FORTRESS OF SOLITUDE OR LAIR OF MALEVOLENCE? RETHINKING THE DESIRABILITY OF BRIGHT-LINE PROTECTION OF THE HOME

LEE C. MILSTEIN*

Fourth Amendment jurisprudence currently affords the home great protection against searches by law enforcement; since its decision in Kyllo v. United States, *the Supreme Court has even protected the home from non-invasive scans. In this Note, Lee C. Milstein argues that focusing on the location of the search or scan rather than on the nature of the activity has a perverse effect on the protection of privacy interests. Scanning technologies that alert only to the presence of contraband or illegal activities, for example, could prevent the need for traditional searches of homes that incur substantial collateral damage to an individual's privacy rights. At the same time, the focus on the home allows law enforcement virtually unfettered powers of surveillance in public, which can give law enforcement officers significant amounts of information about an individual. Milstein concludes by proposing a new approach to Fourth Amendment jurisprudence that would permit the use of highly particularized scanning technologies for law enforcement and by exploring the potential for the development of new technologies that would minimize invasions of privacy while making the enforcement of the criminal law more effective under this alternate approach.*

INTRODUCTION

Imagine a world in which a police officer is permitted to follow you around during a typical day. The officer does not enter private establishments with you, does not listen in on your conversations, and does not read any of your documents, but does write down the name of every location you visit and the name of every person with whom you interact. After several days, the officer notices that you are an acquaintance of a known heroin dealer, and that you are a regular customer in a store that sells drug paraphernalia.

So, the officer approaches you on the street, in front of your office building, and asks if he can frisk you. Perhaps, not knowing

* B.A., 2000, University of Rochester; J.D., 2003, New York University School of Law. I would like to thank Professor Roger Schechter for the extraordinary effort that he put forth and for his guidance in writing this Note. I would also like to thank Professor Louis Michael Seidman, whose Criminal Procedure class helped mold my views. Additionally, I would like to thank the members of the *New York University Law Review* for their thoughtful feedback. Finally, I would like to thank the Cognitive Science Department at the University of Rochester for its inspiration.

your legal rights and not desiring to seem uncooperative, you consent to the frisk. The officer conducts the frisk, finds nothing, and lets you go.

Perhaps you do not consent to the frisk, so instead of searching you on the street, the police officer takes the evidence he has collected, goes to a magistrate, and convinces the magistrate that there is probable cause to believe that you possess illegal drugs. The magistrate grants the police officer a warrant to search your house. The officer arrives at your house, serves you with the warrant, and ransacks your home. He finds no drugs and leaves, but not before scaring your family, moving all of your belongings, looking through your unmentionables, and providing gossip for the neighbors. While there are no criminal repercussions, these police actions are laden with collateral damage.

Now imagine another situation in which a police officer walks his beat with a small device, similar to a radar gun, which he periodically aims at various individuals as they pass by, without stopping those individuals, drawing attention to those individuals, or following those individuals around. Additionally, imagine that this device is capable of identifying the chemical signature of heroin within its path and, upon identifying this signature, displaying an alert; if the signature is not present, the device gives no readout whatsoever. The officer randomly aims the device at you, no signature is identified, and you continue with your day in ignorance; you are not disturbed by the activity and, in fact, do not even know it is happening. What if, rather than following you around for a few days—finding out who you know and where you shop for the purpose of obtaining a warrant—the police officer simply aims this device at the houses on his beat? No drugs are detected in your house, and you suffer none of the collateral damage described above. Which situation would you prefer?

This Note argues that the second scenario, which relies on scanning technology,[1] is more desirable. Nevertheless, scanning has been limited and, in some cases, declared unconstitutional by the Supreme Court for violating the Fourth Amendment.[2] Perversely, the first scenario, which relies on surveillance activity, has the full backing of the

---

[1] For an explanation of scanning technology, see infra note 44 and accompanying text, as well as infra, Part III.C.

[2] U.S. Const. amend. IV states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

law. This Note argues that declaring scanning activity unconstitutional when it targets a specific area—the home—indicates a problematic scheme for identifying unconstitutional searches. As a result, this Note proposes a new scheme that fixes the problems arising out of current Supreme Court jurisprudence and more honestly accounts for past decisions.

Part I of this Note outlines the relevant Fourth Amendment jurisprudence. It explains that the current doctrine claims to focus on "reasonable expectations of privacy," but has muddied the proverbial waters with exceptions and recharacterizations. It identifies the Supreme Court's decision in *Kyllo v. United States*,[3] which drew a bright line surrounding the home, as indicative of a problematic departure from traditional Fourth Amendment doctrine. Importantly, though, this Note does not argue that the outcome of *Kyllo* is incorrect, but rather that the justification is flawed and the holding too broad.

Part II describes the difficulties with current Fourth Amendment jurisprudence. It explains that most Fourth Amendment case law supports the notion that physical searches and seizures are suspect because of the potential for collateral damage, rather than because of the area invaded. Still, current search and seizure doctrine creates a bright-line rule protecting a specific area—the home—with little consideration of the privacy and collateral damage concerns actually at stake. This Part explains why the Fourth Amendment doctrine is simultaneously over- and under-inclusive and describes some of the undesirable implications of this dichotomy.

Part III suggests a new dichotomy that results in a more coherent and predictable Fourth Amendment jurisprudence. Specifically, this Part suggests that the correct dichotomy should be one that focuses on intrusiveness, embracing binary scans and rejecting intrusive police actions, instead of one that focuses on the physical boundaries of the home. That is, a search should be illegal only if it is intrusive or causes collateral damage; a search should not be illegal merely because of the area to be searched. This Part goes beyond addressing the problems outlined in Part II by exploring policy justifications for the new dichotomy and by explaining that the Court's jurisprudence appears more consistent when viewed through this lens. It will also explore hypothetical situations in which the implication of the proposal could lead to partnerships between law enforcement and technology developers to reduce crime and increase privacy protections.

---

[3] 533 U.S. 27 (2001).

I
THE LAY OF THE LAND: CURRENT FOURTH AMENDMENT JURISPRUDENCE

A. *From Ratification to* Katz v. United States: *A Brief Overview*

The Fourth Amendment was adopted to provide protection against overzealous government.[4] The Framers of the Constitution understood that "power tends to corrupt,"[5] and that authorities could use their power to intimidate and destroy their opponents.[6] To prevent this abuse of power, the Framers constructed the Constitution with safeguards such that certain rights were given to the people.[7]

---

[4] See, e.g., United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) ("The available historical data show . . . that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government . . . ."); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("[The Framers] conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."); William W. Greenhalgh & Mark J. Yost, In Defense of the "Per Se" Rule: Justice Stewart's Struggle to Preserve the Fourth Amendment's Warrant Clause, 31 Am. Crim. L. Rev. 1013, 1017 (1994) ("The Framers in 1789 feared precisely what the English feared in 1621 and precisely what we expect the Fourth Amendment to protect us from today: an arbitrary, capricious, and overreaching government."); Quin M. Sorenson, Losing a Plain View of *Katz*: The Loss of a Reasonable Expectation of Privacy Under the Readily Available Standard, 107 Dick. L. Rev. 179, 198-99 (2002) ("The purpose of the Amendment was to protect the privacy of individual [sic] as against arbitrary deprivations by government officials, who may 'engage in surveillance with more zeal and for different purposes than private citizens.'" (quoting United States v. Kim, 415 F. Supp. 1252, 1256 (D. Haw. 1976))).

The Fourth Amendment was not adopted because the Framers of the Constitution believed that citizens had a specific right to privacy; thus, advocates of a right to privacy have had to find its basis elsewhere. See, e.g., Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890) (finding privacy right in penumbra of Supreme Court Fourth Amendment interpretations—were privacy as such specifically envisioned, it would not need such circuitous explanation). Although this Note will not delve deeply into the issue, it is conceivable that privacy is not even a true desire in our society. It is worth considering the possibility that what we as a society really want is understanding and tolerance. Consider that people might only value privacy because they are afraid of what the reaction of the populace would be if it were to learn of their inner desires. Society deems many desires to be perverse. So, people value the ability to keep their thoughts secret and monitor what parts of themselves will be exposed to society at large in a very conscious way. Devaluing privacy would require monumental changes in the way people view each other. Still, if people could recognize the thoughts and bodily functions of others as natural to that person, without judging, very few "privacy" issues would be so important; corrupt invasions by government agents, however, would nevertheless be highly undesirable.

[5] Letter from John Emerich Edward Dalberg, First Baron Acton, to Bishop Mandell Creighton (Apr. 3, 1887), in 1 The Life and Letters of Mandell Creighton 372 (Louise Creighton ed., 1904) quoted in The Columbia World of Quotations (Robert Andrews et al. eds., 1996), available at http://www.bartleby.com/66/9/2709.html ("Power tends to corrupt, and absolute power corrupts absolutely. Great men are almost always bad men . . . .").

[6] See supra note 4 and accompanying text.

[7] See supra note 4 and accompanying text.

The Fourth Amendment bestows the right to be free from unreasonable searches and seizures.[8] Notably, the only requirement actually articulated by the text of the Fourth Amendment is that a search or seizure not be "unreasonable."[9] Still, the Supreme Court has adopted a default rule that a warrant is required prior to the execution of a

---

[8] U.S. Const. amend. IV. Prior to 1928, the term "unreasonable" was understood as a prohibition only against a general warrant. See David A. Sullivan, Note, A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology, 44 Ariz. L. Rev. 967, 970-71 (2002) (providing history of "Fourth Amendment Search Analysis"). A general warrant is "[a] warrant that gives a law-enforcement officer broad authority to search and seize unspecified places or persons; a search or arrest warrant that lacks a sufficiently particularized description of the person or thing to be seized or the place to be searched." Black's Law Dictionary 1579 (7th ed. 1999).

[9] For the text of the Fourth Amendment, see supra note 2. For evidence that the original purpose of the warrant clause was to provide agents a defense to tort actions, see Richard A. Posner, Rethinking the Fourth Amendment, 1981 Sup. Ct. Rev. 49, 51 (1982) ("Where the search or seizure is done under warrant, the second clause of the Fourth Amendment sets forth the requirements that must be satisfied for possession of the warrant to constitute a defense to a tort action."); see also California v. Acevedo, 500 U.S. 565, 581 (1991) (Scalia, J., concurring) ("The Fourth Amendment does not by its terms require a prior warrant for searches and seizures; it merely prohibits searches and seizures that are 'unreasonable.' What it explicitly states regarding warrants is by way of limitation upon their issuance rather than requirement of their use."); Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 762-63 (1994) (discussing textual interpretations of Fourth Amendment and discounting interpretations that mandate warrants).

There are, of course, many exceptions, including "a warrant for another object, hot pursuit, [or] search incident to lawful arrest." Horton v. California, 496 U.S. 128, 135-36 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)); see Chimel v. California, 395 U.S. 752, 762-63 (1969) ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape."); Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (finding no violation of Fourth Amendment based on hot pursuit exception to warrant requirement); Schmerber v. California, 384 U.S. 757, 770-71 (1966) (using exigency exception to warrant requirement to justify taking of blood sample to determine blood alcohol content in drunk driving case). Another exception is the car search exception. See, e.g., *Acevedo*, 500 U.S. at 580 ("The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.").

The safeguard envisioned by the Framers was review of the reasonableness of a search or seizure by an independent magistrate. See Thomas Y. Davies, Recovering the Original Fourth Amendment, 98 Mich. L. Rev. 547, 576-90 (1999) (discussing Framers' belief that subordinate officers should not be given power to intrude without direction from higher authority). If the magistrate determined after the fact that an official had conducted a search or seizure in an unreasonable manner, that official would be civilly liable. See Akhil Reed Amar, The Bill of Rights as a Constitution, 100 Yale L.J. 1131, 1178 (1990). An official could insulate himself from liability by appearing before a magistrate in advance to obtain a warrant. Id. Since that time, however, the law has shied away from direct liability for government officials behaving in their official capacities, and has limited the situations in which government bodies can be subject to suit. See, e.g., Williams Elec. Co. v. Honeywell, Inc., 772 F. Supp. 1225, 1229 (N.D. Fla. 1991) ("[I]t appears well-settled that federal agencies and their officials acting in their official capacity are immune from federal antitrust liability.").

search or seizure.[10] The Court has also recharacterized the reasonableness requirement of the original text so that probable cause must be present even when a warrant is unnecessary.[11] However, there are persuasive reasons to believe that neither the text of the Amendment, nor the intent of the Framers specifically required either one of these things.[12]

An overview of the Supreme Court's Fourth Amendment decisions demonstrates the departure from what was contemplated by the Framers or required by the text of the Amendment. Prior to 1967, Fourth Amendment jurisprudence declared that the only way government agents could violate rights in the realm of searches and seizures was to commit a physical trespass.[13] However, in deciding *Katz v.*

---

[10] As has been succinctly summarized:

> Today it is well established in the opinions of the Supreme Court that searches and seizures conducted without a warrant are presumed to be unreasonable. The language of the Court is that "searches conducted outside the judicial process, without prior approval by judge or magistrate [sic] are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." . . . The Court has deemed this "a cardinal principle" of Fourth Amendment law.

Stephen A. Saltzburg & Daniel J. Capra, American Criminal Procedure: Cases and Commentary 77 (6th ed. 2000) (quoting Mincey v. Arizona, 437 U.S. 385, 390 (1978)).

[11] See, e.g., Carroll v. United States, 267 U.S. 132, 153 (1925) (holding that car search is legitimate without warrant so long as there is probable cause). The actual text of the Fourth Amendment requires probable cause to secure a warrant, not to render a search reasonable, but holdings such as this one illustrate that the Court has extended the requirement of probable cause to all search contexts. See, e.g., Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (applying *Carroll* to warrantless car search based upon probable cause, Court found "that the Framers would have regarded such a search as reasonable").

[12] See Payton v. New York, 445 U.S. 573, 621 (1980) (Rehnquist, J., dissenting) ("There is significant historical evidence that we have over the years misread the history of the Fourth Amendment in connection with searches, elevating the warrant requirement over the necessity for probable cause in a way which the Framers of that Amendment did not intend."). Rehnquist's statement cites Telford Taylor's *Two Studies in Constitutional Interpretation*, which states in part:

> There is no evidence that suggests that the framers of the search provisions of the federal and early state constitutions had in mind warrantless searches incident to arrest. If there was any 'original understanding' on this point, it was that such searches were quite normal and . . . 'reasonable.'

Telford Taylor, Two Studies in Constitutional Interpretation 38-50 (1969). Furthermore, academics interpreting Fourth Amendment law permitting a stop and frisk have stated: "[It] did not insist that all . . . searches and seizures be preceded by warrants . . . and more dramatic still, [it] did not insist that all warrantless intrusions be justified by probable cause." Akhil Reed Amar, 72 St. John's L. Rev. 1097, 1098 (1998); see supra note 9 and accompanying text.

[13] See, e.g., Goldman v. United States, 316 U.S. 129, 135-36 (1942) (finding no violation of Fourth Amendment when detectaphone placed against wall for purposes of overhearing conversation based on lack of physical trespass); Olmstead v. United States, 277 U.S. 438, 466 (1928) ("[T]he Fourth Amendment [has not been violated] unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible

United States[14] in 1967, the Supreme Court abandoned the trespass standard. This landmark decision held that a listening device attached to the outside of a telephone booth amounted to an unconstitutional search, not because there was a physical trespass, but because it infringed on a person's reasonable expectation of privacy.[15]

The Court used this decision to create a two-pronged test for identifying an unconstitutional search.[16] The first prong of the test asks if the subject of the search has an actual expectation of privacy. The second prong asks if society is prepared to recognize that expectation as reasonable.[17] This decision changed the frame of reference for thinking about the constitutionality of searches from one centered around a physical location to one based more on a theoretical right to privacy.

Since *Katz*, courts and scholars alike have struggled to determine when a person's expectation of privacy is reasonable. Courts have held, however, that reasonableness is only a factor of the inquiry if the activity is actually a search.[18] In so holding, courts have explained that neither public surveillance nor scans for contraband constitute searches.[19] Thus, no reasonableness inquiry is required for surveillance or scans.

B. Search v. Nonsearch Activity: Surveillance and an Introduction to the Scan

Even before determining the reasonableness of a search, a court must determine if the law enforcement activity constitutes a search at

---

material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure.").

[14] 389 U.S. 347 (1967).

[15] The majority opinion actually never uses the phrase "reasonable expectation of privacy." The first mention of this phrase appears in Justice Harlan's concurrence. Id. at 360 (Harlan, J., concurring). What the majority does say is that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Id. at 351. The Court continues by observing that it is "clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." Id. at 353.

[16] Id. at 360-61 (Harlan, J., concurring).

[17] Id. at 361 (Harlan, J., concurring).

[18] Kyllo v. United States, 533 U.S. 27, 31 (2001) (characterizing question of "whether or not a Fourth Amendment 'search' has occurred" as "antecedent question").

[19] For support for the argument that public surveillance is not a search, see *Hester v. United States*, 265 U.S. 57, 59 (1924) ("[I]t is enough to say that . . . the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields. The distinction between the latter and the house is as old as the common law."). For the argument that a scan is not a search, see infra Part I.B; see also Louis Michael Seidman, The Problems with Privacy's Problem, 93 Mich. L. Rev. 1079, 1087 (1995) (describing collateral damage as only real indication of unreasonableness for Fourth Amendment searches).

all.[20] If no search occurs, Fourth Amendment protections do not apply, and no violations can occur.[21]

Public surveillance is not generally considered a search.[22] The Supreme Court repeatedly has held that there is no reasonable expectation of privacy in activity that occurs in public.[23] Thus, if a law enforcement agent[24] witnesses public activity, no search has taken place. This doctrine captures the common-sense observation that a police officer who, while walking down the street, witnesses a mugging or a drug deal should be able to do something about it.[25]

The notion of what is public, however, has been given an expansive reading. For example, the Court has found that no search took place where police uncovered activity or objects that were exposed to public view. The Court has held that wide-open areas of fields that are nonetheless private property can be considered public for Fourth Amendment purposes.[26] It has even held that airspace is public and thus there is no expectation of privacy in areas that can only be viewed from aircraft passing overhead.[27] Additionally, lower courts have held that a law enforcement agent can use binoculars to look into an unobstructed window of a residence, so long as the agent is

---

[20] *Kyllo*, 533 U.S. at 31.

[21] See Florida v. Riley, 488 U.S. 445, 450-52 (1989) (holding surveillance from helicopter flying above mandatory minimum altitude not subject to Fourth Amendment scrutiny).

[22] *Hester*, 265 U.S. at 59.

[23] See, e.g., United States v. Dunn, 480 U.S. 294, 300 (1987) ("[T]he Court observ[ed] that the distinction between a person's house and open fields 'is as old as the common law.'" (quoting *Hester*, 265 U.S. at 59) (citations omitted)); Oliver v. United States, 466 U.S. 170, 178 (1984); United States v. Katz, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."); Thompson v. Johnson County Cmty. Coll., 930 F. Supp. 501, 507 (D. Kan. 1996), aff'd, 108 F.3d 1388 (10th Cir. 1997) ("[V]ideo surveillance 'in public places . . . does not violate the fourth amendment; the police may record what they normally may view with the naked eye.'" (quoting United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991))).

[24] By law enforcement agents, this Note refers to all police officers, federal agents, or other government representatives acting under the color of law. The terms police officer, law enforcement officer, law enforcement agent, government official, government agent, and government officer will be used interchangeably throughout the piece.

[25] See California v. Greenwood, 486 U.S. 35, 41 (1988) ("[P]olice cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.").

[26] California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (holding warrantless aerial surveillance of backyard was not search for Fourth Amendment purposes because there was no reasonable expectation of privacy); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding aerial photography of open areas of industrial plant analogous to open field, not the "curtilage" of a dwelling).

[27] See *Dow Chemical*, 476 U.S. at 239; see also Florida v. Riley, 488 U.S. 445, 450-51 (1989).

located in a legal position.[28] Although the Supreme Court has not heard this issue, these lower courts have classified this activity as "not a search."[29]

Accordingly, law enforcement agents are justified in monitoring any activity that occurs in public, and even recording such activity for later use.[30] For the purposes of this Note, such activity will be called "surveillance," and any technology used to aid in the monitoring or recording will be called "surveillance technology."[31] The fundamental characteristic of surveillance technology is that it monitors, observes, and records, in contrast to what this Note will call "scanning technology," which refers to devices that monitor and only alert upon given stimuli.[32]

These lower court holdings regarding what constitutes a "search" fail to protect (the unreasonable expectation of) privacy rights surrounding activity that takes place in public. In fact, these decisions allow law enforcement agents to monitor actively an individual's every "public" move. This seems counterintuitive for a rule intent on protecting privacy.

For the past two decades, another type of nonsearch activity has called into question the extent of reasonable expectations of privacy: the scan. In *United States v. Place*,[33] the suspicious behavior of an airline passenger led authorities to believe that he was carrying drugs from Miami to New York.[34] Upon arrival in New York, the police confronted Raymond Place and ultimately detained his luggage so that a trained police dog could sniff it for the presence of narcotics.[35] Place argued that this seizure and sniff constituted a violation of his

---

[28] See, e.g., People v. Oynes, 920 P.2d 880, 883 (Colo. Ct. App. 1996); State v. Thompson, 241 N.W.2d 511, 512-13 (Neb. 1976).

[29] *Oynes*, 920 P.2d at 883; *Thompson*, 241 N.W.2d at 512-13.

[30] So-called "red light cameras" are one example of the recording of public surveillance for later use. These cameras are used to snap pictures of motorists who run red lights; tickets for the infractions are later mailed to the registered owners of the cars. For more information on these cameras, see generally Steven Tafoya Naumchik, Stop! Photographic Enforcement of Red Lights, 30 McGeorge L. Rev. 833 (1999); Mary Lehman, Comment, Are Red Light Cameras Snapping Privacy Rights?, 33 U. Tol. L. Rev. 815 (2002).

[31] Such technology might include binoculars as in *Oynes*, 920 P.2d at 881, or aerial photography as in *Dow Chemical*, 476 U.S. at 229, or maybe even flashlights, see infra text accompanying notes 60 and 87.

[32] Scanning technology will be described in detail infra Part III.C.

[33] 462 U.S. 696 (1983).

[34] Id. at 698 (describing behavior while in line, discrepancies in addresses on luggage tags, and comments made to police).

[35] Id. at 698-99. Although the central holding in this case was that law enforcement agents may detain luggage for reasonable periods of time in order to conduct a canine sniff, the question of whether a canine sniff violates the Fourth Amendment is essential to the holding. Id. at 697-98.

Fourth Amendment rights. The Supreme Court concluded that a "sniff" by a dog trained to alert only to the presence of narcotics did not constitute a search because of the limited "manner in which the information is obtained and . . . the content of the information revealed by the procedure."[36] This holding suggests that the amount and type of collateral damage associated with a search is important to the determination of reasonableness.[37] Lending persuasiveness to this suggestion, the Court also noted that the canine sniff "ensures that the owner of the property is not subjected to the embarrassment and inconvenience entailed in less discriminate and more intrusive investigative methods."[38] The Court in *Place* explained, however, that a canine sniff was sui generis, and did not implicate the same concerns that other search-like behavior may generate.

Later, in *United States v. Jacobsen*,[39] the Court recognized that there could be other narrowly tailored "nonsearch" investigative activity, and extended the reasoning from *Place* to chemical field-tests.[40] The field tests described in *Place* alert authorities only to whether a substance is or is not cocaine.[41] Here, an accident at a Federal Express office damaged a package, leading employees to open the package and view the contents. They believed the contents were narcotics and alerted the DEA.[42] Upon arrival, the DEA tested the exposed substance. The Court held that such testing by the DEA was not an unlawful search or seizure because "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy."[43]

---

[36] Id. at 707. The Court determined, correctly, that in order for the protections of the Fourth Amendment to apply, there must actually be a search or seizure, so the first inquiry courts address is always the presence or absence of one of these qualifying activities. A search is defined as the act of "mak[ing] a thorough examination of; look[ing] over carefully in order to find something; explor[ing]." The American Heritage Dictionary of the English Language 1571 (4th ed. 2000). It might appear to a nonlawyer that a sniff that thoroughly probes an area for the presence of narcotics is a search, but, rather than focusing on the Fourth Amendment prohibition of "unreasonable" searches and seizures, the Court has decided to characterize certain otherwise search-like behavior as not a search. In doing so, the Court has adopted its own formulation of the word, and made the doctrine more complex than plain meaning requires.

[37] The role of collateral damage in ascertaining reasonableness is discussed further infra Part II.B.1.

[38] *Place*, 462 U.S. at 707.

[39] 466 U.S. 109 (1984).

[40] Id. at 123-24.

[41] Id. at 123.

[42] Id. at 111. The holding in *Jacobsen* includes an analysis of the interaction between a private search to discover narcotics and a search by DEA agents, but it discusses in a separate analysis the constitutionality of the seizure of a potential narcotic substance. Id. at 115-18, 122-24.

[43] Id. at 123.

In these cases, the Court has indicated that if the law enforcement agents have a right to be present in a given location, searches constructed in such a way that only illegal activity can be identified are constitutional.[44] The fundamental characteristic of scanning technology is that it monitors and alerts to a given stimulus, but otherwise provides no information. After *Place* and *Jacobsen*, it was understood that any scan, i.e., any search so narrowly tailored that it identifies only illegal activity, does not sufficiently infringe on privacy to constitute a violation of the Fourth Amendment.[45]

C. *The Introduction of the* Kyllo *Doctrine*

Although it seemed clear that the Supreme Court would not consider scans to be searches, the cases suggesting this interpretation have been limited in scope, if not partially overruled. The Court called these cases into question by drawing a bright line that limits the ability of law enforcement to use even nonsearch investigative activities to gather information about the activities inside an individual's home. In 1985, the Second Circuit, in *United States v. Thomas*, determined that a canine sniff of the hallway of an apartment building constituted an illegal search because it intruded on the expectations of privacy that are unique to the home.[46]

This case questioned the legality of a search conducted pursuant to a warrant, which was granted in part on the basis of a positive alert of a dog sniff. The sniff took place in the hallway of a shared apartment building. The defendant owner of the apartment claimed that the sniff constituted an illegal search in and of itself because it revealed information about the interior of his home. The Second Circuit accepted this argument:

> It is one thing to say that a sniff in an airport is not a search, but quite another to say that a sniff can *never* be a search. The question

---

[44] See Saltzburg & Capra, supra note 10, at 57 ("[T]he Supreme Court has held that there is no legitimate expectation of privacy in illegal activity. Therefore, an investigative activity is not a search if it can *only* reveal illegal activity."). The illegal activity in most cases was the possession of narcotics.

For the purposes of this Note, such binary "searches" are called "scans," and the technology enabling scans is called "scanning technology." Currently, there are not many functionally accurate and effective scanning technologies. Those that exist and have been proven accurate have been discussed in these two cases. Still, it is likely that more scanning technology will be developed in the future. This is especially true if the value of scanning technology is fully understood and embraced by the courts as proposed in this Note. See infra Part III.C.

[45] See supra notes 43-44 and accompanying text.

[46] 757 F.2d 1359, 1366-67 (2d Cir. 1985).

always to be asked is whether the use of a trained dog intrudes on a legitimate expectation of privacy.[47]

The court answered this question in the affirmative because there is a "heightened privacy interest that an individual has in his dwelling place."[48] The court seemed to have considered the expectation of privacy surrounding one's home to be so great that even a "nonsearch" for the presence or absence of contraband that intruded in no other way would be unlawful. Supreme Court rulings in the previous two years supported this idea. In these cases, the Court held the Fourth Amendment limited law enforcement's ability to use tracking devices, known as beepers, to monitor the location of items once the items have entered a home.[49]

Still, even though this reasoning is supported by Supreme Court precedent, no other circuit has followed the reasoning in *Thomas* in other situations outside of the context of the home.[50] Indeed, no other circuit has even entered into an analysis of whether the area invaded evidenced any of the same heightened expectations as the home. Instead, courts have held fast to the notion that where the scan is nonintrusive and poses no risk for collateral damage, a mere interest in concealing contraband is not a valid privacy concern.

However, in *Kyllo v. United States*,[51] when again confronted with the home as the center of questionable activity, the Supreme Court adopted the Second Circuit's reasoning in *Thomas*. The question in *Kyllo* concerned the use of a forward-looking infrared device (FLIR)[52] rather than a canine sniff, but the Court still used the oppor-

---

47 Id. at 1366.

48 Id. at 1366-67.

49 See United States v. Karo, 468 U.S. 705 (1984) (discussing police use of covert tracking device within and beyond private dwellings); United States v. Knotts, 460 U.S. 276 (1983) (same). These cases are not dispositive here because the beepers often monitored mundane objects, like paint cans. Thus, these cases did not hold that there was an expectation of privacy in contraband once inside the home, but rather that police may use technology to monitor movements clandestinely that could otherwise have been monitored openly.

50 See, e.g., United States v. Roby, 122 F.3d 1120 (8th Cir. 1997) (concluding that dog sniff of corridor outside of hotel room is not illegal search); United States v. Ludwig, 10 F.3d 1523 (10th Cir. 1993) (allowing canine sniffs of exteriors of cars parked in hotel lot at random); United States v. Colyer, 878 F.2d 469 (D.C. Cir. 1989) (holding that dog sniff of common hallway outside of sleeper compartment on train is constitutional).

51 Kyllo v. United States, 533 U.S. 27 (2001).

52 A Forward-Looking Infrared Device (FLIR) operates in the infrared spectrum to detect heat gradients. They are useful for many purposes besides law enforcement, including detecting faulty insulation in buildings as well as locating in-wall electrical fires. Interview with John Hodge, Law Enforcement Sales Manager, FLIR Systems, in Boston, Mass. (June 3, 2003).

tunity to strengthen the protection of the home and overrule important parts of *Jacobsen* and *Place*.

In this case, Danny Kyllo was found to be growing more than one-hundred marijuana plants in his home using halide lamps.[53] He was caught, in part, because the police used thermal imaging technology to discern abnormal heat activity within his house.[54] The Supreme Court, however, ruled that the use of this technology constituted a search,[55] and that the search was unreasonable.[56] Justice Scalia, writing for a 5-4 majority, held that "obtaining by sense-enhancing technology *any* information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search—at least where (as here) the technology in question is not in general public use."[57] In using these words, the Court discarded any notion that the holding of the case was narrowly tailored to account for a technology believed to be too revealing.[58] In fact, had the judgment not included this language, and not followed closely upon cases limiting the use of drug-sniffing dogs around a home, *Kyllo* could be explained by declaring the FLIR device alone to be overly intrusive into privacy. This, however, was not the holding. To further enforce this point, Justice Scalia explained: "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[59]

These holdings go far beyond deciding that the thermal imaging technology at issue is too revealing, and instead actually adopt the rule of law set forth in *Thomas*. This formulation provides no room for identification of illegal activity when it occurs within the home, even using scanning technology as narrowly tailored as, or even more so than, a canine sniff. Still, it does allow for the use of technology that is "in general public use."[60] This is problematic, however, because it essentially means that a more sophisticated system that

---

53 *Kyllo*, 533 U.S. at 30.

54 Id.

55 Id. at 34-35.

56 Id. at 40.

57 Id. at 34 (emphasis added) (citations omitted).

58 It is certainly possible to read *Kyllo* as allowing for the possibility that if FLIR was only able to reveal illegal activity, the decision would be different and, therefore, the broad reading given in this Note unnecessary. *Thomas* and other cases, however, suggest that a different reading is more appropriate. These cases illustrate a trend beyond *Kyllo* and show why concerns exist as to how *Kyllo* will impact the development of future law enforcement technologies.

59 *Kyllo*, 533 U.S. at 36.

60 Id. at 34.

might be more protective of privacy, designed specifically for law enforcement purposes, will be unconstitutional when used without a warrant, but if the consumer market develops x-ray or night-vision goggles, which are potentially far more invasive of privacy, law enforcement officers will be able to use those without offending the Constitution. Making the constitutional inquiry turn on such a distinction creates the perverse result of greater intrusion on privacy as further discussed in the next Part.[61]

II
THE PROBLEMS WITH CURRENT FOURTH AMENDMENT JURISPRUDENCE

The effect of the decisions described in Part I is an interesting one. The decisions limit the ability of law enforcement officials to conduct scanning activities that would be minimally privacy-intrusive, while allowing law enforcement to engage in unfettered surveillance activity that raises privacy concerns. Part II.A describes why this dichotomy, based upon the home, is too broad; Part II.B describes why it is at the same time too narrow.

A. Current Search and Seizure Doctrine Is Too Broad

Fourth Amendment doctrine as it stands after *Kyllo*, requiring a warrant before using technology to obtain *any* information about the activities inside of a home,[62] is too broad to the extent that it disallows scanning activity. After *Kyllo*, scanning may not be used to identify illegal activity occurring within the home. This bright line, however, is undesirable and unnecessary.

Although the thermal imaging scanner used in collecting information on Danny Kyllo's home may not fit the definition of scanning technology, because it reveals relative levels of heat rather than only indicating illegal activity,[63] the Supreme Court's decision is not limited to just that technology.[64] Instead, the Court forbids the use of all technology that reveals information about the goings-on inside of a home. It does this even though there is no need to put any limits on

---

[61] See infra text accompanying note 87.

[62] *Kyllo*, 533 U.S. at 34.

[63] Indeed, as Scalia points out:

> The [imager] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on.

Id. at 38.

[64] Id. at 36-38.

true scanning technology. True scanning technology, as defined above, can only alert to the presence or absence of a stimulus.[65] If the stimulus for which the device is programmed to alert is an illegal activity (either in the form of possession of contraband or an actual activity), the device will only alert authorities to that activity and no other.[66] It is one of the contentions of this Note, supported by the holdings in *Jacobsen* and *Place*, that there is no reasonable expectation of privacy in such illegal activity.[67]

So, the question becomes whether it is appropriate, given the nature of scanning technology, to draw a bright line at the home. Consistent with current analyses regarding the reasonableness of a search activity, an individual's privacy interest must be weighed against the government's interest in the activity.[68] The interests at stake here can be categorized as general privacy interests and constitutional guarantees.

1. General Privacy Interests

One argument for requiring warrants prior to any search revealing information about activities in the home is simply that people want their homes to remain private. For most citizens, the home is the center of their personal lives and is where they store their belongings. A standard search of the home would reveal personal information and be both disconcerting and potentially embarrassing to the owner. This is indicative of the problems with searches in

---

[65] See supra note 44 and accompanying text.

[66] For a discussion of the possibilities for scanning technology in the future, see infra Part III.C.

[67] See United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that there is no legitimate privacy interest in "privately" possessing cocaine); United States v. Place, 462 U.S. 696, 707 (1983) (identifying content of information—illegal drugs—as justification for constitutionality of search); see also Posner, supra note 9, at 51 ("What is important is that the Fourth Amendment not be seen as protecting the criminal's interest in avoiding punishment. It is a real interest . . . but not a lawful interest."); supra note 44 and accompanying text.

[68] The *Katz* test for reasonableness includes a prong questioning society's willingness to accept an expectation of privacy as reasonable. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This suggests that there are factors that can override an individual's expectation of privacy. See Chimel v. California, 395 U.S. 752, 762-63 (1969) (justifying search incident to lawful arrest as necessary for police safety); Warden v. Hayden, 387 U.S. 294, 298 (1967) (justifying hot pursuit exception to warrant requirement by balancing police interests in exigency); Carroll v. United States, 267 U.S. 132, 153 (1925) (justifying car search exception to warrant requirement by balancing police interests in practicality).

general.[69] Given these societal concerns, it makes sense to protect this private area.

Unfortunately, the home also may be the center of criminal life. Criminals may use their homes to plan crimes, carry out offenses, and store evidence and fruits of crimes.[70] This danger is growing greater with advancements in technology and weaponry. It is no longer the case that the building of weapons of mass destruction requires classified information and rare, highly regulated raw materials such as plutonium; chemical and biological warfare (and the potential for nanotechnology advancements in the next few decades) create the possibility that massive destruction could arise out of activity conducted entirely within the home.[71]

The fact that criminal activity may take place exclusively within the home poses a significant problem for deterrence, one of the most compelling justifications for criminalizing behavior.[72] Criminal law

---

69 Searches and seizures, as currently defined in Fourth Amendment jurisprudence, permit collateral damage and corrupt use of the fruits of a search. The collateral damage associated with a typical search is that law enforcement agents see more than necessary when locating evidence. This can happen for many reasons—the agents might be looking for a gun and, in the process, open drawers to see items as mundane as sweaters or as potentially embarrassing as nude photographs. In either case, the sweaters or the photographs are not the gun, so the agents have seen more than necessary. This damage can multiply quickly as the law enforcement agents are forced to open drawers and dump their contents in search of evidence. See Seidman, supra note 19, at 1087. Beyond opening drawers, law enforcement agents are even justified in slicing open upholstery, see United States v. Ross, 456 U.S. 798, 821 (1982) ("When a legitimate search [of a vehicle] is under way, and when its purpose and its limits have been precisely defined, nice distinctions . . . between glove compartments, upholstered seats, trunks, and wrapped packages . . . must give way to the interest in the prompt and efficient completion of the task at hand."), and possibly even breaking through walls, see United States v. Weinbender, 109 F.3d 1327 (8th Cir. 1997) (allowing police to remove seemingly unfinished section of dry wall). In most cases, the search is broader than desired by the one subject to it, and broader than necessary to obtain the relevant information.

70 Many crimes can be fully conducted within the home. Examples of this include growing and possessing illegal drugs, Kyllo v. United States, 533 U.S. 27 (2001), and possessing images of child pornography, Osborne v. Ohio, 495 U.S. 103 (1990).

71 See Bill Joy, Why the Future Doesn't Need Us, Wired ("[T]hese . . . abuses [of materials of mass destruction] are widely within the reach of individuals or small groups. They will not require large facilities or rare raw materials. Knowledge alone will enable the use of them."), (Apr. 2000) http://www.wired.com/wired/archive/8.04/joy_pr.html; see also John L. Petersen & Dennis M. Egan, Small Security: Nanotechnology and Future Defense, Def. Horizons, Mar. 2002, at 4-5 ("Military applications of molecular manufacturing have even greater potential than nuclear weapons to radically change the balance of power." (quoting David E. Jeremiah, Nanotechnology and Global Security, paper presented at Fourth Foresight Conference on Molecular Nanotechnology (Palo Alto, CA, Nov. 9-11, 1995), available at http://www.ndu.edu/inss/DefHor/DH8/DH08.htm)) (on file with *New York University Law Review*).

72 Despite arguments suggesting that current criminal laws and sentencing do not provide adequate deterrence, see, for example, Paul Dryer, Note, *Bennis v. Michigan*: Guilty Property—Not People—Is Still the Focus of Civil Forfeiture Law, 28 U. Tol. L. Rev. 371

expects that criminals will weigh the likelihood of being caught and the punishment likely to be received if caught against the benefits of committing the illegal act.[73] After *Kyllo*, if activity can occur wholly within a home, and there is no external member of society to report the behavior, the probability of being caught will be exceptionally low, which would arguably increase the number of individuals who are willing to commit an illegal act. The possibility of increased participation in illegal activity, combined with the nature of the potential activity (everything from terrorist plots to drug use and sales, domestic abuse, and possession of unregistered firearms) adds additional weight to the government's interest in deterring criminal activity within the home.

The government interest in using this method of law enforcement is also substantial, and should be weighed against any existing notions of desires for privacy. Scanning technology can give law enforcement agents a tool to help them locate illegal activity.[74] It can do so without the collateral damage associated with standard searches.[75] Because the potential for collateral damage is the real problem with standard searches,[76] the ability to accomplish the same goals without incurring the same costs is preferable.

2. *Constitutional Guarantee*

One might argue that the home is specifically protected by the Constitution, justifying a requirement that law enforcement agents

---

(1997) (arguing for increase in risk of forfeiture rather than sentencing to effectuate deterrence); Christopher Mascharka, Comment, Mandatory Minimum Sentences: Exemplifying the Law of Unintended Consequences, 28 Fla. St. U. L. Rev. 935 (2001) (discussing how sentencing alone will not provide adequate deterrence), deterrence is still an accepted method by which to control criminal activity, see, for example, Tracey L. Meares, Signaling, Legitimacy, and Compliance: A Comment on Posner's *Law and Social Norms* and Criminal Law Policy, 36 U. Rich. L. Rev. 407 (2002) (emphasizing importance of deterrence as justification for criminal law).

[73] This illustrates the standard cost-benefit analysis that law-and-economics scholars argue represents the calculus underlying decisions, which is put forth in *United States v. Carroll Towing Co.*, 159 F.2d 169 (2d Cir. 1947).

[74] It is important to remember that this Note does not argue that FLIR, as used in *Kyllo*, is actually scanning technology. Possible future applications of FLIR and other devices that would constitute scanning technology are discussed infra Part III.C.

[75] In discussing the effects of intrusive searches, it has been said that

> [o]ne thing [collateral damage] might involve is an invasion of informational privacy. If the police search my house for drugs, generally it will not be possible to do so by means of a surgical strike. In the course of looking for the drugs, they are likely to see many other things—personal possessions, private papers, and so on—that will tell them something about me.

See Seidman, supra note 19, at 1087.

[76] Id. (characterizing collateral damage as main problem with searches, even those pursuant to valid warrants).

obtain a warrant prior to using these technologies on a home.[77] Current jurisprudence, however, has shown that searches of the home are constitutional if the police activity can be accepted as reasonable.[78]

Police activity has been accepted as reasonable when police officers obtain warrants. Search warrants and arrest warrants, in some situations, allow law enforcement officials to enter a home and conduct privacy-intrusive searches.[79] Police activity has also been accepted as reasonable without warrants even when the police intrude into the home.[80]

3. *Government Interests Should Win*

Since scanning technology can only alert authorities to illegal activity, there is no legitimate privacy interest inherently invaded by its use.[81] In fact, the technology protects privacy interests because it identifies only illegal activity, and no additional information is conveyed to law enforcement officers. The use of scanning technology may prevent the police from obtaining a warrant for physical invasion of a home under suspicion when scanning results in a negative reading. This is beneficial because it will prevent the collateral damage associated with standard searches and seizures, and save police and innocent suspects' time that otherwise might have been spent on a physical search.[82] Furthermore, there is no justification for believing that society is prepared to recognize a privacy interest in illegal activity.[83] If society is prepared to respect a privacy interest in the home, but not in illegal activity, the goal of preventing illegal activity should trump the mere idea of the sacred home when no other privacy interests are at stake. Thus, the law enforcement use of scanning technology would seem reasonably justified, and the Fourth Amendment doctrine after *Kyllo*, which limits the use of scanning technology, would seem too broad.

---

77 Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

78 See supra note 9 and accompanying text.

79 See, e.g., *Kyllo*, 533 U.S. at 31-32 (discussing warrantless searches and implying that searches pursuant to warrants may be constitutional).

80 See supra note 9 and accompanying text. Also note that these other situations are much more troubling than scanning technology due to the collateral damage problem. See supra notes 19 and 75 and accompanying text.

81 See supra notes 66-67 and accompanying text.

82 See Posner, supra note 9, at 51 ("The old-fashioned (that is to say, pre-electronic) search, or arrest or other seizure, threatens interests [protected by the Fourth Amendment] . . . .").

83 See supra note 44.

B. Current Search and Seizure Doctrine Is Too Narrow

Fourth Amendment doctrine is also too narrow in that it permits law enforcement to engage in activity that largely compromises privacy. It allows constant public surveillance, infringing upon privacy by creating additional arenas for collateral damage. Moreover, it allows more general intrusions into areas that should be protected by failing to adequately define those spheres that deserve protection.

1. Surveillance Begets Collateral Damage

Currently, a law enforcement officer can witness activity and make observations either by monitoring activity occurring in public or by conducting a standard search of a private location. In either case, the agent does not need to clear any hurdles to be permitted to take pictures or video images, or write down observations and impressions, even if they appear to be unrelated to any criminal activity.[84]

Current jurisprudence allows this recording on the theory that the agent is in an appropriate location and therefore is not conducting a search by making additional observations.[85] The current doctrine even allows the use of technology that is in general public usage to monitor activities that occur within private spheres.[86] Presumably,

---

[84] See, e.g., United States v. Santana-Garcia, 264 F.3d 1188, 1194 n.8 (10th Cir. 2001) (referencing Utah Code § 77-7-2 allowing officers to make warrantless arrests for any "public offense" committed in officer's presence, where "'presence'" includes all of the physical senses or any device that enhances the acuity, sensitivity, or range of any physical sense, or records the observations of any of the physical senses"). This is not to say that the captured observations will be necessarily admissible in court; they are nevertheless not prohibited in practice.

[85] One could argue that this activity is not a search, but a seizure: The recording can be used at a later time by the recorder to the detriment of the recorded, and for use there must first be possession. Thus, the possession ensues by seizing information from the subject of the recording. See Larry Downes, Electronic Communications and the Plain View Exception: More "Bad Physics," 7 Harv. J.L. & Tech. 239, 257, 263-64 (1994). Even if this activity is recharacterized as a seizure, an argument could be made that the plain view doctrine would allow the activity to continue. In either case, the exact characterization of this activity is not important for the current argument.

[86] In *Kyllo*, the Court held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—*at least where (as here) the technology is not in general public use*." Kyllo v. United States, 533 U.S. 27, 34 (2001) (emphasis added) (citations omitted). The Court in *Kyllo* simply assumes that thermal imaging technology is not in the public use but gives no indication of how it reached this conclusion. In fact, thermal imagers can be purchased by the general public from many supply stores, including the manufacturer of the device used in the *Kyllo* case. Interview with John Hodge, supra note 52 ("An equivalent performance unit, in terms of sensitivity and readouts, is now and was available for sale in 1992 to nongovernment consumers."). They are expensive, but so are the helicopters and airplanes like those used in *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (allowing use of air space to photograph open parts of production plant).

this allows law enforcement agents to use binoculars and flashlights to look through windows.[87] It also creates the perverse result that a highly-tailored law enforcement device with no real consumer purposes, that might be extremely protective of privacy, would be illegal due to its infrequent usage.

The search and seizure doctrine that allows this type of surveillance, searching, and recording is problematic because it is too narrow to protect individuals' privacy. Much of the information seen or recorded is not relevant to law enforcement purposes. The use of surveillance information can be equally as damaging as physical seizure, if not more so.[88] Surveillance technology exacerbates this problem because its use allows the police readily to record information, activities, and public communications, rather than merely seizing personal property.[89] Therefore, the current state of the law allows law enforcement agents to gain access to information that they do not need. This is another form of collateral damage.[90]

---

[87] General public use, however, is not defined anywhere within the opinion, or elsewhere for that matter. See Courtney Dashiell, Comment, Thermal Imaging: Creating a "Virtual" Space, 34 U. Tol. L. Rev. 351, 367 (2003) (discussing failure to define terminology); Gregory Gomez, Comment, Thermal Imaging and the Fourth Amendment: The Role of the *Katz* Test in the Aftermath of *Kyllo v. United States*, 46 N.Y.L. Sch. L. Rev. 319, 321 (2003) (same). In addition to the lack of definition, the fact that what *is* in the general public use will constantly change makes the standard unpredictable and more confusing. For a more complete discussion of why the reliance on general public use poses more questions than answers, see Sarilyn E. Hardee, Note, Why the United States Supreme Court's Ruling in *Kyllo v. United States* Is Not the Final Word on the Constitutionality of Thermal Imaging, 24 Campbell L. Rev. 53 (2001). Thus, law enforcement agents have no good standard with which to judge when they are able to conduct warrantless binary scans because they have to constantly evaluate whether the technology is in general public use.

[88] The American Bar Association (ABA) has worried about regulating technology with surveillance uses that currently would not be defined as a "search" by the courts. Am. Bar Ass'n, ABA Standards for Criminal Justice Electronic Surveillance, Section B: Technologically-Assisted Physical Surveillance 23-24 (3d ed. 1999). However, courts could resolve these concerns by declaring the activity a seizure. See supra note 85.

[89] Downes, supra note 85, at 242, 263-65 (outlining difference between physical surveillance and electronic surveillance in suggesting that "Plain View exception has minimal application in the context of electronic communications").

[90] In fact, these possibilities are even scarier when government officials could use the information in a corrupt manner. "Corrupt" means any use that is not legal or foreseeably pertinent to current, legitimate law enforcement aims. Therefore, the use of the fruits of a search or seizure to effectuate any arrest stemming directly from the search or seizure is not corrupt—instead, it is reasonably foreseeable because the purpose of a search or seizure is to uncover incriminating evidence. Further, if the purpose of a search or seizure is to gain specific evidence of a crime, the use of the information garnered to make a case for a warrant or conviction would be foreseeable as well; the use of information obtained to blackmail or harass, however, would be considered a corrupt use. It would also be a corrupt use if seemingly mundane information were stored for a time when that information might be used to blackmail or harass; if there is no way to connect information

From the law enforcement perspective, however, surveillance is a useful method for obtaining the evidence necessary to support a warrant and a subsequent intrusive search. Without public surveillance, it would be very difficult for police to engage in the detection and apprehension of more typical criminals.[91] It would also create a situation where the police could not be aware of activity readily observable to the public.

2. *Areas Protected from Physical Intrusion Are Too Narrow*

Fourth Amendment doctrine is also too narrow because it does not protect the spheres that the courts have otherwise said deserve protection from physical intrusion. In fact, people have relatively high expectations of privacy in areas where the Court has deemed the expectation of privacy to be lower,[92] and the areas in which such a right has been recognized are not protected equally.[93] The doctrine is inconsistent even when focusing on the narrow area of the home, which the *Kyllo* Court maintains should be protected to a greater extent than other areas.

---

obtained to evidence of a crime, it would be "corrupt" to store it for a possible future time when a connection might be made or fabricated. Please note that the information discussed here is not standard information that would normally be used in the private sector (such as name, social security number, date of birth, bank account information, etc.) but rather information gained from surveillance (daily routines, associates, apartment layout, etc.).

91 While this has not been expressly articulated, it would appear that the Court has accepted public surveillance as a principal method of attaining sufficient evidence to secure warrants for searches, wiretaps, and arrests. See, e.g., Spinelli v. United States, 393 U.S. 410 (1969) (discussing probable cause to obtain warrant and describing surveillance and observation as method to obtain probable cause).

92 The car is a perfect example of this legal fallacy. While studies have shown that citizens believe that various car searches are relatively more intrusive than other searches, see Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society," 42 Duke L.J. 727, 737-38 tbl.1 (1993), the Supreme Court has nonetheless held that the warrantless search of an automobile is constitutionally permissible, Carroll v. United States, 267 U.S. 132, 153 (1925). Though the Court has recognized an expectation of privacy in the car, they have not used this expectation to prevent intrusion, thus subverting the method proposed by the Court in establishing permissible searches. See generally David A. Moran, The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time, 47 Vill. L. Rev. 815 (2002) (discussing expectations of privacy and car search exception doctrine).

93 The home is protected because most personal activity still occurs there, and it is where people "expect" to have a private life. See generally Slobogin & Schumacher, supra note 92, at 737-40 (demonstrating that citizens find search of areas of home relatively more intrusive than other areas); see also Kyllo v. United States, 533 U.S. 27, 37 (2001) (relying on subjective belief in expectation of privacy due to nature of activity occurring in home to draw protections around home).

The decision in *Kyllo* attempts to create a simple, bright-line rule regarding the expectation of privacy within the home.[94] Essentially, *Kyllo* stands for the proposition that the home is a place so deserving of privacy that even a nonsearch investigative activity that would be allowed without a warrant in any other sphere requires a warrant when conducted in a home. This seemingly simple rule is actually much more complicated. In many cases, the Court has created exceptions to the protection of the home. The Court has found that no warrant is needed to search the home in cases of emergency or hot pursuit. Also, no warrant beyond the arrest warrant is needed to search the vicinity of a subject to a lawful arrest.[95]

While these exceptions are justifiable on policy grounds, there are arguably stronger policy arguments for allowing pure scanning technology to focus on the home.[96] Still, perhaps the most troubling complication with drawing a bright line around the home is that the Court has not treated all types of housing equally. Instead, the Court has held that occupants of mobile homes have the same expectations of privacy as occupants of more standard housing, yet do not deserve the same protections nor are they afforded the heightened level of protection provided to stationary homes.[97]

3. *Which Interest Wins?*

In the above instances, the current search and seizure doctrine appears too narrow because it is internally inconsistent, and it fails to protect people from the collateral damage associated with surveillance and with atypical housing. However, it is not clear that this means that government interests should lose. Some degree of public surveillance seems necessary for societal demands on law enforcement, and some degree of recognition that certain private spheres are more easily manipulated than others is also necessary. Part III sets forth a dichotomy for understanding Fourth Amendment jurisprudence that will attempt to strike balances in this arena while simultaneously taking into account the conclusions regarding scanning technology from Part II.A.

---

[94] See *Kyllo*, 533 U.S. at 40 ("We have said that the Fourth Amendment draws 'a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright . . . ." (citation omitted)).

[95] See supra note 9 and accompanying text.

[96] See infra Part III.

[97] California v. Carney, 471 U.S. 386, 392-94 (1985) (permitting warrantless search of mobile home). The Court justified this decision using the car search exceptions because of the unique problems mobility provides to law enforcement's desire to monitor an area. It is unclear whether this is an indication that *Kyllo* has overruled these cases as well.

III
A More Coherent Fourth Amendment Dichotomy

The key to understanding when a search is unreasonable is to look at the actions of law enforcement on a macroscale. From the historical days of King George III of England to the satirical days of Boss Hogg of Hazzard County, the idea of an intrusive and corrupt police force has concerned Americans. The Founders added the Fourth Amendment to the Constitution to ensure that government could not become too powerful.[98] By limiting government agents' abilities to intrude on the lives of individuals, they sought to protect other basic freedoms, such as freedom of speech, association, and equality.[99] This notion that the Fourth Amendment is necessary to curtail police actions, which in turn will protect privacy, however, has been lost. Instead of examining the actions of police, the Fourth Amendment jurisprudence asks overwhelmingly about the expectations of the citizenry. Although the law attempts to use one as a proxy for the other, these inquiries are not the same nor are they separable. Rather than asking what activities and areas a citizen expects to keep private, Fourth Amendment jurisprudence should ask what police actions the citizenry reasonably expects to be able to avoid.

As Part II of this Note explained, Fourth Amendment doctrine is both too broad and too narrow. It is too broad because it unnecessarily limits the use of technology that is minimally privacy-intrusive and too narrow because it allows law enforcement agents to conduct questionable surveillance activities. Where the Court has said that using technology to see into a house is not allowed,[100] the rule is overinclusive. Such police activity should be allowed only if it is narrowly tailored to discover illegal activity. Activity could be defined as "narrowly tailored" if it revealed only illegal actions (e.g., scanning technology).[101]

---

98 Sean D. Thueson, Case Note, Fourth Amendment Search—Fuzzy Shades of Gray: The New "Bright-Line" Rule in Determining When the Use of Technology Constitutes a Search, Kyllo v. United States, 121 S. Ct. 2038 (2001), 2 Wyo. L. Rev. 169, 173-76 (2002) (providing brief history of search and seizure).

99 It was, and still is, believed that privacy and the right to be free of intrusion are essential to combat the chilling effect that could exist if activities and associations were subject to discovery at the whim of law enforcement. See, e.g., Warren & Brandeis, supra note 4; Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 99 (1994) (discussing motive behind U.S. Privacy Protection Act as seeking "to lessen the chilling effect of intrusive searches on those engaged in First Amendment activities").

100 Kyllo v. United States, 533 U.S. 27 (2001).

101 Another definition of "narrowly tailored" that is more sweeping might include allowing searches if the information revealed was vague as to the conclusions that could be drawn from the readings. A vague reading is one that cannot be determined readily. For

Conversely, surveillance technology involves precisely all of the harms that scanning technology can avoid. It is the nightmare that George Orwell described in his dystopic novel, *1984*, in which Big Brother monitors each citizen's every thought and action.[102] For that reason, surveillance activity should be regulated to protect members of society from excessive use of these law enforcement techniques. This Note does not claim to identify in which area such safeguards should lie, but instead proposes a new thought process that should underlie the decisionmaking structure.

Part III.A explains why this new dichotomy more honestly describes the past holdings of the Court. Part III.B explains collateral benefits derived from the new dichotomy that are desirable from a policy standpoint. Part III.C then describes ways to think about new technologies, with this new dichotomy in mind, that could enable superior protections against crime and minimize intrusions on privacy.

A. An Honest Interpretation of Past Decisions

A doctrine based on reasonable expectations of privacy that nonetheless permits intrusions under numerous circumstances is not consistent with the general principle of expectation of privacy; how can people expect privacy if they can also expect the grant of privacy to be riddled with exceptions? The simple notion of a warrant is proof that reasonableness cannot be based solely on expectations of privacy. The *Katz* doctrine also suggests the inadequacies of the reasonable expectation of privacy standard by identifying a second prong that requires that society, through objective evidence, accept the expectation of privacy.[103]

Once objectivity is introduced, the issue is no longer whether privacy was, in point of fact, expected. Indeed, studies have shown that

---

example, a heat-sensing device that indicated a ninety-degree area in a house is vague because this temperature could be reached due to many different activities. This type of search is "narrowly tailored" in that it does not reveal sufficient information to form conclusions and is designed only to reveal one type of information. It is conceivable, however, that two or more of these activities could be combined to draw inferences that would be less "narrowly tailored." For examples of these combinations, see Part III.C, infra. Still, sometimes a combination of technologies will create a "narrowly tailored" legitimate search. For example, while a thermal imaging device might relay too much information on its own, the imager combined with a scan of phone calls and a chemical analysis of external air that does not give individual readouts but instead combines the results, runs them through a heuristic, and declares that illegal activity is occurring would be legitimate. There are various justifications for either of these definitions of "narrowly tailored"; it is sufficient, for the sake of this Note, however, to focus on searches that can reveal only illegal activity.

[102] George Orwell, 1984 (Plume 2003) (1949).

[103] See supra note 17 and accompanying text.

individuals manifest expectations of privacy in areas that are routinely invaded.[104] Cars and mobile homes are two of the more striking examples of uses in which the public's expectations of privacy and the courts' understandings have differed.[105] It is also quite likely that, rather than merely identifying expectations already within society, courts actually dictate expectations.[106] What this doctrine really addresses is the acceptability of police actions. If one is to hope for an adequate treatment of police actions, doing so expressly would better accomplish the goal and create a more straightforward jurisprudence.

An analysis of *United States v. Thomas*[107] might suffice to explain the way an application of the proposed dichotomy would differ from an application under the currently existing dichotomy. In *Thomas*, later followed by *Kyllo*,[108] the Second Circuit distinguished *Place*[109] on the grounds that the drug-sniffing dog was in a residence rather than an airport, and thus the reasonable expectation of privacy was invaded.[110] However, perhaps the real problem in *Thomas* was not the presence of the drug-sniffing canine, but rather the police officers who necessarily accompanied the animal. Intuitively, it seems disconcerting to have police officers roaming the hallways of apartment buildings. Also, collateral damage can result from this action: The officers can hear noises from within apartments, witness activities in the hallways, and look into rooms when doors happen to be open. So, under the proposed dichotomy, rather than distinguishing *Thomas* on the basis of the location of the activity, the court could have distinguished *Thomas* because there is collateral damage associated with the activity. This holding would more directly address the question of police activity and would not corrupt the view that dog-sniffs in particular, and scans generally, are permissible.[111]

---

104 See supra note 92 and accompanying text.

105 See supra notes 92-93, 97 and accompanying text.

106 See, e.g., Madeline A. Herdrich, Note, *California v. Greenwood*: The Trashing of Privacy, 38 Am. U. L. Rev. 993, 1008 (1989) (pointing out that lower courts held that individuals probably do have expectations of privacy with respect to their garbage). Since the Supreme Court has now determined that no expectation of privacy in garbage is reasonable, individuals must no longer maintain those expectations. Cf. Todd M. Wesche, Reading Your Every Keystroke: Protecting Employee E-mail Privacy, 1 J. High Tech. L. 101, 117 (2002) (identifying courts and Congress as capable of creating expectations of privacy).

107 757 F.2d 1359 (2d Cir. 1985); see supra text accompanying notes 46-50 for a detailed discussion of *Thomas*.

108 533 U.S. 27 (2001).

109 462 U.S. 696 (1983).

110 *Thomas*, 757 F.2d at 1366-67.

111 See supra Part I.B.

B. *Policy Support for the New Bright-Line Rule*

As shown above, there is no defensible policy basis for drawing a bright-line rule at the home with respect to scanning technology. A search that can only indicate whether an illegal act is taking place without revealing other information minimizes collateral damage. It is unnecessary, therefore, to protect the home from such a search. In addition, there are collateral benefits to such a rule that deserve attention.

For example, increased searches and seizures using scanning technology might reduce bias or the appearance of bias in law enforcement. Currently, enforcement of the criminal law is often biased, or at least appears that way in many instances.[112] That bias manifests itself in practices such as racial profiling and increased police presence in poor neighborhoods.[113] This perceived bias further enhances feelings of prejudice on both sides of the table.[114] Recognizing that there is no right to privacy in illegal activity, no matter where it occurs, would allow law enforcement to utilize technology that pinpoints criminal activity without relying on practices like profiling. Law enforcement would not have to generate statistical proofs and checklists for when probable cause might exist. They would not have to depend on individual characteristics that are truly unrelated to criminal activity to locate criminal activities that could be detected by scanning. On the other side of the equation, increased regulation of surveillance would promote diversified use of the scanning technologies and ensure that there are justifications for targeting individuals and areas to greater extents.[115]

---

[112] Anthony C. Thompson, Stopping the Usual Suspects: Race and the Fourth Amendment, 74 N.Y.U. L. Rev. 956, 957 (1999) ("Recent studies support what advocates and scholars have been saying for years: The police target people of color, particularly African Americans, for stops and frisks.").

[113] See id.; Erika L. Johnson, "A Menace to Society": The Use of Criminal Profiles and Its Effects on Black Males, 38 How. L.J. 629, 642-43 (1995).

[114] The targets of racial profiling may feel that they are victims of prejudice, but also may begin to harbor prejudices against outsiders to the bias. Outsiders to the bias, on the other hand, also see the bias occurring and believe that it is justified, thereby reinforcing prejudice. See Johnson, supra note 113, at 634 ("In sum, racial prejudice continues to be a significant factor in society's determinations of criminal suspicion. Because formulation of criminal suspicion occurs in the initial stage of the criminal justice process, racial prejudice only exacerbates the problem of disproportionate detention and arrest patterns among black males.").

[115] Logic would indicate that if one law enforcement mechanism is limited by the Court, while another is given the presumption of constitutionality, the second mechanism will be used more frequently. This is especially true if the mechanism is cheaper, easier, provides more accurate information, or keeps law enforcement agents safer than the previous mechanism. Scanning technologies have the potential to realize all of these benefits.

The proposed dichotomy could also result in a criminal code that criminalizes only those behaviors that society believes should be criminalized. Some critics of the proposal to allow all binary searches for illegal activity might be concerned that the use of such technologies will result in increased detection and prosecution of crimes that, while defined as such by the law, are widely criticized. Prime examples of concern among the public right now are drug laws,[116] and, until the recent Supreme Court decision in *Lawrence v. Texas*,[117] consensual sodomy laws.[118] Those who see the ability of the police to monitor this illegal behavior as overly intrusive have not pointed to a critical flaw in the analysis of this Note, but instead to one in the law itself. It is not the purpose of this Note to argue the substantive law at stake in the issues laid out above; however, it is important to realize that if a majority of society considers police monitoring of certain crimes intrusive, perhaps it is time to respect society's views and repeal or overturn the laws where they exist, as occurred in *Lawrence*.[119]

It is possible for the proposed method of analyzing Fourth Amendment violations to help account for society's views by bringing violations to the forefront of debate. It is also possible for this proposed method to allow for greater ease of enforcement by police for certain dangerous yet hidden crimes and to protect against searches that are overly intrusive. All of these potential benefits are in addi-

---

116 Drug laws are widely seen as paternalistic. It is true that the government has many laws regulating health and safety, and it is equally true that drugs represent a severe threat to both. Some, however, would argue that much drug use is victimless and even less harmful than alcohol abuse, which is merely regulated rather than outlawed. See Richard S. Frase, Comparative Criminal Justice as a Guide to American Law Reform: How Do the French Do It, How Can We Find Out, and Why Should We Care?, 78 Cal. L. Rev. 539, 567-68 & n.127 (1990) (identifying proponents of this type of decriminalization). This Note takes no position on the debate raging in America today, but merely points out that utilizing the proposals above should lead to increased debate in this area so that the laws will conform to the will of our democracy.

117 123 S. Ct. 2472 (2003).

118 Sodomy laws were viewed as, and largely enacted for, prosecution and persecution of homosexuals. See Bowers v. Hardwick, 478 U.S. 186, 192 (1986) (refusing to extend right of privacy to homosexual sodomy); see also Lambda Legal, Issues, Criminal Law, at http://www.lambdalegal.org/cgi-bin/iowa/issues/record?record=11 (last visited Sept. 24, 2003) (listing links to cases concerning laws that criminalize same-sex relations). These laws were also nearly impossible to enforce because of the intrusive nature of the monitoring that would be necessary to detect infractions. See *Bowers*, 478 U.S. at 195-96 (identifying difficulty of enforcement, yet failing to negate law). While it is true that the proposal above might enable the monitoring of such activity and allow for easier enforcement, it would instead hopefully lead to greater understanding of the harm this type of law can cause to members of society and lead to the repeal of such laws. After *Lawrence*, of course, the criminalization of sodomy is no longer constitutional. *Lawrence*, 123 S. Ct. at 2484.

119 *Lawrence*, 123 S. Ct. at 2484.

tion to the benefit of having a Fourth Amendment doctrine that articulates the exact concerns of the amendment rather than creating a doctrine with many exceptions. None of these benefits are possible, however, without new technologies that account for the needs of law enforcement from the design stage.

C. *New Technologies for a New Dichotomy*

The Court has demonstrated confusion regarding possibilities for new technology. In *Kyllo*, Scalia explained that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[120] This language demonstrates a fundamental misunderstanding by the Court about how advancements in technology are as likely to help protect privacy as invade it. A clear understanding of the law enforcement interests at stake in the proposed dichotomy could lead to technological developments that would enable scanning and protect privacy during surveillance.

Taking the current example from *Kyllo*: It is true that one way that technology might advance is by finely tuning thermal imaging, which currently gives only crude temperature readings, to produce images of physical objects from heat gradations of miniscule proportions.[121] However, if law enforcement agents understand that technology will be most useful to them if it protects privacy because that will make its use legal, they will create a demand for binary searching devices.[122] Responding to the increase in demand, technology development companies might consider an alternate advancement in thermal imaging technology that accounts for law enforcement needs. This new thermal imager could remove the pictures from the read-

[120] Kyllo v. United States, 533 U.S. 27, 36 (2001). This statement is problematic on numerous fronts. One problem is that the Court appears to be engaging in policymaking. A number of commentators question whether the Court should ever act in a forward-looking, legislative-like manner. See, e.g., Conference, Harvard Electricity Policy Group: Regulatory Decisionmaking Reform, 8 Admin. L.J. Am. U. 789, 823 (1995) (statement of Richard D. Cudahy) ("First of all, courts are not supposed to make policy, and they repeatedly deny that they make policy.") (citing Steven D. Smith, Courts, Creativity, and the Duty to Decide a Case, 1985 U. Ill. L. Rev. 573 (1985)). These commentators might suggest that Scalia wants to act as a legislative rulemaker rather than stick to the facts of the case. Because of the dubious precedential value of such "rulemaking," any future citation to this language is likely to characterize it as dicta. However, these considerations are largely beyond the scope of this Note.

[121] It appears this is the Court's concern in *Kyllo*. 533 U.S. at 36.

[122] If binary searching is recognized as presumptively legal, law enforcement agencies will tend to utilize it more often. See supra Part III.B. Therefore, given the laws of supply and demand, if more binary searching is occurring, there should be more demand for the technology that makes the activity possible.

outs altogether, analyze the exact wavelength of the heat emanating from the house and indicate only when halide lamps are being used to grow plants with certain characteristics of marijuana plants. This may seem like a farfetched example, but it should be remembered that the future capabilities of technology are wholly unknown in the present.[123]

To see more familiar examples, one need only turn to various forms of surveillance technology currently in place or in development. One of the more controversial technologies today is millimeter imaging. This imaging technology utilizes passive millimeter wave imagers to produce an image like an x-ray machine.[124] Privacy advocates might be concerned with millimeter imaging either because the devices are capable of producing an image of a person's physical features underneath clothing or because this level of detail can reveal information about anything the subject has in his or her possession.[125] Whether this technology can be used in its current state consistently with the Fourth Amendment is irrelevant for the purposes of this Note; it is enough to know that the technology reveals more information than necessary for law enforcement purposes. Again, it is possible to adapt this technology using other technological advancements to protect privacy while maintaining functionality.[126] In the future, one possibility may be to combine computer analysis and identification technologies with devices like millimeter imagers. In such a con-

---

[123] Past predictions of what technology will be capable of have been proven wrong time and again. A well-known and humorous example of this includes Lord Kelvin, President of the Royal Society, who, in 1899 was quoted as saying, "Heavier-than-air flying machines are impossible." Greg Bartlett, Eyeing the Sky While Looking Deep Inside: Futurists See Bold Progress and Quest for Basics in New Millennium, USA Today, Nov. 23, 1999, at 5D (quoting Lord Kelvin of the British Royal Society, one of the 19th century's top experts on thermodynamics).

[124] Jason Lazarus, Note, Vision Impossible? Imaging Devices—The New Police Technology and the Fourth Amendment, 48 Fla. L. Rev. 299, 300-02 (1996).

[125] See Alyson L. Rosenberg, Comment, Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?, 9 Alb. L.J. Sci. & Tech. 135, 138-40 (1998) (detailing capabilities of one variation of device).

[126] At least one company is already attuned to this concern:

> Millitech Corporation is sensitive to the privacy concerns generated by its camera. It therefore has planned to ultimately design its millimeter wavelength scanners with a device that will only display an image of a body to a human operator if "a suspicious object is detected by the internal image processing algorithms, giving 'probable cause' for the operator to ascertain the potential threat from the detected object."

George Dery III, Remote Frisking Down to the Skin: Government Searching Technology Powerful Enough to Locate Holes in Fourth Amendment Fundamentals, 30 Creighton L. Rev. 353, 389 (1997) (citation omitted).

figuration, the device would indicate a subject's possession of items such as guns or drugs rather than display revealing pictures.[127]

One concern with the ability to identify objects such as guns is that, when registered, these objects are often legal. A device that alerts to the presence of a gun, therefore, might be overly intrusive and its use by the police might violate the Fourth Amendment.[128] A possible solution might be to use a complex biometric recognition device attached to a database that could identify the subject from among those people with permits to carry guns; if the subject did not appear in the database, only then would an alert indicate the presence of the gun.[129]

Combinations of similar technologies could be used for many surveillance goals. For example, the identification of illegal communication could be achieved in a manner consistent with privacy protection by combining monitoring devices, including those used for computer monitoring,[130] with logical syntax processors.[131]

---

[127] See id.; Rosenberg, supra note 125, at 138-40 (explaining that different objects have unique millimeter wave signatures).

[128] See Steven Salvador Flores, Note, Gun Detector Technology and the Special Needs Exception, 25 Rutgers Computer & Tech. L.J. 135, 143-44 n.65 (1999) (using Florida as example of state protecting carrying of concealed firearms and suggesting additional Fourth Amendment problems with detector technology as result).

[129] Biometrics can be defined as "the use of a person's physical characteristics or personal traits for human recognition." John D. Woodward, Jr., (RAND) Super Bowl Surveillance—Facing Up to Biometrics 3 (2001). Facial recognition and gait recognition are two examples of biometrics that could be used to aid in the proposed circumstances. Facial recognition is defined as "an automated method to record the spatial geometry of distinguishing features of the face." John D. Woodward, Jr. et al., (RAND) Army Biometric Applications: Identifying and Addressing Sociocultural Concerns 16 (2001). Gait recognition is similar, but focuses on an individual's stride. By maintaining a database of those registered to carry concealed weapons, scanning devices described above could identify an individual carrying a gun, take measurements necessary to identify the user, compare the measurements to a database, and, upon a failure to match the individual, alert the authorities. There are technological concerns with the viability of this suggestion; currently, "[n]oncooperative behavior by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies." Id. But increased computing power and advancements in the field of three-dimensional object recognition could make these possibilities a reality. For suggestions and analysis of other technologies that could allow for locating guns while minimizing the intrusive effects, see Sam Kamin, Law and Technology, The Case for a Smart Gun Detector, 59 L. & Contemp. Probs. 221 (1996).

[130] Various methods of monitoring computers have been used by the police and other government officials. See, e.g., United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (use of Key Logger System to decipher password upheld).

[131] The Carnivore, or DCS 1000 system, used by the FBI to track electronic communications, is an example of a technology that could work in this manner. While it is not wholly clear how the DCS 1000 currently works, it is known that it is capable of "monitor[ing] and record[ing] the full content of messages that a targeted user has sent in real-time." Maricela Segura, Note, Is Carnivore Devouring Your Privacy?, 75 S. Cal. L. Rev. 231, 234

Advancements in scanning technology and regulations on consumer products could also solve the problems such as those in *Arizona v. Hicks*,[132] a frequently cited case in which the police unlawfully turned over a record turntable to discover whether the serial number matched that of stolen merchandise. In that case, the unlawful activity was a physical act, not a passive technological scan.[133] The physical act of lifting the turntable and checking its serial number gives the police information that they did not have a right to know, specifically, the serial number of the turntable that had as much chance of being lawfully purchased as stolen, as well as the possibility of revealing other information (e.g. documents or pictures stored underneath).[134] If each item sold had a unique identifier of sorts, a database of stolen merchandise could be created, and police could then scan a room for items emitting unique identifiers matching the stolen goods list. Alternatively, all goods could emit a signal that would be turned off upon purchase; thus, any device emitting such a signal could immediately be identified as stolen.[135] In either case, use of this technology in *Hicks* would have avoided the Fourth Amendment violation because the scan would not have the capability to reveal information other than presence or absence of contraband.[136] Again, this is a way in which an understanding of the demands of Fourth Amendment law can be combined with innovation to produce law enforcement technology that is both useful and constitutional.

(2001). It is also capable of "acquir[ing] the address information for the origin and the destination of all communications to and from a particular ISP customer. This function provides the TO and FROM addresses on an e-mail and is viewed as the electronic equivalent of a telephone pen-register or trap and trace search." Id. A pen-register is defined as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (analyzing constitutionality of warrantless use of pen-register recordings) (quotations omitted). If this system has these capabilities, connection to a processor that could identify not just keywords, but context and tone, could limit the information received by government monitors to only troublesome communications.

132 480 U.S. 321 (1987).

133 Id.

134 Id. Ex ante, there was no way to know the merchandise was stolen. Id. at 326-29.

135 It is important to note that neither of these alternatives is foolproof, since a thief could develop technology to remove the signal. Still, every increase in the cost of thieving will force some thieves to exit the business, thus preventing some crime, and every safeguard taken by the police may lead to greater arrests and recovery of merchandise. See supra note 73 and accompanying text.

136 This is analogous to the cocaine field test in *United States v. Jacobsen*, 466 U.S. 109, 123-24 (1984).

CONCLUSION

While this Note does not provide a bright-line rule that demarcates the line between constitutional and unconstitutional searches, it proposes a framework through which these searches may be more easily identified. The Fourth Amendment is instrumental in protecting individuals from unreasonable intrusions by the government. Therefore, Fourth Amendment doctrine should be concerned mostly with the actions of government agents. In *Kyllo v. United States*, the Court got the doctrine wrong. Instead of addressing the reasonableness of the police activity itself, they focused on the protections that they believed were due the location where the activity took place. This decision is broader than necessary to resolve the case, calling into question the usefulness of law enforcement technology. The Court suggests that technology used to identify activity within the home will always be an unreasonable intrusion into privacy. This Note suggests that instead, the Court should have recognized that some technologies might be more protective of privacy than standard, physical searches, and should be accepted and applauded rather than restricted. To do so, the Court's Fourth Amendment discussions of searches should focus on reasonable police actions, similar to Fourth Amendment jurisprudence prior to the decision in *Katz v. United States*. This proposed framework will allow for a jurisprudence more in line with that focus and will do so in a way that will promote cooperation between law enforcement and inventors. New technology is inevitable, but the uses to which the technology are put are within society's control; clearer understandings between lawmakers and innovators can provide greater advancements in both law enforcement and constitutional protections.