conversely, if the police officer had merely detained the defendant for fifteen minutes until a witness could appear to identify him, he would have been seized but not searched. In other words, the separate constitutional prohibition against unreasonable seizures can, should, and does apply to inappropriate or abusive government tactics which unjustifiably infringe on the bodily integrity of the individual. So, for example, the kind of food that a person ate for breakfast in a public restaurant may be a fact in which the person has no reasonable expectation of privacy—but a government agent must acquire the information in a way that does not constitute an unreasonable seizure. The investigating agent could observe the person while eating or interrogate others that observed the meal, but not force the person to contribute saliva samples for testing nor force the person to accompany the officer to the hospital for an X-ray of the suspect's stomach.

Thus, the intuitive objection that physically invasive methods of surveillance somehow seem more objectionable than non-invasive ones is countered, at least in part, by noting that consideration of property-rights invasions were firmly rejected in Katz and more significant concerns about infringing on bodily integrity would be covered under the prohibition against unconstitutional seizures. But the third and perhaps the most important response to the intuition that the invasiveness of the search should matter is that it is this very intuitive feeling which will lead to an inexorable narrowing of the

103. An example of the dual analysis can be found in United States v. Place, 462 U.S. 696 (1983), in which federal agents seized the defendant's suitcase at the airport and kept it for ninety minutes while it was transferred to a location where a trained dog could sniff it to determine if cocaine were present. The Court first determined whether the ninety minute "seizure" of the luggage was appropriate—which involved a balance between "the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion"—which relies heavily on the actions of the government agents in conducting the seizure. Id. at 703. The Court then conducted a separate inquiry into whether the canine sniff itself was an unreasonable search, and applied a test that was heavily results-based. Id. at 706-70. See also infra note 194 and accompanying text.

104. The year after Terry, the Supreme Court decided the somewhat analogous case of Davis v. Mississippi, 394 U.S. 721 (1969). In investigating a rape case in which the victim said her assailant was African-American, police officers rounded up at least twenty-four African Americans without cause and fingerprinted them all at police headquarters. The Court held that these actions violated the defendant's Fourth Amendment rights, and, as in Terry, appeared to hold that the officers in question had conducted both an unreasonable "search" (in taking the fingerprints) and "seizure" (in detaining the defendant for the fingerprinting and a subsequent interrogation). See id. at 727-28.
scope of Fourth Amendment protection as technology progresses and increasingly intimate information can be acquired or intercepted without any physical invasion at all. Perhaps more ominously, a focus on physical invasiveness will reinforce the popular conception that certain government investigations/observations are not a search as long as they don’t feel like a search, leading to a world where ubiquitous video cameras, police use of sensors that can see through walls and clothes, and even monitoring of electronic mail, will become accepted by both the courts and the public, even as our true scope of privacy becomes narrower and narrower. And as one commentator has noted, non-intrusive sense-enhanced searches are by definition undetectable, and so may chill free speech (since average citizens cannot know whether they are under surveillance at any given time) and decrease police accountability (since the community as a whole may never learn of unjustified or mistaken police searches).  

In order to see how improving technology will erode Fourth Amendment protection if search methods are taken into account, we need only re-examine the cases in which judges object to certain types of surveillance based on the method used by the government. In every case, we can envision—quite easily—a technological advancement that would satisfy the concerns regarding invasiveness, thus allowing the government to conduct a nearly identical investigation which reveals identical information as the search that was supposedly invalid. For example, in *Oliver v. United States*, the dissent objected to the conduct of the police in ignoring “No Trespassing” signs and walking across defendant’s land without permission to find marijuana plants growing in an open field, and argued that the search should be unconstitutional in part because the police violated trespassing laws when they entered the land. Yet only three years later, in *California v. Ciraolo*, the Court upheld a search in which government agents flew a plane over the defendant’s property and observed illegal drugs from the air—clearly not violating any trespassing laws and thus robbing the *Oliver* dissent of much of its strength. In *Ciraolo*, it was the majority that improperly considered the “non-intrusive” nature of the search, noting that the officers were “within public navigable airspace [i.e., not trespassing]” and observing “in a physically non-intrusive manner.” Meanwhile, the dissent (consisting of two of the three dissenting Justices in *Oliver*) now sought to return to *Katz*’s true purpose:


107. *Id.* at 195-96. (Marshall, J., dissenting).


109. *Id.* at 213.
Reliance on the manner of surveillance is directly contrary to the standard of *Katz*, which identifies a constitutionally protected privacy right by focusing on the interests of the individual and of a free society. Since *Katz*, we have consistently held that the presence or absence of physical trespass by police is constitutionally irrelevant to the question whether society is prepared to recognize an asserted privacy interest as reasonable.  

The same concern applies to *Bond v. United States*, the recent case in which the Court invalidated a search because the customs agent felt the defendant's bag in "an exploratory manner." It is not difficult to imagine a customs agent in the near future equipped with a device that can see through the sides of an opaque bag. Under the majority's analysis, this would presumably allow a customs agent to examine the contents of everyone's bag on the bus, as long as he did not squeeze any of the bags. Surely the Court did not mean for the Fourth Amendment protection in such cases to be so fragile.

The problem of improving technology was also a key issue in the *Katz* decision itself. For over fifty years before *Katz*, technological advances had made focusing on the method of the search (where the agents stood in electronic eavesdropping cases) less and less relevant to the real questions: what information was being intercepted and what areas were under observation? In the post-*Katz* era the same misdirection is occurring. Courts still return to the method of search even when changing technology causes this analysis to lead to absurd and inconsistent results—for example, allowing a police officer to use binoculars to observe a living room from a neighboring property or a public alley, but not allowing a police officer to use a high-powered telescope to observe the inside of an apartment from an apartment across the street. In each case the police are using technology to

---

110. Id. at 223 (Powell, J. dissenting). As noted in the text, this dissent was joined by Justices Marshall and Brennan, who three years earlier had respectively written and joined the dissent in *Oliver* which declared that "when the owner of undeveloped land has taken precautions to exclude the public" such that "a deliberate entry by a private citizen . . . will expose him to liability," that government officials should also "be obliged to respect such unequivocal and universally understood manifestations of a landowner's desire for property." *Oliver*, 466 U.S. at 194-95. To be sure, the *Oliver* dissent also includes a number of arguments consistent with *Katz*, including an analysis of the owner's traditional legal right to exclude others from his or her property, and consideration of the sometimes intimate purposes for which privately owned land is used. Id. at 191-92. However, the focus on the physical trespass undertaken by the officers, as well as the proposal of a rule which differentiates the protection given to private land based on the posting of "No Trespassing" signs (which would be impossible to perceive from the air), indicate that the *Oliver* dissent still considered the method of search to be a significant factor. Id. at 235.

111. 529 U.S. 334 (2000).

112. Id. at 338-39.


114. See, e.g., United States v. Taborda, 635 F.2d 131 (2d Cir. 1980) (observation from apartment across the street using telescope is a search); State v. Thompson, 241 N.W.2d
peer into a very private (and constitutionally protected) area. How they position themselves and what kind of technology they use is irrelevant to whether a legitimate expectation of privacy has been infringed upon—just as the “trespass” that was or was not committed by the microphone should have been irrelevant in Silverman and Goldman.

B. Historic Support for a Purely Results-Based Katz Test

As noted above, the “reasonable expectation of privacy” test had numerous precursors in the language of Fourth Amendment opinions prior to Katz. Similarly, the concept of a results-based test is also supported by language in many pre-Katz decisions. In fact, the concept of focusing solely on the result of the surveillance and not the method formed the basis of one of the earliest and most significant Fourth Amendment cases. One hundred and fifteen years ago in Boyd v. United States, the Supreme Court considered the validity of a federal law which allowed the United States to subpoena a defendant’s private papers in order to use the information recorded on the papers against the defendant in a revenue case. Under the law, if the defendant refused to produce the papers, the allegations against the defendant regarding the content of the papers were deemed to be admitted by the defendant. The Court held that this constituted an unreasonable “search” even though nothing was

511 (Neb. 1976) (police looking from a neighboring alley is a search). But see United States v. Whaley, 779 F.2d 585 (11th Cir. 1986) (police looking through binoculars from neighboring property is not a search).

115. 116 U.S. 616, 621 (1886). Thirty-six years after Boyd, Justice Brandeis stated that the case “will be remembered as long as civil liberty lives in the United States.” Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). The Boyd case is best-known for helping to give birth to the exclusionary rule of evidence. Because the items that were the subject of the “search” were writings made by the defendants, the Court ruled that this coerced disclosure violated both the Fourth Amendment’s search and seizure provision and the Fifth Amendment’s right against self-incrimination. Boyd, 116 U.S. at 633. Thus the Court concluded—quite reasonably—that the invoices that were acquired by the government could not be used at trial, since such use would be tantamount to using the defendants’ own improperly seized testimony against himself. Id. at 638. Other cases then cited Boyd for the proposition that any evidence illegally acquired by the government should be excluded from trial, even if the evidence was not of a “testimonial” nature and thus no Fifth Amendment principles were at stake. See, e.g., Agnello v. United States, 269 U.S. 20, 32 (1925) (citing Boyd as authority to exclude cocaine from evidence because of illegal search). See also Akhil Reed Amar, Fourth Amendment First Principles, 107 HARV. L. REV. 757, 787-88 (1994) (classifying the early exclusionary cases as part of the now-discredited Lochner era: “a person has a right to his property, and it is unreasonable to use his property against him in a criminal proceeding.”).

116. See 18 Stat. 187 §5 (1874) (“if the defendant or claimant shall fail or refuse to produce such book, invoice, or paper in obedience to such notice, the allegations stated in the said motion shall be taken as confessed . . . .”).
physically being searched: "It is true that certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting . . . but it accomplishes the substantial object of . . . forcing from a party evidence against himself."117

This emphasis on the result of the search rather than the method of search ensured that the government could not acquire information which was protected by the Fourth Amendment simply by avoiding the traditional, physically invasive search. In Boyd, the government attempted the "back door" of legal compulsion, but today government agents have a far more efficient way of acquiring protected information without a physically invasive search: technology. When courts today consider the physically invasive aspect of the intrusion in order to determine whether a "search" has occurred, they are opening another back door for the government to acquire previously protected information.

The concept of focusing on the result of the search and ignoring the method re-emerges frequently throughout the next century of case law. In the very first wiretapping case, Olmstead v. United States,118 Justice Brandeis' dissent uses a result-oriented test in analogizing wiretapping with reading the mail, declaring that "the [Fourth] Amendment is violated by the officer's reading the paper without a physical seizure, without even touching it,"119 and concluding that in order to protect Fourth Amendment rights, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."120 Brandeis believed this results-oriented analysis was necessary because, as he warned somewhat prophetically:

The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.121

Twenty-four years later, Justice Murphy dissented in Goldman v. United States122 and similarly suggested that the government's conduct in any given search "may be wholly immaterial:"

There was no physical entry in this case. But the search of one's

---

118. 277 U.S. 438 (1928).
119. Id. at 478 (Brandeis, J., dissenting).
120. Id. (emphasis added).
121. Id. at 474.
122. 316 U.S. 129 (1942).
home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment. Surely the spirit motivating the framers of that Amendment would abhor these new devices no less.\footnote{123}

Justice Murphy also criticized the \textit{Olmstead} opinion for focusing on the method and not the result of the search, since it "keeps inviolate the most mundane observations entrusted to the permanence of paper but allows the revelation of thoughts uttered within the sanctity of private quarters . . . ."\footnote{124}

Twelve years later in \textit{Silverman v. United States},\footnote{125}—which struck down the "spike-mike" surveillance because it intruded on private property interests—Justice Douglas concurred with a scathing attack on the majority's reasoning. In comparing \textit{Silverman} with \textit{Goldman}, Douglas points out that the "invasion of privacy is as great in one case as in the other,"\footnote{126} and asks rhetorically: "[w]as not the wrong done in both cases done when the intimacies of the home were tapped, recorded, or revealed?"\footnote{127} He concludes with yet another incarnation of a results-based test: "[T]he command of the Fourth Amendment [should not] be limited by nice distinctions turning on the kind of electronic equipment employed. Rather our sole concern should be whether the privacy of the home was invaded."\footnote{128}

As noted above, Harlan's concurrence in \textit{Katz} appeared to be following this line of reasoning, but due to the vagueness of its language it did not clearly articulate that the method of the search should no longer be considered by courts in evaluating whether a search occurred. This lack of specificity in \textit{Katz} has caused the dissonance in the opinions we have seen since, and threatens to cause more problems as technologies advance, as discussed \textit{infra} in Part III.

\section*{C. The Caveat: Well-Established Technologies Can Change Reasonable Expectations}

If we are to completely ignore the conduct of the government agent in determining whether or not a "search" occurred, what elements do we consider in determining whether or not an expectation of privacy is reasonable? Justice Murphy's dissent in \textit{Goldman} relied to a large extent on original intent—arguing that the framers would never have countenanced the kind of "devices" that

\footnotesize
\begin{itemize}
\item \footnote{123} \textit{Id.} at 139 (Murphy, J., dissenting).
\item \footnote{124} \textit{Id.} at 141.
\item \footnote{125} 365 U.S. 505 (1961).
\item \footnote{126} \textit{Id.} at 512-13 (Douglas, J., concurring).
\item \footnote{127} \textit{Id.} at 513.
\item \footnote{128} \textit{Id.} (emphasis added).
\end{itemize}
enable government agents to eavesdrop on private conversations. But it is too simple—and unrealistic—to argue that we should return to the original intent and try to surmise what an eighteenth century rural society considered to be a reasonable expectation of privacy. There is obviously the standard problem faced by those who advocate original intent; namely that of finding credible and uncontroversed proof as to what eighteenth century society "believed" to be a reasonable expectation of privacy. Even if this could be reliably determined, modern-day crimes and the technological tools used to commit them today—cell phones, computers, and so on—are so different than those of two hundred years ago that many of the "traditional" rules would be ineffective. But most importantly, society itself has changed, so that what might seem to be a "reasonable" search today would never have been accepted by individuals in the 1780's. In other words, a workable test must be flexible enough to change as society changes, but rigid enough to stay constant even as technology changes. And technology—if it is widely accepted by the public—can legitimately change society's expectations about what kind of information is considered to be public.

As an example, consider the technology of electric lights. At the time of the adoption of the Fourth Amendment, it might easily be argued that what a person did outdoors in the dark was reasonably considered to be private. But electric lights have become so pervasive and essential to our society that this expectation has changed. The Supreme Court recognized this long ago in holding that the use of an electric light did not constitute a "search." Other technologies may not change society's expectations—for example, the ability to bug telephones has been around for as nearly as long as the telephone itself, and yet the content of a phone conversation is still considered private information.

The "flyover" cases of Ciraolo and Riley also provide examples of how new technologies can become so commonplace and affect society so fundamentally that—at least in theory—they can change people's conception of what areas are considered private.

129. See, e.g., Kyllo v. United States, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advances of technology.") (citing the flyover cases as an example of technology changing our conception of what areas are considered private).

130. See United States v. Lee, 274 U.S. 559, 563 (1927) ("Such use of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution"). See also Texas v. Brown, 460 U.S. 730, 740 (1983) ("[T]he use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection") (citing eight circuit court cases and seven state court cases in support).
Unfortunately, these cases also provide examples of how courts in practice can abuse this flexibility beyond its intended function. The *Ciraolo* court attempted to apply this theory of technologies changing expectations when they held that the defendant did not have a reasonable expectation of privacy in marijuana plants on his property that were visible only from the air: "In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected...." The Court's reasoning in reaching this conclusion is suspect, however—essentially the Court held that because "[a]ny member of the public flying in this airspace who glanced down could have seen everything [the] officers observed," all areas that are visible from public airspace are therefore no longer private. Here the Court conflates what modern technology has made possible (which by itself does not change what society views as public or private) with how modern technology has changed society (and thus changed reasonable expectations of privacy). Although it is now possible for law enforcement officials—or the general public—to fly in the air and observe the activities in private backyards, the practice is hardly considered routine and commonplace. A contrast can be made to the use of electric lights at night—not only is it now possible for law enforcement officials and the general public to observe outdoor nighttime activities (in a way that was not contemplated in the 18th century), but it is also so commonplace that society arguably no longer considers such activities private.

This distinction between what new technologies make possible and what new technologies have made commonplace is even sharper in a subsequent flyover case, in which the Court held that observations made from a helicopter hovering at 400 feet were legitimate because "[a]ny member of the public could legally have been flying over [defendant's] property in a helicopter at the altitude of 400 feet." As noted above, this reasoning improperly considers whether the government was violating state or federal law when conducting the surveillance—a factor which *Katz* should have banished altogether. But more subtly, it assumes that society's expectations have changed just because a new technology has made it possible for the public to make certain observations, without pausing to consider whether or not such observations are in fact occurring.

132. *Id.* at 213-14.
133. As the *Ciraolo* dissent noted, "the actual risk to privacy from commercial or pleasure aircraft is nonexistent." *Id.* at 223 (Powell, J., dissenting).
135. *See supra* notes 58, 59 and accompanying text.
often enough to make the defendant's expectation of privacy "unreasonable."\footnote{136}

Given this context, the methods-based "caveat" that the \textit{Kyllo} court added to its result-oriented test seems more sensible. As noted above,\footnote{137} \textit{Kyllo} stated that the use of technology to observe activity or details that would otherwise be unobservable without physical intrusion was a search, but only if "the Government uses a device that is not in general public use."\footnote{139} The opinion itself goes into very little detail about why the caveat is included or—more importantly—how to determine whether a given technology is "in general public use."\footnote{139} The dissent argued that thermal imagers of the kind used by the government in \textit{Kyllo} are available to the public, and over 10,000 units had been manufactured.\footnote{140} The majority provided a cursory response to this point by quoting Ciraolo's description of commercial flight as being "routine," and credibly stating that "thermal imaging is not "routine.""\footnote{141} Of course, "routine" is not the same as "in general public use"—technologies such as helicopters, night vision goggles, supercomputers, and arguably thermal imagers may be "in general public use," but none of them are "routinely" used the way personal computers, telephones, binoculars, and walkie-talkies could be considered routine. And neither term conveys (though "routine" comes closer) what the court probably meant to convey: that if a technology becomes so widespread and commonplace that it changes societal expectations of privacy, its use is no longer considered a "search."\footnote{142}

\footnote{136} Thus, the \textit{Riley} decision was faulty on two grounds: first, because it improperly considered the method of search (noting repeatedly that the observation was made "legally") and second, because it focused on what technology made possible, not on whether or not technology had actually changed expectations. The \textit{Riley} dissent was quick to argue these two points as well, though it tended to conflate the two fallacies: The question before us must be not whether the police were where they had a right to be, but whether public observation of Riley's curtilage was so commonplace that Riley's expectation of privacy in his backyard could not be considered reasonable. To say that an invasion of Riley's privacy from the skies was not impossible is most emphatically not the same as saying that his expectation of privacy within his enclosed curtilage was not one that society is prepared to recognize as reasonable. \textit{Riley}, 488 U.S. at 460 (Brennan, J., dissenting) (internal citations and quotations omitted).

\footnote{137} \textit{See supra} note 86 and accompanying text.


\footnote{139} And as noted in \textit{supra} note 86, the dissent notes that thermal imagers of the kind used by the government in \textit{Kyllo} are available to the public, and over 10,000 units had been manufactured. \textit{Id.} at 47 n.5 (Stevens, J., dissenting).

\footnote{140} \textit{See supra} note 86.

\footnote{141} \textit{Kyllo}, 533 U.S. at 39 n.6.

\footnote{142} The \textit{Kyllo} case was obviously struggling with how to craft a results-based search that would remain flexible enough to adapt as technology changed society. The primary
The point is that in saying the method of search is irrelevant, we are not necessarily ignoring the dramatic effects that certain technologies have had on society generally and our expectations of privacy specifically. Courts can—and should—consider how technology has changed society. However, courts must do so carefully, always keeping in mind that the ultimate test is whether technology has sufficiently changed society such that the area (or item) in question is now one that is considered “public” in modern society. Courts must resist the temptation to conclude that just because a certain technology is available and the public could use it to render once-private realms public, that in fact it has been used to render them public. The Ciraolo and Riley Courts were unable to resist this temptation; thus they applied the proper test, but they applied it poorly, without considering the underlying reasons behind the test. The Kyllo Court attempted to provide a caveat that would take this factor into account, but the phrasing it used is likely to cause more problems than it solves. The balancing act is admittedly difficult, but it is essential. In applying a results-based test that remains flexible enough to adapt to technological advances, courts must not consider changes in technology, but rather how technology changes society.

III. Case Studies: Cybercrime, Sense-Enhancing Technologies, and Binary Searches

A results-based application of the Katz test becomes increasingly important as the method of searches becomes more technologically

language of its test, “obtaining by sense-enhancing technology any information regarding the home’s interior that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’” is too rigid and affords too much protection—it would forbid the government from using electric lights or binoculars. Kyllo, 533 U.S. at 34. Indeed, the Court states that this test “assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” Id. But of course that is not the goal, as the Kyllo Court itself noted one paragraph earlier: “It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advances of technology.” Id. at 33-34.

Although very little of this question made its way into the final opinion, this was a hotly debated question at Kyllo’s oral arguments, as the Justices asked defendant’s attorney numerous questions regarding less-sophisticated technologies such as binoculars and flashlights. Oral Argument at 22-23, 28-29, Kyllo v. United States, 533 U.S. 27 (2001). At one point a Justice hypothesized a world in which “thermal imaging becomes very common and every kid has a $5 thermal imager,” and asked the defendant’s attorney whether that would change the reasonable expectation of privacy. Id. at 23-24. Predictably, the defendant’s attorney answered in the negative, but under this article’s conception of the Katz test, such a dramatic change in society would and should change the outcome of Kyllo.
sophisticated. Specifically, three of the most difficult aspects of search and seizure law today—computer searches and/or surveillance, sense-enhancing technology, and binary or content-discriminatory searches—suffer from lack of consistency because methods-based factors still survive to varying degrees.

A. Investigations of Cybercrime and Other Computer-Related Offenses

(1) The Legacy of Smith v. Maryland

The difficulty in applying the Fourth Amendment to computer searches and surveillance can be traced to Smith v. Maryland, a case from 1979 that had nothing to do with computers. In Smith, the police (without obtaining a warrant) asked the phone company to install a "pen register"—which records all phone number dialed out from a given telephone—on the defendant's phone. The pen register revealed that the defendant made a phone call to the victim, a woman whose car had been stolen and who had been receiving numerous obscene phone calls from a man claiming to be the robber. Based on this information, the police obtained a warrant and searched the defendant's home, which resulted in further incriminating evidence. At trial, the defendant moved to suppress the use of the "pen register" (and the fruits thereof), claiming that the police had conducted a "search" when they acquired the phone numbers that he dialed, and the trial court denied the motion. The Supreme Court ultimately agreed, holding that the defendant had neither a subjective nor an objective expectation of privacy in the phone numbers that he dialed.

The Smith Court claimed to be using the Katz test as its "lodestar," and appropriately sought to determine whether or not the information that the government acquired—the phone numbers the defendant had dialed—was information that society considered to be private. In doing so, however, the Court spent almost no time considering the nature of the information itself, and instead focused on the fact that the defendant had "voluntarily" turned the supposedly private information over to a third party, i.e., the phone

143. 442 U.S. 735 (1979).
144. Id. at 737.
145. Id. at 737-38.
146. Id. at 742-43.
147. Id. at 739-40.
148. The Court conducts a brief examination of the nature of the item being "searched," noting that pen registers do not record the contents of the phone call, but this analysis is only meant to demonstrate that the facts of the case are not identical to those of Katz; that a pen register is different enough from a microphone to require independent consideration. Id. at 741-42.
company. The Court thus placed dialed phone numbers in the same category as statements made to an informer—information which an individual makes available to a third party and in which an individual therefore no longer has a reasonable expectation of privacy.

This analogy between freely making statements to an individual who may or may not be an informer and communicating the phone numbers that you dial to the phone company as a necessary function of using a phone is dubious. The dissent in Smith noted that in the informer cases, the Court relied on the doctrine of "assumption of risk," which implies some "freedom of choice" on the part of the individual. But no such choice is involved when one uses the telephone—essentially, the Court is ruling that everyone who uses the telephone is waiving his or her right to privacy in the phone numbers he or she is dialing.

Viewed in this light, Smith's overly formalist analysis looks suspiciously like a method-of-search analysis dressed up in disguise. Certainly if a person chooses to give information to a third party, the government can credibly argue that the nature of the information has changed; it is no longer private, and society no longer recognizes an individual's expectation that it will be kept secret. Thus, allowing the government to obtain such information without a warrant is consistent with a results-based test: the result of the search is information that is no longer considered private. But when the Court claims that information automatically enters the public arena without the individual taking any action at all (aside from creating the information in the first place, i.e., dialing the telephone), there is no realistic argument that the information thus automatically becomes public. Instead, when the Court applies the third-party doctrine to such information, it is engaging in a methods-based analysis—the government did not place a device on a person's phone nor spy on the individual dialing the phone; instead, it merely asked the phone company for records that were already kept in the ordinary course of business. This sanitized method of search apparently makes it more palatable—but we have seen that argument before: in Boyd when the government sought to gain private information through subpoena; in

149. Id. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").


the line of now-discredited cases upholding phone tapping and eavesdropping; and finally in *Katz*, where it was firmly rejected.

This is not to say that the holding of *Smith* is wrong; it may well be that the phone numbers a person dials are not something that society is prepared to recognize as private information. But answering this question requires more than a finding that this information is capable of being recorded by a third party. It would require an analysis of the information itself. Do we generally believe that the identities of the people that we communicate with is private information? If the telephone did not exist, individuals would have to physically travel to other people's homes, or to public meeting places, and this activity could presumably be monitored by government agents without violating the Fourth Amendment. When individuals communicate by mail, the Fourth Amendment clearly allows the government to observe to whom the envelopes are addressed as the mail is sent through the system. All of these factors point towards allowing the government to use a pen register without a warrant—but none of these factors were considered by the *Smith* Court.

The most unfortunate aspect of *Smith* involves a short paragraph near the end of the opinion, seemingly of little importance at the time. The defendant noted that he had never actually revealed the phone numbers to a live person; they had merely been recorded by the phone company's "automatic switching equipment." The Court rejected this argument in broad terms, and held that "revealing" information to an automated system was the same as revealing it to an individual.

Given the technological revolution that has occurred in the twenty-three years since *Smith* was decided, this doctrine is now

153. Since *Smith* was decided, a number of technological advances (such as Caller I.D.) have become prevalent enough that society's expectations may have changed as to the privacy a person should receive in the phone numbers that he or she dials. A modern-day Supreme Court re-examining *Smith* should take this into account as well. See generally *supra* notes 126-142 and accompanying text on how technology can change society's expectations of privacy.

154. This principle was first settled over 120 years ago, in *Ex parte Jackson*, 96 U.S. 727 (1877) (any information available without opening the mail (size of package, name of sender and receiver, etc.) is available to the government without a warrant).

155. *Smith*, 442 U.S. at 744-45. In fact, the telephone company's system did not automatically record every phone number that was dialed in, only those necessary for billing purposes (such as long-distance numbers) or those requested by the government (for example, in tracing obscene phone calls). Even so, the Court held that the mere fact that a third party could be receiving this information meant that under the law defendant had voluntarily given this information to a third party: "Regardless of the phone company's election [to record or not to record specific numbers], petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Id.* at 745.
problematic, to say the least. Taken literally, this rule would give the
government the power to monitor every piece of electronic mail that
is sent through the internet, since every electronic transmission that is
sent from one person to another travels through numerous switching
computers, each of which are independent third parties and any of
which have the capability of recording the addresses and the content
of the transmissions. As noted infra, the Smith case—like all
computer-related Fourth Amendment jurisprudence—has been
largely supplanted by statute, but the constitutional problem remains
waiting beneath the surface.

(2) The ECPA and the Fourth Amendment in Computer Surveillance—The
Need to Distinguish Among Content

The past twenty years have seen a revolution in communications
technology comparable to that of the telephone—and subsequently a
revolution in communications surveillance technology comparable to
the electronic listening device or the phone tap. Technology now
makes it possible for law enforcement agents located literally
anywhere in the world to easily and conveniently read electronic
communications between two parties, in the same way that electronic
listening devices and wiretaps made it easier to eavesdrop on oral
communications from remote locations. Perhaps even more
dramatically, the advent of the new communications medium gives
law enforcement officers the ability to scan through literally millions
of electronic communications every minute, searching for
incriminating content or addresses in a way that was inconceivable for
traditional mail. And as with the wiretapping and electronic
surveillance technologies, these searches can occur without the
knowledge of the individual under surveillance.

As we have seen, the judicial response to the new surveillance
technologies of the early twentieth century took many decades to
evolve into a model that recognized the realities of the new
technology. Perhaps as a result, after Katz, Congress began taking
matters into its own hands, first with regards to oral and electronic
communications, and then with regard to electronic communications.

In 1967, the Supreme Court held in Katz that the use of
electronic listening devices was a "search," and held in Berger v. New
York that wiretapping a telephone could be a "search." The next
year, Congress passed the Wiretap Act of 1968, ubiquitously known
as "Title III." This Act sets out strict rules for government
monitoring of oral and wire communications: before the government

156. See infra Part III.A.2.
can use a bug or wiretap a phone, it has to acquire a court order (a "Title III order"). The requirements for such an order are more onerous than what would be required under the Fourth Amendment: the government must demonstrate that (1) "normal investigative procedures" have been tried and failed, are unlikely to succeed, or are dangerous; (2) probable cause that the specific communications facility is being used in a crime; (3) the surveillance will be conducted in a way that minimizes the interception of irrelevant information; (4) there is probable cause to believe that the interception will reveal evidence of one of a limited list of predicate crimes. In addition, the original legislation required the order to be signed by a federal judge and authorized by a high-level Department of Justice official. Finally, any Title III order is time-limited to thirty days, although the government can request an extension.

In the case of oral communications, the statute tracked the *Katz* language and only protected conversations in which an individual had a "reasonable expectation of privacy;" however, in the case of wire communications there was no such limitation, presumably because Congress assumed that every "wire communication" (i.e., phone call) was private and thus deserved full statutory protection.

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") which amended Title III to include protections for electronic communications. The language of the ECPA tracked the "wire communication" provisions, setting the same high requirements for all electronic communications, regardless of whether there was a "reasonable expectation of privacy" in the communication. At least one commentator has criticized this omission, since internet traffic now includes not just private, personal communications but also "[w]eb pages in transit, commands sent to remote servers, picture or music files, network support traffic, and almost everything else in cyberspace." In this sense, statutory protection for electronic communications is too broad, treating all internet traffic as deserving of an equal amount of protection and thus forcing government agents

159. *Id.* § 2518.
160. *Id.* § 2516.
161. *Id.*
162. See *id* § 2510(2).
163. See *id* § 2510(1).
165. *Id.* at 1300. In this sense, statutory protection for electronic communications is too broad, forcing government agents to acquire a Title III order for even the most mundane transmissions that would not deserve privacy under the *Katz* test.
to acquire a Title III order for even the most mundane transmissions that would not deserve privacy under the *Katz* test.\(^\text{166}\)

But if the ECPA is overbroad in that it treats every piece of internet traffic the same without discriminating as to its content, under *Smith* the Fourth Amendment has the opposite problem for the same reason. Under *Smith*, any time an individual “voluntarily” conveys information to a third party in the course of a conversation, and that third party has “facilities for recording” the information, the government can acquire that information from the third party without infringing on the individual’s Fourth Amendment rights—without regard to society’s actual expectation of privacy in the specific transmission that is being made.\(^\text{167}\) This is significant because while Government agents who violate the ECPA can be civilly or even criminally liable (though good faith and qualified immunity defenses may apply),\(^\text{168}\) there is no statutory suppression remedy for the ECPA.\(^\text{169}\) Thus, any electronic communications that are acquired in violation of the statute are admissible unless the search also violated the Fourth Amendment.

We saw that in the context of a telephone communication, the argument that the individual “chose” to reveal the phone numbers he or she is dialing to a third party was more or less a formalist construct, since phone companies have the ability to electronically record every phone number that is dialed from any telephone. In the context of electronic communications, this formalism becomes even more strained, since electronic communications might pass through dozens of servers and Internet Service Providers (“ISP’s”) before they reach their destination. The supposedly “results-based” test in *Smith*—that

\(^{166}\) Since the ECPA was passed in 1986, the internet has grown in use so dramatically that nearly every kind of interaction, transaction, or communication that could occur in the outside world can now occur in cyberspace as well. Thus, applying the Title III restrictions to every internet-based search would be the equivalent of requiring a warrant under the Fourth Amendment for observing or monitoring every kind of interaction or transaction in the real world: “Much like human behavior in realspace, electronic behavior in cyberspace is too varied to fit within a single paradigm. One-size-fits-all doesn’t work.” *Id.* (citations omitted).

\(^{167}\) See *Smith*, 442 U.S. at 745.

\(^{168}\) See 18 U.S.C. § 2520(d) (“[a] good faith reliance on . . . a court warrant or order . . . or a statutory authorization . . . is a complete defense against any civil or criminal action brought under this chapter or any other law”); Tapley v. Collins, 211 F.3d 1210, 1216 (11th Cir. 2000) (allowing a qualified immunity defense in an action filed for violations of Title III). For an excellent overview of these subjects see generally COMPUTER CRIME & INTELL. PROP. SECTION, UNITED STATES DEP’T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 120-26 (2001). (hereinafter DOJ MANUAL).

\(^{169}\) See DOJ MANUAL, supra note 168, at 120; Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994). There is a statutory suppression remedy under Title III for oral and wire communications. See 18 U.S.C. § 2518(10)(a) (2000).
acquiring such information does not violate the *Katz* test because the result (the information acquired) has been voluntarily offered up to the public—is nonsensical. In reality such searches would be allowed under *Smith* because the government action in acquiring the information—taking it off an anonymous server—is less offensive than invading a person's private computer files. A true results-based test would focus on the information itself—was it a piece of electronic mail (which would surely deserve complete Fourth Amendment protection given the precedents for traditional mail); was it a financial transaction sent from one company to another company (which may deserve less protection); or a message sent to an internet chat room (which truly has been offered up to the world and in which society is not prepared to recognize a reasonable expectation of privacy).

The ECPA tacitly acknowledges the anomalous outcome of *Smith*'s reasoning by setting a low standard for intercepting the internet version of pen registers (as well as devices that record the identity of incoming calls or messages, known as "trap and trace" devices in the phone context). The "header" of an electronic mail contains a "To" line, a "From" line, and a "Subject" line; thus, a device that reads the header off an e-mail will not only acquire information about the identity of the sender and receiver, but also information about the content of the e-mail itself. The ECPA quite sensibly treats the "To" and "From" lines differently than the "Subject" line—even though they are intercepted at the same time and under *Smith* the sender has no reasonable expectation of privacy in any of them (or in the rest of the message, for that matter). In order to receive an order authorizing a "pen/trap" device for monitoring the "To" and "From" lines of electronic transmissions, government agents need only certify that the information that is likely to be obtained is relevant to an ongoing criminal investigation. By

170. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles").


173. 18 U.S.C. § 3122(b) (2000). *See also DOJ Manual*, supra note 168; United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (describing the judicial role in approving such devices as "ministerial in nature").
Because the ECPA provides broader protection than the Fourth Amendment in most instances, almost no cases involving monitoring of electronic communications reach the Fourth Amendment question. Therefore Smith's thinly veiled methods-based test still stands as Fourth Amendment law. When courts do address the extent to which the Fourth Amendment protects electronic communications, a faithful application of the Katz test would require them to avoid both the overbroad blanket protection of the ECPA itself (which ignores the "reasonable expectations" language of the Katz test) as well as the Smith application of Fourth Amendment doctrine (which misinterprets the "reasonable expectations" language). Instead, courts should consider the nature of the information and the actions of the defendant regarding that information in determining whether there is a "reasonable" expectation of privacy in the information.

B. "Sense-Enhancing" Devices

Applying the Katz test to surveillance with sense-enhancing devices poses serious challenges for a number of reasons. First, as we saw in Kyllo, the very nature of these devices requires courts to understand the distinction between an "intrusion" in the sense of a physical invasion, and an "intrusion" in the sense of an improper observation of private information. Sense-enhancing devices are

174. The "subject" line would be considered content and thus beyond the scope of a pen/trap device.

175. As noted in supra note 165 and accompanying text, the ECPA not only protects a broader range of internet traffic than would be protected under Katz, but also sets a higher standard for a Title III order than what would be required for a warrant under the Fourth Amendment. The only significant way in which the ECPA is less protective is that it does not provide for a suppression remedy. See generally DOJ MANUAL, supra note 168, at 104-26.

176. Unfortunately there is some precedent from video surveillance cases for courts to simply import the requirements and standards set by Title III (as amended by the ECPA) into Fourth Amendment jurisprudence. Neither Title III nor the ECPA make any mention of covert video surveillance, and so there is no federal statute regulating such activities. Every court that has considered the issue agrees—unsurprisingly—that the Fourth Amendment does apply to video surveillance, and every court so far has rather inexplicably imported the language and requirements of Title III into the Fourth Amendment, holding that video surveillance is constitutional provided it complies with Title III. See United States v. Biasucci, 786 F.2d 504 (2d. Cir. 1986), cert. denied, 479 U.S. 827 (1986); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990); United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992), cert. denied, 506 U.S. 1005 (1992); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994). For a spirited critique of this practice, see Koyomejian, 970 F.2d at 542-51 (Kozinski, J., concurring).
popular because they are generally far less physically invasive, but they have the potential to reveal a far greater amount of information than more traditional searches. Thus, they may be less "intrusive" in the first sense (which is irrelevant under the Katz test) and more intrusive in the second sense (which goes directly to a results-based analysis).

The confusion in this field stems from defining what is meant by a "sense-enhancing device." Numerous courts and commentators have distinguished between "sense-enhancing" devices that simply magnify or improve existing senses (such as binoculars, flashlights, or parabolic microphones) and "sense-replacing" devices that actually detect or record information that is beyond any of our senses (such as x-ray machines or thermal imagers). This is a false dichotomy; as Justice Harlan said about the physical trespass rule in Katz, the distinction is "bad physics as well as bad law." In terms of physical science, the difference between "sense-enhancers" and "sense-replacers" simply means distinguishing between a device that enhances inputs (such as light waves or sound waves) which would be detectable to us if they existed in greater magnitude, and inputs (such as X-rays, ultraviolet waves, or radio waves) that our senses could never detect no matter what their magnitude. Why this distinction should have a legal significance is unclear. Consider, for example, the thermal imager in Kyllo; by any meaningful scientific definition, it merely enhances an input (heat) which we are able to detect on our


Unlike the electronic 'beeper' in Knotts, however, a dog [trained to react to the smell of narcotics] does more than merely allow the police to do more efficiently what they could [already] do using only their own senses. A dog adds a new and previously unobtainable dimension to human perception. The use of dogs, therefore, represents a greater intrusion into an individual's privacy.

Id.


[G]un detectors do not do what lights, telescopes, binoculars, and like devices do—put police officers artificially closer or provide illumination enabling them to observe what would be visible anyway but for distance or darkness. Rather, gun detectors allow police to see what they never could. . . . Gun detectors do not so much enhance police senses as they do replace them with something superhuman, an ability to perceive that people simply do not have.

Id.

Other judges have come up with equally suspect classifications. See, e.g., United States v. Bronstein, 521 F.2d 459, 464 (2d Cir. 1975) (Mansfield, J., concurring) (describing a category of devices which "detect[] hidden objects without actual entry and without the enhancement of human senses" including narcotics dogs, magnetometers, x-ray machines, and microphones).

own; yet it amplifies this input to such an extent that it provides information about the activities inside the home that we could never know merely by using our natural ability to detect heat. Why should courts treat this differently from a device that can pick up inputs completely undetectable to us (such as X-rays or neutrinos) as they pass through the walls but gives the same picture of the interior of the house? Consider also a dog trained to sniff for narcotics. Some Justices considered this "technology" to be a "sense-replacer" since it allegedly "adds a new and previously unobtainable dimension to human perception." But other courts have appropriately pointed out that this technology merely amplifies an input that we can already detect; if the smell of cocaine were more powerful, a human being could detect the contraband without relying on the dog.

As the foregoing analysis implies, the distinction is bad law because it focuses on the method of search, rather than the result. Assume a hypothetical case in which law enforcement agents enter the defendant's property at night without a warrant. As the agents make their way across the defendant's property using night-vision goggles, the infrared sensors in the goggles allow them to detect a large grove of marijuana plants that have been planted in an open field approximately a half-mile away from the house. They then approach the darkened house and remove their goggles. One of them climbs a tree and then shines a flashlight into the second-floor window of the house and observes bales of harvested marijuana stacked against the wall of the room. The agents then acquire a search warrant and return to confiscate both the marijuana growing outside the house and the harvested marijuana inside the house.

A court considering the validity of these searches should not (and probably would not) care which observations were made with the "sense-replacing" night vision goggles and the "sense-enhancing" flashlight; the relevant inquiry would focus on what kind of information the agents observed and whether the defendant had a reasonable expectation in keeping that information private. The

---


180. See, e.g., *Horton v. Goose Creek Indep. Sch. Dist.*, 690 F.2d 470, 477 (5th Cir. 1982) ("The dog's olfactory sense merely 'enhances' that of the police officer in the same way that a flashlight enhances the officer's sight."). See also *United States v. Kelly*, 128 F. Supp. 2d 1021, 1024 (S.D. TX. 2001). Sometimes the courts use language that seems to put canine sniffs in a middle category; see, e.g., *United States v. Thomas*, 747 F.2d 1359, 1367 (use of a dog is not a "mere improvement" of their sense of smell, but "a significant enhancement accomplished by a different, and far superior, sensory instrument.").
distinction between the unfenced marijuana field far from the house and the stacks of marijuana inside the private home carries great constitutional significance; the distinction between the type of device should carry none. The same principle holds true in comparing agents who observe a backyard from a distance using a high-powered telescope with those who observe the same backyard by installing a miniature video camera on an adjacent fence. It is the area under observation (as well as the actions taken by the defendant to ensure its privacy) that is relevant, not the type of technology used to conduct the observation.

As noted above, *Kyllo* has gone a long way to clarifying this area of law. The government in *Kyllo* essentially argued that thermal imagers were merely sense-enhancing and thus fundamentally different from a sense-replacing device that could see through the wall. The Court, however, made clear that the type of technology was irrelevant; whether they were reading inputs “off the wall” or “through the wall.”

But this doctrine did not begin with *Kyllo*. In 1982, the Court decided *United States v. Knotts,* in which the government had inserted an electronic tracer (called a “beeper”) into a container of chemicals purchased by the defendants. The government monitored the beeper’s location in order to follow the defendants as they drove back to a secluded mountain cabin, and the Court held that following the beeper’s signal was not a “search” under the Fourth Amendment. The critical aspect of the ruling was that the government only used the tracer in order to locate the chemicals as they passed over public highways. The Court noted that once the container reached the defendant’s cabin, the defendant enjoyed the traditional expectation of privacy within a private dwelling place, and implied that if the government had used the beeper to trace the container’s movements within the cabin, the defendant’s rights may well have been violated.

In contrast, the government only used the tracer to determine where

181. See Oliver v. United States, 466 U.S. 170 (1984) (no “search” takes place when government agents trespass on property and observe items in an open field outside the curtilage of the home). By contrast, observation of the inside of a home is deserving of the highest level of Fourth Amendment protection. See, e.g., Kyllo v. United States, 533 U.S. 27, 37, (2001) (“In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes.”) (emphasis in original).

182. The government’s opening argument began with the observation that “thermal imaging senses heat gradients on the exterior of a surface. It does not penetrate the walls of the house.” (Oral Argument at 12-13, 30, Kyllo v. United States, 533 U.S. 27 (2001)).

183. See Kyllo, 533 U.S. at 35-36 (rejecting dissent’s “mechanical” distinction between “off-the-wall” and “through-the-wall” technologies).


185. Id. at 282.
the container was transported over a "public highway" or its movements in the "open fields" outside the cabin.\footnote{186}

The electronic tracer in \textit{Knotts}, like the thermal imager in \textit{Kyllo}, was a "sense-replacing" device—it emitted radio waves that could only be detected by a special receiver.\footnote{187} But again the Court focused not on the \textit{method} the police used, but the \textit{result}: the information they obtained was information that was open to the public; i.e., where the defendant drove on the public highways and where he placed the container outside his cabin in public view. Given the Court's argument in \textit{Knotts}, any kind of technological enhancement would have been appropriate, as long as it revealed only "publicly observable" information. In other words, the government could have attached a video camera to the container to show where it was being taken—as long as the agents stopped monitoring the camera once it was taken into a private place.\footnote{188}

\footnote{186. \textit{Id.}} Visual surveillance from public places along [co-defendant] Petschen's route or adjoining Knott's premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.

\footnote{187. Although because it was only used \textit{in this case} to detect what could theoretically be seen, it was later described by Justice Brennan as a "sense-enhancing" device: "Unlike the electronic 'beeper' in \textit{Knotts}, however, a dog [trained to react to the smell of narcotics] does more than merely allow the police to do more efficiently what they could [already] do using only their own senses." United States v. Place, 462 U.S. 696, 719 (1983) (Brennan, J., concurring). Of course, the device itself did much more than "merely allow the police to do more efficiently what they could [already] do using only their own senses[.]"] The Supreme Court had properly limited the use of the device so that it could only be \textit{used} to transmit information that was available to their senses, i.e., so that it only could be used to transmit information in which the defendant had no reasonable expectation of privacy.

\footnote{188. \textit{Knotts}, 460 U.S. at 285.} A police car following [co-defendant] Petschen at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car. This fact, along with others, was used by the government in obtaining a search warrant which led to the discovery of the clandestine drug laboratory. But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.

\textit{Id.} \textit{See also} United States v. McIver, 186 F.3d 1119 (9th Cir. 1999), in which defendant's growing of marijuana in a national forest was caught by motion-activated video camera. There, the Court of Appeals upheld defendant's conviction: "Illegal activities conducted on government land open to the public which may be viewed by any passing visitor or law
Thus, *Knotts* and *Kyllo* demonstrate that, although the terminology occasionally becomes confused, and certain Justices do try to distinguish between types of sense-enhancing devices, in the end the Court has appropriately treated all sense-enhancing devices alike and—consistent with the *Katz* test—it has looked to the result rather than the method of the search.

C. "Binary" Searches and Content-Discriminating Technologies

This Article has argued that applying the *Katz* test to consider only the results and not the method of the search will help to ensure that Fourth Amendment rights are protected even as technology improves to give law enforcement more effective tools of surveillance and investigation. For the most part, then, focusing on results and ignoring the method of search will effectively broaden the reach of the Fourth Amendment, ensuring that as technology improves, an individual's zone of privacy does not diminish—unless technology changes society to such an extent that reasonable expectations of privacy are fundamentally altered. However, a results-based *Katz* test will arguably favor law enforcement in a special category of searches: so-called "binary" or content-discriminatory investigations, in which the technology used is designed in such a way that the only result of the investigation is information about whether contraband or illegal activity is present.

So far only two Supreme Court cases have considered binary investigations, and in each case the Court has upheld the government action. In *United States v. Place*, the Court held that the use of a dog who only reacted to the presence of cocaine was not a "search," and in *United States v. Jacobsen*, the Court held that testing a substance with a chemical that only reacted to the presence of narcotics was also not a "search." These cases have always sat uneasily alongside the other post-*Katz* cases. At first glance, they seem to be the worst example of a methods-based approach—in *Place*, for example the Court obviously found significance in the fact that the search was not physically invasive. How are such cases different from any other sense-enhancing case, in which law enforcement agents are able to use technology to learn about otherwise private information in a non-invasive manner?

enforcement officer are not protected by the Fourth Amendment because there can be no reasonable expectation of privacy under such circumstances.” *Id.* at 1125-26.

191. *Place*, 462 U.S. at 707. ("A 'canine sniff' by a well-trained narcotics detection dog . . . does not require opening the luggage.") Later the Court notes that the "manner in which the information is obtained" is limited. *Id.*
The answer again comes from a closer consideration of the *Katz* test and its underlying rationale. In defining the objective prong from the *Katz* test, the Court has used the analogy of a "burglar plying his trade in a summer cabin during the off-season," who may have a subjective expectation of privacy, but not one which society recognizes as legitimate.\(^{192}\) In other words, a person conducting an illegal activity or possessing an illegal substance has no legitimate interest in not having law enforcement agents learn of his illegality. The problem, of course, is that in searching for illegal activity, law enforcement agents will inevitably also observe or detect legal and private activity.

If the police carried out nightly warrantless searches of everyone’s home, they would doubtless observe and recover quite a bit of unlawful activity and contraband—but at the unacceptable cost of exposing a vast amount of legitimate private activity and items to an unreasonable search. But what if the police were able to detect whether narcotics were present in a home or on a person merely by pointing a specialized “narcotics detector” at the home or person? Would the use of such an instrument constitute a “search?”

If the narcotics detector yielded no information other than the absence or presence of an illegal substance, and it was close to 100% accurate, *Place* and *Jacobsen* suggest strongly that using such a device should not be considered a search. This conclusion also logically follows from the results-based test advocated in this Article: if the only “result” of the surveillance is the presence of illegal activity or contraband—situations in which individuals do not have a legitimate expectation of privacy—then conducting such a surveillance does not constitute a search.\(^{193}\)

A close examination of the case law supports this analysis. Although in *Place* the Court does consider the non-invasive nature of the search on two occasions, it also relied upon the limited information provided by the search: “[The search] does not expose noncontraband items that otherwise would remain hidden from public view... the sniff discloses only the presence or absence of


\(^{193}\) To return to the analogy of the burglar in the summer cabin, the police would obviously be prohibited from simply forcing their way into every summer cabin during the off-season to look for burglars. However, if the burglar sets off an alarm, the police are perfectly within their rights to enter the cabin and search for illegal activity—in this case the alarm acts as a sort of “burglar detector,” which will only react when there is illegal activity occurring. Of course, police also have implied consent from the legitimate owner to enter a home when the alarm has been triggered, which also insulates their actions from impropriety. But the “binary search” of the alarm system at least intuitively makes their search more justifiable.
narcotics, a contraband item." Ultimately, the Court implies that both the physical invasiveness and the content of the information are equally relevant to determining whether a search occurred, finding that no search occurred in this case because the canine sniff "is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure." The "method-based" prong of this test can and should be treated as an unfortunate holdover from pre-Katz days, just like the analysis in Bond and Riley. As this Article has argued, this analysis is both contrary to the spirit of Katz and dangerous to apply in an age of increasingly superior technology. If the federal agents in Place had been able to look through the sides of the defendant's suitcases with special goggles to see all of the contents—i.e., not just the narcotics but also the defendant's personal legitimate possessions—the observation would and should have been deemed a "search" even though the method used was less physically invasive than a canine sniff.

The Court's only other binary search case, United States v. Jacobsen, strongly supports this interpretation of Place. Not only does the Court's analysis focus solely on the result of the search in Jacobsen, it also re-visits Place and essentially repudiates the methods-based prong of the test that was used in that case:

Respondents attempt to distinguish Place, arguing that it involved no physical invasion of Place's effects, unlike the [government] conduct at issue here. However...the reason [the canine sniff in Place] did not intrude upon any legitimate privacy interest was that the governmental conduct could reveal nothing about noncontraband items. In other words, it was not the limited nature of the governmental conduct in Place which immunized the canine sniff; it was the limited amount of information which it could reveal.

In deciding Jacobsen itself, the Court applied a purely results-based test: first noting that the field test "could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine." The Court then reviewed the case law on "legitimate expectation of privacy," noting that an expectation of privacy for "wrongful" conduct is not one which society is prepared to

194. Place, 462 U.S. at 707.
195. Id. (emphasis added).
196. See critique of Bond, supra note 67 and accompanying text; critique of Riley, supra note 136 and accompanying text.
198. Id. at 124 n.24 (emphasis in the original).
199. Id. at 122.
recognize as "reasonable." If the results of the test are negative, "merely disclosing that the substance is something other than cocaine—such a result reveals nothing of special interest." If the result is positive, the government has merely learned that the defendant possesses narcotics, and "the interest in 'privately' possessing cocaine [is] illegitimate." Thus, "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest."

Although the Court has not considered a binary-test case in nearly twenty years, the implications for emerging technology are obvious. To take an example from the computer world, the federal government currently possesses an internet sifting device known as "Carnivore," which, when placed on a server on the internet, will store all e-mails passing through the server that are to or from a certain individual. The unfortunate name is actually meant to represent an improvement in this technology: predecessors to Carnivore merely stored all the e-mails without discrimination; now the software is able to recognize and retain only those that originate or are sent to a certain computer—thus, it only saves the "meat" and lets the irrelevant (and thus less appetizing) e-mails pass through unexamined. Any sorting based on content, however, must be conducted by a human being, who necessarily must read through many legitimate, constitutionally (and statutorily) protected messages before finding those which relate to the investigation.

200. Id. at 122-23 n.22 (quoting Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978)).
201. Id. at 123.
202. Id.
203. Id. (footnote omitted).
204. See E. Judson Jennings, Carnivore: U.S. Government Surveillance of Internet Transmissions, 6 VA. J.L. & TECH. 10 at § 9 (2001) (citing Stephen P. Smith et. al., ILL. INST. TECH. RES. INST., INDEP. REV. OF THE CARNIVOR E SYS. §3.4.1 at 3-10 (2000) [hereinafter IITRI Report]). Because analyzing each piece of data as it passes through would disrupt the flow of information, Carnivore copies all of the internet traffic and then searches through the copies it makes in order to determine which data packets are relevant. These copies are stored, and the rest of the copied transmissions are deleted. As the FBI has described the process: "Carnivore chews all the data on the network, but it only actually eats the information authorized by the court order." Id.
205. Id. § 5.
206. See id. § 56 (citing IITRI Report, §3.2.3, at 3-5). Under Title III, oral, wire, or electronic surveillance must be conducted "in a way that minimizes the interception of irrelevant communication." See 18 U.S.C. § 2518(5) (2000). For example, in conducting a wiretap, agents must monitor the wiretap continuously to ensure that irrelevant conversations are not recorded. If a conversation occurs that is not covered by the Title III order, the monitoring agent must shut off the recorder and allow the conversation to go unrecorded. See, e.g., Scott v. United States, 436 U.S. 128, 137-38 (1978) (holding that courts should evaluate the monitoring agents' actions in minimizing the interceptions under an objective reasonableness test, taking into account the facts and circumstances at the time of the interception). In the context of Carnivore, the analogous procedure is the
In order to monitor the electronic transmissions that are coming to or from a certain individual, government agents must acquire a court order. But consider an improved version of Carnivore—one designed only to eat a very specific kind of meat—which did not filter based on address but instead could sift through the content of all the transmissions passing through the server to which it was attached and copy only those which contained unambiguously illegal content: pictures of child pornography, for example, or orders to transfer funds in illegal amounts. Let us also assume that these transmissions would be copied, but they would not be opened or read by human beings without a warrant; thus, the only information that would result from this monitoring of the internet would be that a given transmission contained evidence of illegal activity. Under Place and Jacobsen, this device would not be conducting a "search," since it would only respond—like the trained dog or the chemicals in the field test—when there was unambiguous evidence of illegal activity, and it would report nothing other than the presence or absence of that activity. Applying a purely results-based test would lead a court to the same result as following Place; namely, that no search occurred. Granted, the method may seem oppressive—essentially warrantless monitoring of every transmission on the internet—but under Katz there are no Fourth Amendment implications because the only possible results of the surveillance do not infringe on legitimate expectations of privacy.

Outside of the computer context, sense-enhancing technologies could also be designed so as only to respond when there was unambiguous evidence of a crime. Devices could be created that could "detect the odor of deadly bacteria or chemicals for making a new type of high explosive," and could be used indiscriminately—

---

207. Either a Title III order (if the use of Carnivore represents an "interception" of electronic transmissions); or a search warrant under 18 U.S.C. § 2703(a) (if the use of Carnivore represents a reading of stored communications).

208. United States v. Kyllo, 533 U.S. 27, 47-48 (2001) (Stevens, J., dissenting). Justice Stevens expressed concern in his dissent that the Kyllo test would preclude using devices that could detect obvious contraband, such as the dog in Place, since such devices would reveal more than could otherwise be seen without physical invasion. However, since the Court in Jacobsen essentially held that there is no legitimate privacy interest in possessing
provided they did not reveal any further information about the area or person that they scanned. Small portable gun detectors are already being used by law enforcement agents throughout the country; if designed so that they reported only the presence or absence of a gun, and if only used in circumstances in which possession of a gun were clearly illegal, these devices could also be used on individuals without a warrant.

Although the constitutionality of such observations logically follows from applying a results-based test, this conclusion is controversial for two reasons, one doctrinal and the other practical. The doctrinal objection attacks one of the premises of the argument: that those engaged in illegal activity are not entitled to a legitimate expectation of privacy. Although the Supreme Court has supported this premise in Place and Jacobsen, some Justices and commentators have resisted the idea that the government could use binary-search devices indiscriminately.

This objection collapses, however, when one considers the extremely limited information provided by a truly binary search. For example, Professor David Harris worries that allowing the

illegal substances, the Court could easily harmonize the Kyllo test with the Place doctrine by confirming that Kyllo only applies to areas, activities and items in which an individual has a legitimate expectation of privacy. The specific language used in Kyllo already implies this, since it limits the test to "details of the home," which clearly deserve constitutional protection.

209. See generally Harris, supra note 177, at 5-14.

210. Meeting the second criteria may be a formidable challenge, however, given the proliferation of new laws easing restrictions on acquiring a permit to carry a handgun. As of 1995, twenty-five states allowed adults with a permit to carry concealed firearms. See Harris, supra note 177 at 56-57, 57 n.309; see also infra note 222 and accompanying text.

211. See United States v. Jacobsen, 466 U.S. 109, 136-43 (1984) (Brennan, J., dissenting) (arguing that courts should always look to the context in which an item is concealed, not the identity of the concealed item). See also Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-wide Search, 105 YALE L.J. 1093, 1100-11 (1996) (claiming that scanning citizens at random with such devices would violate their "right to be let alone"); Harris, supra note 177, at 41 (it is "flawed" to ignore the conditions and circumstances of the search and focus only on the discriminating method). But see Arnold H. Loewy, The Fourth Amendment as a Device for Protecting the Innocent, 81 MICH. L. REV. 1229, 1245-46 (1983) (detecting presence or absence of contraband does not violate the Fourth Amendment); Harris, supra note 177, at 43-44 n.240 (Professor Wayne LaFave argues that police need not have probable cause to use a "gun detector" that only conveys information about whether or not a person is armed in a context in which being armed is illegal) (citing letter from Wayne LaFave, Professor, University of Illinois College of Law, to David A. Harris, Professor, University of Toledo College of Law (Aug 18, 1995) (on file with Professor Harris)); Professor Christopher Slobogin also agreed with Professor LaFave's analysis, see id. (citing letter from Christopher Slobogin, Professor, University of Florida College of Law, to David A. Harris, Professor, University of Toledo College of Law (Sept. 5, 1995) (on file with Professor Harris)).
warrantless use of devices as long as they are "unintrusive and discriminating" would result in a Fourth Amendment that would progressively weaken as technology improved. As noted above, this is indeed a critical concern in modern society, and the primary reason that the method of the surveillance should not matter in determining whether a search has occurred. But Professor Harris ends up conflating content discrimination with broader methods-based considerations (such as "intrusiveness"), and thereby conjures up a society where law enforcement can conduct "visual observation" of items inside a house. Of course, a truly binary search could never be a "visual observation"—it would only provide the law enforcement agent with a "yes" or a "no"—and, as the Supreme Court noted in Jacobsen, neither answer implicates any legitimate expectation of privacy.

But this first objection highlights the importance of the second objection, which focuses on how binary tests might work in practice. In an ideal world, law enforcement officials would design devices that (1) only produced a binary response when used and conveyed no other information about the person or area searched; (2) were 100% accurate; and (3) that only responded when the individual possessed an item—narcotics, firearms, child pornography, etc.—that was clearly illegal. In reality, such perfect devices might be difficult, if not impossible, to create (though a child-pornography-sniffing Carnivore might be quite feasible). Neither Place nor Jacobsen undertook an examination as to the accuracy of the binary search; the Place Court merely noted that the dog was a "trained narcotics

212. Id. at 43.
213. Id. at 44.
214. Opponents of warrantless binary searches offer up a weaker objection to the premise, namely that a search cannot be justified after the fact merely because it resulted in the finding of contraband. See, e.g., Jacobsen, 466 U.S. at 140 (Brennan, J., dissenting) ("The Court [in Place and Jacobsen] has ignored the fundamental principle that a search prosecuted in violation of the Constitution is not made lawful by what it brings to light") (citations and quotations omitted); Harris, supra note 177, at 41 ("It seems almost too basic a proposition to restate, but what police find as a result of a search can play no part in determining whether the officers violated the Fourth Amendment in conducting the search."). This objection misses the point entirely; a binary search is not constitutional because of what it does find, but because of what it is capable of finding. Under Place and Jacobsen—and under the results-based interpretation of the Katz test—a binary search is incapable of revealing any information that deserves a legitimate expectation of privacy.

215. Just a few months before Place was decided, Professor Arnold H. Loewy hypothesized just such an "evidence-detecting divining rod" which could be used by police indiscriminately to locate contraband. See Loewy, supra note 211, at 1244. As real-life (and thus imperfect) examples of such "divining rods," Professor Loewy put forward drug-sniffing dogs and undercover agents (assuming they do not entrap their targets). Id. at 1245-51.
detection dog" that reacted "positively" to one of the bags; a footnote in Jacobsen simply states that liquids in the test will take on certain colors when cocaine is present. Since these precedents implicitly assume (whether correctly or not) 100% accuracy from the binary search in question, they provide little guidance about analyzing cases in which the accuracy of the device might be less than perfect.

If binary searches do become more common (as they are likely to, given their constitutionality under Place and their growing feasibility as technology improves), courts will have to define how close devices must come to reaching all three of the above criteria in order to be considered a true binary search device. In order to satisfy the first criterion, technology will have to be created that can automatically sift through images or other input which may reveal too much information and mechanically determine whether the information contains evidence of contraband. For example, some current models of gun detectors produce a grainy picture of dark metallic objects showing up against a gray outline of the body and rely on the user's expertise to determine whether the outline represents a weapon, but because this imparts more information than a mere "yes" or "no" to the operator, it cannot be considered a binary search. Any attempt to create an improved version of Carnivore will meet with the same problem.

Unfortunately, in automating the evaluative aspect of the search, there is a good chance that the device will become less accurate, thus creating problems with the second criterion. In other words, a trained law enforcement officer is probably better than a pre-programmed algorithm in determining whether an image of a metal object is a firearm; likewise, a human being is probably better equipped than a software program in determining whether an image is child pornography. Thus the problem of false positives is likely to

216. See Place, 462 U.S. at 699. The concurrence does note that the District Court found the dog search had been conducted in a way that avoided a "tainted reaction from the dog." Id. at 723 n.3 (Blackmun, J., concurring) (citation omitted).

217. See Jacobsen, 466 U.S. at 112 n.1.

218. Obviously, drug-sniffing dogs are not 100% accurate, and in some cases can be wildly inaccurate. In Doe v. Renfrow, 475 F. Supp. 1012 (N.D. Ind. 1979), modified by 631 F.2d 91 (7th Cir. 1980), cert. denied, 451 U.S. 1022 (1981), a dog was employed to sniff all 2,763 students in a school. The dog found fifty "positives," but only seventeen of those fifty were in possession of contraband. This translates into a respectable 1.2% false-positive rate (33 false positives out of the 2,780-student sample), but a rather poor positive predictive value of 34% (defined as the thirty-three innocent students out of the fifty positive responses).

219. See Harris, supra note 177, at 11-12.

220. Justice Potter Stewart's famous definition of obscenity, "I know it when I see it," Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring), probably works only
increase as the devices are altered to become truly binary devices. What percentage of accuracy is necessary to survive constitutional scrutiny (95%? 99%?) is a difficult question.

This question is further complicated by the third criterion—how likely is it that the item that is detected is illegal? At least one critic of binary searches has concluded that if the item being detected is not certain to be contraband, the binary search doctrine might not apply at all. Even if the binary search doctrine does apply, the chance that the item being detected might be legal in this context must be factored into the technical accuracy of the device. For example, if a gun detector is 95% accurate, but 20% of the guns it detects are possessed lawfully, the device only accurately detects an illegal item 72% of the time.

How courts will balance these criteria is yet to be seen. But given the legal and technical confluence of factors (that is, an established constitutionality of binary searches combined with the advent of computer "sniffers" such as Carnivore and sophisticated sense-enhancing technologies such as gun detectors), law enforcement agents are almost certain to utilize binary search devices more and more frequently in the future. Justice Brennan's hypothetical in his Jacobsen dissent no longer sounds like science fiction: "[I]f a device were developed that could detect, from the outside of a building, the presence of cocaine inside, there would be no constitutional obstacle to the police cruising through a residential neighborhood and using the device to identify all homes in which the drug is present."

for people and not computers; thus, what is an obvious and intuitive task for humans could conceivably become a challenging task for software engineers.

221. See Harris, supra note 177, at 58 (citations omitted).

If one of the central underpinnings of [Place and Jacobsen] is that the method in question detects only contraband, the new concealed weapons laws make for a drastically different outcome. Simply put, under these laws concealed guns are not always contraband. Therefore, applying the Place and Jacobsen reasoning would seem questionable at best.

222. This concern is most applicable to gun detectors, since many people may carry guns legally in a number of states. As of 1998, "[thirty-one] states have enacted 'shall issue' laws, which require local law enforcement authorities to issue concealed-handgun-carrying permits to any applicant who meets a set of specific criteria." Jens Ludwig, Concealed-Gun-Carrying Laws and Violent Crime: Evidence from State Panel Data, 18 INT'L REV. OF L. & ECON. 239, 240 (1998). In addition to the "shall issue" states, there are a number of "may issue" states who allow citizens to carry concealed firearms under more stringent requirements. As of 2002, forty-three states in the country had laws allowing adults to carry concealed firearms with a permit. See http://www.bradycampaign.org; www.packing.org (only Illinois, Kansas, Missouri, Nebraska, New Mexico, Ohio, and Wisconsin do not allow citizens to carry concealed firearms).

Justice Brennan later terms this scenario "Orwellian," and indeed it is chilling to imagine the police freely and indiscriminately "scanning" all of our houses and our persons. But again, if one considers the extremely limited nature of the information the police receive with their scan—the presence or absence of illegal activity—the instinctive reaction to such techniques seems misplaced. After all, police already cruise down residential streets monitoring for criminal activity in far less efficient ways: they listen for screams, gunshots, threats, or other loud noises; they look for windows or doors that are broken or inexplicably open; they might observe or even follow "suspicious" actors for extended periods of time. In conducting all of these activities, the police are intruding into our lives far more than they would with a "narcotics detector," since the vast majority of what they see and hear under traditional circumstances—the results of their observations—has nothing to do with illegal activity. Once again, when one considers the results of such binary searches—even on a widespread scale—and compares them to the results of normal police activity, they fit comfortably within Fourth Amendment jurisprudence.

Conclusion

In deciding Katz, the Supreme Court took a dramatic step towards adopting a results-based test for applying the Fourth Amendment to new technologies. However, the language in Katz was sufficiently vague to muddle the distance that was traveled in that step. This ambiguity has created a troubling dissonance in Fourth Amendment jurisprudence. It is now time for courts to clarify the mandate in Katz and confirm that the landmark case rendered irrelevant any consideration of the methods used in government surveillance. This clarification is becoming only more critical as technology continues to advance, allowing law enforcement officials access to more and more intimate information without any physical intrusion—and indeed without the target's knowledge. We must learn from the absurdity in the case law before Katz, and at the same time consider the implications of the surveillance technologies which will become more ubiquitous as time progresses. In this way both the

224. Id.

225. A slightly related objection might be constructed around the many laws that are still on the books but never enforced or enforced halfheartedly in many jurisdictions—laws prohibiting the use of marijuana, for example, or sodomy laws. But this objection ultimately would be attacking the efficiency of such searches, not their intrusiveness; if it is troubling to people that, say, a "marijuana detector" would make it impossible for anyone to smoke marijuana even in the privacy of their own home, the appropriate response, of course, is to amend the law which makes marijuana illegal. See Loewy, supra note 211, at 1248 n.86.
past and the future lead us to a better understanding of Katz—one which looks beyond the method of the search.