University of Dayton Law Review

Volume 27 | Number 2 Article 2

3-1-2002

# The Supreme Court Announces a Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails to Define It

Douglas Adkins
*University of Dayton*

# THE SUPREME COURT ANNOUNCES A FOURTH AMENDMENT "GENERAL PUBLIC USE" STANDARD FOR EMERGING TECHNOLOGIES BUT FAILS TO DEFINE IT: *KYLLO V. UNITED STATES*

*Douglas Adkins*

## I. INTRODUCTION

New and rapidly advancing technologies continue to challenge the courts in the area of Fourth Amendment warrantless search and seizure. Courts have addressed these intrusive technologies on a case by case basis, struggling to draw the line between the legitimate use of technology by law enforcement and the privacy guaranteed by the Fourth Amendment against unreasonable searches of one's home.[1] The United States Supreme Court recently had another opportunity to strike an appropriate balance between technology and personal privacy interests.

In *Kyllo v. United States*, the Court held that the use of a thermal imaging device from a public street that detected heat emanating from the inside of a private residence was a search within the meaning of the Fourth Amendment and thus required a warrant in order to be constitutional.[2] The Court based this conclusion, in part, on the finding that such a device was not in "general public use."[3] In adopting such a standard without giving any guidance or explanation on how to implement it, the Court has left judges, lawyers, and citizens with no way to distinguish technology that unconstitutionally invades the intimate details of the home from technology in general public use that requires citizens to take proactive steps to guard against it.

This Note will argue that the Court failed to articulate a standard which can be used to predict when technology has crossed the line from a new technology, unavailable in law enforcement searches without a warrant, to an existing technology in general public use that courts may not now consider a search at all under the Fourth Amendment. Section II will outline the background of the case and will catalog the general state of technology today in relation to Fourth Amendment warrantless searches.[4]

---

[1] *See generally Fla. v. Riley*, 488 U.S. 445 (1989) (approving warrantless use of helicopters flying overhead); *Dow Chem. Co. v. U.S.*, 476 U.S. 227 (1986) (allowing warrantless searches with airplanes using mapping cameras); *Smith v. Md.*, 442 U.S. 735 (1979) (using a pen register to track telephone numbers dialed); *Silverman v. U.S.*, 365 U.S. 505 (1961) (regulating the use of eavesdropping devices).

[2] *Kyllo v. U. S.*, 533 U.S. 27 (2001).

[3] *Id.* at 34.

[4] *See infra* nn. 6-64 and accompanying text.

Section III will outline the factors the Supreme Court could have reviewed in defining the general public use standard.[5] Specifically, this Note will argue that general public use must be defined as wide spread use in and around the public sector and not as actual use by the general public, in order to remain consistent with previous Fourth Amendment technology cases. When viewed under a public sector definition, however, the thermal imaging camera in *Kyllo* and other highly intrusive emerging technologies present other significant privacy issues under a *Kyllo* general public use standard. As a result of this lack of clarity, the general public use standard cannot rationally be used to balance future interactions between law enforcement use of technology and citizens' privacy interests of the home.

## II. BACKGROUND

### *A.* Kyllo v. United States

As technology advances and what was once unique becomes commonplace, courts have had to adapt standards of privacy to the changing pace in technology, manufacturing and distribution. Below are the facts in *Kyllo*, the opinions of the Supreme Court and a current catalog of existing technologies and their relationship to unreasonable warrantless searches under the Fourth Amendment.

#### 1. Facts of *Kyllo v. United States*

In 1991, an agent for the United States Department of the Interior suspected that Danny Kyllo was growing marijuana in his home in Florence, Oregon.[6] Indoor marijuana growing operations often utilize high intensity halide lamps, which generate a substantial amount of heat.[7] The agent used a thermal imaging camera to scan both Kyllo's home and the two homes that were attached as part of the triplex in which Kyllo lived.[8] An agent made the scan, taking only a few minutes, from an automobile across the street and the scan showed that one exterior wall and the roof of

---

[5] *See infra* nn. 65- 122 and accompanying text.

[6] *Kyllo*, 533 U.S. at 29.

[7] *Id.*

[8] *Id.*

Kyllo's house were warmer than the rest of Kyllo's house and were also warmer than either of the other triplex neighbors.[9]

The agent inferred that the additional heat from Kyllo's house was the result of using high intensity lamps to cultivate marijuana within the residence.[10] Based on a previous tip, on utility bills showing the electric usage from Kyllo's residence and on the thermal imaging scan, a warrant was issued to search Kyllo's home.[11] Searching the house under the warrant, agents found over one hundred marijuana plants.[12] Kyllo moved unsuccessfully to suppress the evidence gathered from the warrant and entered a conditional guilty plea to one count of manufacturing marijuana under 21 U.S.C. § 841(a)(1).[13]

The Ninth Circuit Court of Appeals remanded the case for an evidentiary hearing regarding the intrusiveness of thermal imaging.[14] On remand, the District Court for the District of Oregon found that the thermal imaging camera was a non-intrusive device that showed only crude images of the heat radiated from a house.[15] The District Court upheld the validity of the warrant and again denied Kyllo's Motion to Suppress. The Ninth Circuit Court of Appeals affirmed, holding that Mr. Kyllo had no objective expectation of privacy because the thermal imaging camera did not expose any intimate details of Kyllo's life, only amorphous hot spots on the roof and exterior wall.[16]

In review of the Ninth Circuit decision, the United States Supreme Court[17] found that the use of the infrared thermal imaging camera *was* a search under the Fourth Amendment.[18] The Court determined that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[19]

---

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.* at 31.
[17] Justice Scalia penned the Court's opinion.
[18] *Kyllo*, 533 U.S. at 40.
[19] *Id.*

2. Majority Opinion

The Court promulgated the general public use standard out of the Court's purported application of *Katz v. U.S.*,[20] which held that citizens' subjective expectation of privacy must be one that society is prepared to recognize as reasonable.[21] Although the thermal imaging technology used in this case was relatively crude, the Court in *Kyllo* reasoned that the rule adopted needed to be flexible and usable in future decisions to strike a balance between privacy interests and the needs of law enforcement.[22]

The Court molded this holding out of two basic propositions. First, the Fourth Amendment protects the privacy interests of people, not places.[23] Second, the Fourth Amendment's protection is not tied to the "measurement of the quantity or quality of information obtained" by technology,[24] because *all* details revealed of a home are intimate details and are thus protected.[25] The Court found no connection between the sophistication of the equipment used and the intimacy of the details revealed.[26]

Upon these two premises, the Court held that when technology not in general public use explores details of the home that could not have been found without a physical intrusion, "the surveillance is a 'search' and is presumptively unreasonable without a warrant."[27]

The Court failed to explain what general public use meant and how it should be applied both in *Kyllo* and in future cases. The opinion offers no explanation and no illustrations to guide either this Court or future courts on the application of this new standard. The general public use standard simply appears in the holding as a fulcrum upon which to balance the capabilities of new technology against the needs of society to protect personal privacy.

---

[20] 389 U.S. 347 (1967).
[21] *Id.* at 361.
[22] *Kyllo*, 533 U.S. at 36.
[23] *See Katz*, 389 U.S. at 351.
[24] *Kyllo*, 533 U.S. at 37.
[25] *Id.*
[26] *Id.* at 38-39.
[27] *Id.* at 40.

3. Dissenting Opinion

Justice Stevens's dissent argued that the use of thermal imaging was nothing more than an extension of the "plain view" doctrine[28] and that the use of the thermal imaging camera in *Kyllo* was not a search at all.[29] The dissent focused its attention on whether the thermal imaging technology actually penetrated the house or merely detected information outside the home that is in plain view of the senses.[30] In the dissent's view, law enforcement not only has the right, but also the responsibility, to use sense-enhancing equipment to measure heat, smoke, odors, gases or radioactive materials that escape from the home, which could pose a hazard to the community.[31]

Under such a standard, if a person wishes to hide the heat escaping from his house, he has a duty to insulate better to protect his subjective privacy interest.[32] Any inferences law enforcement draw from the use of such technology would be under the guise of reasonable public service, not an intrusion into privacy.[33] Only if the technology provides the user with the functional equivalent of actual presence in the area would a constitutional question arise.[34]

Curiously, only one paragraph of the dissent questions the application or existence of the general public use standard.[35] The dissent briefly questions what general public use might entail and asks whether the thermal imager would meet the Court's definition.[36] The dissent points out, however, that the threat to privacy will grow, not recede, as intrusive technology crosses over into general public use.[37]

---

[28] *Katz*, 389 U.S. at 351 (addressing the plain view doctrine, Justice Stevens explained that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").

[29] *Kyllo*, 533 U.S. at 42 (Stevens, J., dissenting).

[30] *Id.* at 43.

[31] *Id.* at 45.

[32] *Id.*

[33] *Id.*

[34] *Id.* at 44.

[35] *Id.* at 46-47.

[36] *Id.* at 47.

[37] *Id.*

*B. Current Legal Status of Technology Used by Law Enforcement*

In order to understand the problems associated with a general public use standard, a brief overview of precedent on other technology-related Fourth Amendment decisions is required. The Fourth Amendment declares that "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated."[38] This right to privacy, however, generally focuses on the traditional home.[39] Different rules or exceptions to the rules operate in commercial or industrial locations[40] and in residential situations other than the traditional house.[41]

The Court articulated the modern standard to determine when a search is unreasonable in *Katz* as an effort to correct the mistakes made in *Olmstead v. U.S.*,[42] where the Court first dealt with the Fourth Amendment and technology. First courts must determine if the individual has an actual, subjective expectation of privacy.[43] Then, if there is a subjective expectation, courts must determine whether the expectation of privacy is one that society is prepared to recognize as reasonable.[44]

The Court also addressed the plain view doctrine in *Katz*.[45] This doctrine states that police are not expected to avert their eyes from evidence of criminal activity that any member of the public could have observed.[46] The doctrine covers not only information that can be obtained from the regular senses, but also items such as discarded garbage[47] or a naked eye overhead view of homes from an airplane.[48]

---

[38] U.S. Const. amend. IV.

[39] *See e.g. Payton v. N.Y.*, 455 U.S. 573, 590 (1980) (holding that without exigent circumstances, police may not enter a home without obtaining a search warrant).

[40] *Dow Chem. Co. v. U.S.*, 476 U.S. 227 (D. Mich. 1986).

[41] *See e.g. U.S. v. Gooch*, 6 F.3d 673 (9th Cir. 1993) (applying the exception to a defendant living in a tent); *U.S. v. Ruckman*, 806 F.2d 1471 (10th Cir. 1986) (defendant living in a cave).

[42] *Olmstead v. U.S.*, 277 U.S. 438, 464 (1928) (holding that while telephone wire tapping may be an objectionable practice, the Fourth Amendment and the Constitution do not forbid the practice unless actual unlawful entry into the home occurs). The Court felt that since the wiretapping occurred at a point where the telephone line was in the public domain, there was no Fourth Amendment violation. *Id.*

[43] *Katz*, 389 U.S. at 361.

[44] *Id.*

[45] *Id.* at 351 (relying on *Lewis v. U.S.*, 385 U.S. 206, 210 (1966) and *Rios v. U.S.*, 364 U.S. 253 (1960)).

[46] *Katz*, 389 U.S. at 351.

[47] *Cal. v. Greenwood*, 486 U.S. 35 (1983).

[48] *Cal. v. Ciraolo*, 476 U.S. 207 (1986).

Based on this framework, courts have attempted to review individual technologies on a case-by-case basis,[49] placing them within or outside the plain view doctrine and thereby establishing whether use of a particular technology was a Fourth Amendment search requiring a warrant. Courts will generally include technology that enhances the senses under the plain view doctrine and use of such technologies by law enforcement is not considered a search at all under the Fourth Amendment. These plain view technologies include airplanes using mapping cameras,[50] helicopters,[51] drug sniffing dogs,[52] pen registers to track phone numbers,[53] binoculars[54] and night vision goggles.[55] Courts have suggested that gas chromatography and mass spectrometry[56] would probably be analogous to a canine sniff and, therefore, would also not be a search.[57]

Other technologies have been clearly placed off limits absent a warrant. These include most eavesdropping devices,[58] use of a beeper to track movement inside a home[59] and the use of high power telescopes.[60] Courts have provided glimpses into how developing technologies will fit into future Fourth Amendment challenges. Advances in intrusive forms of radar-based technologies,[61] X-ray technology[62] or ultrasound technology[63] are unlikely to be included in the plain view doctrine and may always require a warrant. Courts have similarly suggested that satellite-based

---

[49] *See generally Riley*, 488 U.S. 445 (addressing helicopters flying overhead); *Dow Chem. Co.*, 476 U.S. 227 (addressing airplanes using mapping cameras); *Smith v. Md.*, 442 U.S. 735 (addressing the use of a pen register to track telephone numbers dialed); *Silverman*, 365 U.S. 505 (addressing the use of eavesdropping devices).

[50] *Dow Chem. Co.*, 476 U.S. 227.

[51] *Riley*, 488 U.S. 445.

[52] *U.S. v. Place*, 462 U.S. 696 (1983).

[53] *Smith*, 442 U.S. 735.

[54] *N.J. v. Citta*, 625 A.2d 1162 (N.J. Super. 1990).

[55] *U.S. v. Eberle*, 993 F. Supp. 794 (D. Mont. 1998); *U.S. v. Field*, 855 F. Supp. 1518 (W.D. Wis. 1994).

[56] Aline McKenzie, *How Testing Works*, Dallas Morning News 2C (Apr. 1, 2001). In this process, a sample of a gas, liquid, or solid is vaporized and sent through a tube that separates different chemical substances by weight for analysis. *Id.*

[57] Richard S. Julie, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 Am. Crim. L. Rev. 127, 138 (Winter 2000).

[58] *Katz*, 389 U.S. 347 (electronic telephone surveillance); *Silverman*, 365 U.S. 505 (a "spike mike" listening device).

[59] *U.S. v. Karo*, 468 U.S. 705 (1984).

[60] *U.S. v. Taborda*, 635 F.2d 131 (2nd Cir. 1980); *U.S. v. Kim*, 415 F. Supp. 1252 (D. Haw. 1976).

[61] *Kyllo*, 533 U.S. at 36 n. 3.

[62] *McMorris v. Alioto*, 567 F.2d 897 (9th Cir. 1978).

[63] *U.S. v. 15324 County Hwy. E*, 219 F.3d 602 (7th Cir. 2000).

technology would be viewed as similar to a high power telescope and, as such, would be offensive to the Fourth Amendment.[64]

## III. ANALYSIS

In *Kyllo*, the U.S. Supreme Court brought to bear a general public use standard that it had briefly articulated and never defined almost fifteen years ago.[65] The Court continues to leave the concept of general public use undefined. If the Court felt the need to base use of technology by law enforcement on the dissemination of the technology to the general public, the Court had several possible factors upon which to base such a determination. A definition based on *actual* use by the general public, however, disqualifies almost every previously approved technology now in service by law enforcement. A definition which focuses on the wide spread use of technology in and around the public sector would protect existing precedent. The thermal imaging camera in *Kyllo*, however, then fails to meet the Court's new standard. Newer and more intrusive technologies still under development also present significant privacy issues when compared to an "in and around" general public definition. The Court failed to acknowledge the problem and did not examine the possible factors and challenges involved in defining the new standard. The Court also failed to offer a solution upon which law enforcement and the citizenry can depend to predict future interactions between technology use and privacy interests.

### *A. Generic, Dictionary and Precedent Definitions of General Public Use*

Under *Kyllo*, the grounds for warrantless use of technology by law enforcement focused not on the capabilities of the equipment or the intimate details the equipment may reveal, but rather on whether the technology in question was in general public use.[66] The Court offered no illustration or definition as to what general public use might mean, nor did

---

[64] *Dow Chem. Co.*, 476 U.S. at 238.

[65] *See Ciraolo*, 476 U.S. at 215 (stating that "in an age where private and commercial flight in the public airways is routine," it is unreasonable to expect that one's marijuana plants are constitutionally protected from being observed at an altitude of 1000 feet); *Dow Chem. Co.*, 476 U.S. at 238 (stating that "[i]t may well be . . . that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.")

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

it explain how the thermal imaging camera failed to meet the new standard. The Court had many possible ways to define how it would measure general public use, but reference to traditional interpretive tools show that all possible combinations either create conflict with existing precedent or make the actual decision in *Kyllo* inconsistent with the general public use standard articulated.

Courts use the term "general public" in many situations.[67] Seldom do courts, however, actually define the term under existing precedent. The phrase "general public" has been used in past precedent to aid in interpretation of statutory language and to determine legislative intent.[68] When a definition of "general public" is required, courts have broadly included everyone in the community or at least all the possible range of people in the particular group being discussed.[69] The Court's "general public" definitions center on openness to all people without restrictions to any class or group within the community. To use such a definition for the general public use of technology would be consistent with past precedent, and such a distinction would be easy for the average citizen to understand.

The Court could have reviewed the plain meaning of general public use. Under such a view, an item in general public use could be use that permeates our society. Items in general public use might include telephones,[70] television[71] and automobiles.[72] Although these items are not

---

[67] *See e.g. Nunez v. Super. Ct. of Ariz.*, 503 P.2d 420, 422 (Ariz. App. 1972) (using general public to differentiate from students, faculty, staff, or employees at an educational institution), *Good v. Iowa Civil Rights Comm.*, 368 N.W.2d 151, 154 (Iowa 1985) (using general public to help define public accommodations); *PICPA Found. for Educ. and Research v. Cmmw. of Pa.*, 634 A.2d 187, 189 (Pa. 1993) (disqualifying appellant as a non-profit educational institution because the benefits to the general public were incidental).

[68] *Audubon Country Club v. Cmmw.*, 183 S.W. 911 (Ky. App. 1916).

[69] *Lighting of Lodge Halls*, 7 Pa. D. & C. 129 (Pa. Dept. of Justice, Mar. 26, 1925) (quoting the Century Dictionary). The court defined general public as "[o]f or belonging to the people at large; relating to or affecting the whole people of a state, nation, or community; opposed to private . . . open to all the people; shared in . . . or participated in or enjoyed by the people at large; not limited or restricted to any particular class of the community . . . the general body of people constituting a nation, state or community; the people indefinitely." *See also Audubon Country Club*, 183 S.W. at 912 (declaring general public as "[o]pen to all people-shared in or to be shared or participated in or enjoyed by people at large; not limited or restricted to any particular class in the community").

[70] *See* Robert W. Crandall, *Bridging the Divide Naturally*, Brookings Rev. 38 (Jan. 1, 2001); Deseret News (Salt Lake City, Utah) C04 (July 11, 2001) (showing that telephone service is now virtually ubiquitous nationwide and 54% of American households now have at least one cellular phone).

[71] *See* Brian Lowry, *Company Town: Census Data Show Surge in Homes with Televisions*, L.A. Times C6 (Aug. 9, 2001) (noting, "[m]ore than 98% of all U.S. homes currently have at least one television set").

[72] *CBS News: This Morning*, "Census Report Shows Population Explosion" (CBS Dec. 29, 2000) (TV broadcast, transcript available at 2000 WL 6655829) (boasting 281 million people living in the

used or owned by everyone, they are in use by a high percentage of society on a daily basis. This definition is also attractive because it is relatively simple, plain and easy for the average citizen to understand. A plain meaning of general public use would also seem to be consistent with case precedent definitions of "general public."

The dictionary also offers only a generic look at "general public." Although there are variations between dictionaries, most definitions of "general" center on "involving, applicable to, or affecting the whole."[73] "Public" is usually defined as "of, belonging to, or concerning the people as a whole."[74] General public use, under dictionary definitions seems to necessarily include an item in use by or at least accessible to all members of the community. Like case precedent and plain meaning, the dictionary version of general public use offers a simple explanation to the average citizen. Unlike case precedent and plain meaning, however, the average citizen who can read and who has access to a dictionary may look up the definition of these words to form an independent understanding of general public use.

While a plain meaning, case precedent or a dictionary meaning might be the most easily understood definition of general public use by the citizenry, there are two problems with such a generic approach. First, a broad, all inclusive and simple definition of general public use is inconsistent with almost every technology-related Fourth Amendment decision the Court has made to date.[75] A generic meaning of general public use would disqualify all but the most common technology items used in our society. While a pen register of telephone numbers dialed *might* pass constitutional muster under this definition because of the wide availability of telephone service, helicopters, drug-sniffing dogs, night vision goggles and mapping cameras are not used by all the citizens of a community and therefore, would be inconsistent and contradictory to existing Fourth Amendment precedent.

Second, there will always be a portion of society that does not use nor has access to a particular product, either because of a lack of desire, lack of availability or lack of money to purchase the product. Few people have flown in a helicopter[76] or used night vision goggles,[77] yet these devices are approved for use by law enforcement without a warrant.

---

U.S. according to the 2000 U.S. Census); Peter Bacque, *Moving on Automobiles Become Societal Gauge*, Richmond Times-Dispatch (Richmond, Va.) S23 (Jan. 20, 2000) (stating that there were over 206 million motor vehicles in the U.S. by 1997).

[73] *Webster's New World College Dictionary* 591 (Michael Agnes, ed., 4th ed., IDG Books Worldwide, Inc. 2000).

[74] *Id.* at 1160.

[75] See *supra* n. 1 for a listing of these previous decisions.

[76] Trudy Gray, *The Challenges of Copters: Beaver County Airport is Among Few Places Offering Lessons*, Pitt. Post-Gazette W6 (June 27, 2001) (stating that helicopters are often delegated to narrow specific uses such as marine rescue, pest control, traffic control, transportation of critically ill patients,

A generic definition is inherently broad and does not balance the individual's needs for privacy against society's need to prevent crime and to protect public safety. In this loose interpretation, citizens have little need to protect personal privacy against technology because none of the invasive forms of technology used by law enforcement would meet the broad, inclusive definition. Law enforcement's use of technology to advance society's interest in preventing crime would be, for all practical purposes, eliminated without a warrant.

### *B. Specific Objective Factors*

None of the generic definitions of general public use are effective in reconciling past decisions and predicting future interactions. When, then, does a technology cross over into general public use? Objective, quantifiable standards are equally unable to give form to this standard.

#### 1. Sector of Public Using the Technology

The Court could have developed a standard that would classify technology according to the sector of the public using the device. Use of new technology, such as night vision goggles, often starts with military or government applications.[78] Eventually, these breakthroughs are copied or distributed down for use in the commercial and industrial markets.[79] At some point, devices such as night vision goggles will cross over from the commercial sector into the hands of the retail consuming citizenry.[80]

---

and tourism; furthermore, licensing to fly a helicopter requires between fifty and two-hundred hours of instruction and flight training).

[77] See Joe Hanak, *Basic Night-Vision Glasses Give User an Owl's Eye View*, The Plain Dealer (Cleveland, Ohio) 2C (July 2, 2001); James Hannah, *Safety Workers Take Dim View of the Dark Techn.: Police and Rescue Squads Love Night-Vision Goggles but Can't Afford Them*, L.A. Times A10 (Feb. 20, 2000); Mike Wilson & Mary Evertz, *Toys They Won't Put Down*, St. Petersburg Times 5D (Dec. 5, 2000) (noting that although toy versions of night vision can be bought for as little as $14.95, most commercial quality units cost between $450-$12,000 and are used primarily by law enforcement, hunters and hikers).

[78] Hannah, *supra* n. 77 (discussing the fact that only the military can afford the best technology and discussing new research for the military to improve and invent the next generation of night vision goggles).

[79] Hanak, *supra* n. 77 (discussing the entry of night vision goggles into the commercial and retail market and the slow entry into civilian use of night vision goggles by police, park rangers and rescue squads). Prices have come down to a level where avid hunters, hikers, and people concerned with home security can now afford and have availability to moderately priced night vision glasses.

[80] *See* Wilson & Evertz, *supra* n. 77 (noting that while military style glasses are often over $10,000, a simple, but functional, toy set of night vision glasses now goes for as little as $14.95).

A standard that marks the point where technology crosses into a retail citizen market could be the benchmark measuring when technology is in general public use. Although barriers such as money and geography might limit the *actual* use of approved items such as an airplane or binoculars, the fact that such items are for sale to the retail public would be the crossover point.

Perhaps the true intention of the Court was not to measure actual public use but rather to distinguish whether each technology is in general possession either by a large number of individual citizens or by a significant portion of law enforcement. This distinction would put citizens on notice that they have a diminished expectation of privacy and that they can actively take countermeasures to protect their privacy interests.

Under the *Kyllo* test, once a device has crossed over into general public use, a homeowner must take proactive steps to protect his privacy from the intrusive capabilities of that device. As a local retailer picks up a new product, there is no way to distinguish the flash point where technology that was forbidden to law enforcement in a city yesterday now must be proactively protected against today. There are no measuring tools that would allow either law enforcement or the general public to know when technology makes the jump into general public use. Likewise, there are no tools to give notice to the general public when a technology has crossed over into general public use.

The problem with a retail market balance point on technology is that neither the public nor law enforcement will be aware when a technology has crossed the new line. Both law enforcement and citizens in Idaho may not be aware that new technological devices are now for sale to the public in New York. A nationwide retail standard would force rural areas to somehow keep track of retail trends in major metropolitan areas to know when technology is now permissible. This standard is immeasurable and unrealistic.

Localizing a retail standard would open up courts to different standards for the same technology all over the country. Cities right next to each other may have different standards for warrantless searches using the same technological device. Ignorance of the law is generally not considered an excuse.[81] Confusion as to what is required to make a technology-based, warrantless search and an ongoing shift in how technology standards as devices are disseminated would seem to necessitate some form of defense based on ignorance for citizens who are trapped by evidence produced from warrantless, technology-approved searches.[82]

---

[81] *Lambert v. Cal.*, 355 U.S. 225, 228 (1957).

[82] *See e.g.* Model Penal Code § 2.04(3)(a), which allows a defense of ignorance or mistake when "the statute or other enactment defining the offense is not known to the actor and has not been

2. Geography of Use

In the same way that technology often flows from government down to the general population, new products often start their distribution at larger metropolitan areas and slowly disseminate to smaller cities and rural areas. The Court could base the crossover into general public use on the dissemination of that technology into each community. What may be commonplace to Los Angeles may be unheard of in rural Montana. This standard would measure use of technology in each particular city or area to determine when citizens in those areas need to proactively protect their privacy interests.

While this might be helpful for an individual defendant in a particular city, this standard would not proactively predict when general public use occurs in each area. Under what conditions does technology cross over into general public use in your city? What tools are used to measure your local community standard of general public use? Sales data? Geographic city limits? As with a retail sales standard, a geographic standard would seem to necessitate the defenses of ignorance of the law, mistake of fact or mistake of law in fighting evidence obtained during a warrantless search of the home.

3. Media Attention

Most people in America now have a television and telephone,[83] and more people each day are logging onto the Internet.[84] As traditional print media, broadcast media and the Internet inundate us with more information daily, the Court could attempt to measure general public use based not on *actual* usage within the public, but based instead on the quantity of information about technology that is disseminated to the general public that shows use within the public sector.

---

published or otherwise reasonably made available prior to the conduct alleged." The general public use standard of the *Kyllo* court requires a person to proactively protect his privacy interests from technology that is in general public use. As the standard of general public use shifts through dissemination, however, there must be some way for the private citizen to protect himself from a sudden change in his duty to protect his privacy from new technology that has crossed into public use but has not been written into statute or made available to the citizen through other court cases. Perhaps a Model Penal Code approach could be taken to offer such a defense. This note will not, however, explore such a defense.

[83] Crandall, *supra* n. 70 (showing that telephone service is now virtually ubiquitous nationwide and 54% of American households now have at least one cellular phone); Lowry, *supra* n. 71.

[84] *See* Michael J. Weiss, *Online America*, Am. Demographics 53 (stating that as of November 2000, 56% of Americans were logging onto the Internet each month, with steady increases in availability to minority and poor citizens).

Drug-sniffing dogs are not actually used by the general public, but the media has covered their use in recovering drugs, money and people, both living and dead.[85] The Court recognizes a canine sniff as an acceptable device open to law enforcement without a search warrant.[86] A standard based on media exposure could be consistent with items such as binoculars, helicopters and airplanes, which receive media exposure through many sources.

Some of the latest technology in use or in development, however, invariably shows up in national media. Technologies such as night vision goggles were introduced to the public through the media during the Gulf War. In the aftermath of the World Trade Center attacks, the media has covered new airport security technology in development such as biometric systems which identify people from body features, iris recognition systems, face recognition systems, smart identity cards with encrypted security chips and smart camera systems which identify objects and people and then track them from camera to camera.[87] Under a media exposure standard, it would seem that extensive media attention would cause these new technologies to immediately cross over into general public use. Not only would such technology cross over as fast as the news media could develop a story on the technology, but this standard would make the news media, and not the legislature or the courts, the body that determines when technology is in general public use.

While almost all of the public has access to newspapers and television, few Americans actually review news on a regular basis. On an average day, less than 60% of the public read a daily newspaper, less than 40% of Americans watch a network news program daily, less than 25% of us turn to radio for news during the morning commute and only 12% of Americans watch cable television for news daily.[88] It would be a privacy disaster to establish a standard of technology in general public use based on media exposure when significant parts of the general public either lack consistent access to media or are too busy to get current information from media on a regular basis.

Further, there is no meaningful way to determine at what point there is enough media attention to give constructive notice of new technology. Under such a media standard, a citizen's proactive duty to protect his privacy could end up turning on something as arbitrary as the Neilsen

---

[85] *See e.g.* Linda Wilson Fuoco, *Dogs on Duty*, Pitt. Post-Gazette S1 (Mar. 1, 2000).

[86] *Place*, 462 U.S. 696.

[87] *See* Chris Holme, *Big Brother Is Ready to Watch Out for You*, The Herald (Glasgow, Scotland) 4 (Sept. 20, 2001).

[88] Assoc. Press, *More and More News Comes from the Internet*, Grand Rapids Press B4 (June 12, 2000).

ratings of his favorite television show. A media exposure standard is too arbitrary to be applied in a way that would allow the average citizen to be prepared to take proactive steps to protect his privacy against new technology.

### *C. Factors Test*

All of the distinctions listed above help describe when a particular technology might be in general public use. The dissemination of technology to various sectors of the industrial, commercial, or residential market, the number of units in use, the geography of use, and media attention all play a role in our free enterprise economy and in our daily lives. Perhaps the fairest test of general public use would be a factors test, which would review all of these factors when balancing dissemination and warrantless use of technology.

"The Constitution was written to limit the authority of Government, not private citizens."[89] Under our Constitution, searches by law enforcement without a warrant are presumptively unreasonable.[90] The use of technology in a search by law enforcement, therefore, should also be presumptively unlawful to use without a warrant. The new *Kyllo* standard suggests that courts should place the burden on the government to show that the technology used in that particular situation was in general public use in the community. If the government could show, through a balancing of factors, that a reasonable defendant knew or should have known about the technology and its capabilities, then the government could overcome that presumption and the use would be allowed.

The problems with this approach are twofold. First, under such a standard, law enforcement must illegally use the technology without a warrant and then later determine in court if it can overcome the warrant requirement. This "use it until proven wrong" approach creates potential problems for law enforcement. A zealous officer may abuse his discretion, using all technology all the time in illegal, warrantless searches. This would grossly abuse the privacy interests of individual citizens. While the courts may find the technology-based searches unconstitutional at a later date, the privacy interests of the individual citizen would have already been abridged. A more cautious approach to law enforcement could find law enforcement second-guessing where the technology line is currently being

---

[89] Thomas D. Colbridge, Kyllo v. United States: *Technology Versus Individual Privacy*, 70 F.B.I. L. Enforcement Bull. 25, *9 (Oct. 1, 2001) (available at 2001 WL 13957468).

[90] *Ill. v. Rodriguez*, 497 U.S. 177, 181 (1990).

drawn. Portions of the law enforcement community would err on the side of caution and not use permissible technology to solve and prevent crime on the assumption that the individual technology in question has not been expressly permitted.

Second, homeowners neither want to measure balancing factors nor do they have tools to accomplish measurement of those factors. Citizens want to know what is required of them ahead of time to protect their privacy interest in the home. Under a factors test, the public will not know what is required of them until law enforcement invades their privacy and the courts balance the factors to see if warrantless use of technology by law enforcement was legitimate under those particular circumstances.

A factors balancing test provides a reactive standard and a sliding scale of general public use. Under the factors test, the use of a new technology may currently be illegal without the use of a warrant. As the factors change, however, that status may change without warning or notice, requiring citizens to immediately protect their privacy interests from this same particular source or device. Citizens have little understanding of legal factors and an unwritten standard based on a reasonable defendant offers little help for the average citizen in recognizing when a new technology can now permissibly invade his privacy. A factors standard is unworkable for both law enforcement and for citizens and this standard would give the courts endless cases involving changing conditions and inconsistent verdicts.

### *D. The Sliding Scale of General Public Use*

There is no definition of general public use available that either conforms to Fourth Amendment case law or can be used to predict future interactions between technology and privacy. Each possible factor upon which the court could base a distinction of general public use has problems in measurement, in consistent application, or is hopelessly reactive. The result of such definitions can only be an ad hoc evaluation of each case on its merits. This will lead to inconsistent verdicts between jurisdictions and changing standards in the same jurisdiction as technology crosses over into general public use.

Technology naturally moves from sector to sector, into more geographic areas, and receives increased media attention as it moves into the marketplace. As a natural part of the American free enterprise system, technology slides along an imagined scale from private, restricted use to an open, general public use. Even if each technology's crossing point into general public use could be plotted along such a sliding scale, both the general public and law enforcement are unable to see where each

technology is placed on the scale at any given point. This makes any generic standard based on general public use a reactive standard.

Almost all cases and laws are by nature reactive. The legislature often passes legislation in reaction to an existing or perceived evil to be remedied. Likewise, judges can only interpret common law or statutes when there is a case in front of the court.

While this reactive method of interpreting and enacting laws works well in most situations, the right of privacy guaranteed by the Fourth Amendment requires a more exacting, predetermined standard. "The Fourth Amendment has been called the centerpiece of a free, democratic society."[91] Unlike other general protections provided in our laws, the Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[92] "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property" that must be prevented.[93] A standard that allows a violation of that right to privacy and then seeks later to determine the legitimacy of that invasion flies in the face of the penumbra of privacy created and guaranteed by the Bill of Rights.[94]

The court has stated that the Fourth Amendment creates a "right to privacy, no less important than any other right carefully and particularly reserved to the people."[95] With no measurement tools in place and no reporting tools available, law enforcement is left guessing when the warrantless use of new technology is permitted. Using the reactive standards above, average citizens will only know that new technology has crossed over into general public use after their privacy interests have been invaded by the new technology. In addressing one of our most fundamental rights, the Court must not have intended to leave such a void in defining and applying the general public use standard.[96]

---

[91] Ian M. Comisky, Lawrence S. Feld, & Steven M. Harris, *Tax Fraud and Evasion* vol. 2, §14.02[1] (RIA 2001) (quoting Yale Kamisar, *The Fourth Amendment and Its Exclusionary Rule*, XIV The Champion 20, 21 (Sept./Oct. 1991)).

[92] U.S. Const. amend. IV.

[93] *Boyd v. U.S.*, 116 U.S. 616, 630 (1886).

[94] *See Griswold v. Conn.*, 381 U.S. 479, 484 (1965) (discussing the various penumbras and zones of privacy created by the Bill of Rights).

[95] *Id.*

[96] *Kyllo*, 533 U.S. at 36 (stating 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").

1. General Public Use Based Upon Use "In and Around" the Public and Not on "Actual Use" by the General Public.

Actual use by the general public is unworkable and leaves both law enforcement and the average citizen guessing where technology may be used in a search. The Court must have intended something in a general public use standard other than *actual* use by the public. A definition of general public use that is consistent with existing Fourth Amendment precedent is a definition based on use in and around the public sector and not on *actual* use by the general public. A definition based on dissemination and the use of technology in and around the general public would be consistent with such approved technology as airplanes, helicopters, drug-sniffing dogs, binoculars, and night vision goggles. The in and around definition of general public use is consistent when applied to technology that is not approved for warrantless use by law enforcement. While some forms of x-rays and ultrasound technology are used in and around the public in the medical field, courts so far have limited their discussion of these restricted types of technologies to potential applications yet to be developed for the sole purpose of conducting searches.[97]

An argument can similarly be made for satellite technology. The courts have suggested that satellite technology would be offensive to the Fourth Amendment.[98] The use of satellites flying in space, however, would be different from technologies that are in use at ground level, such as binoculars, and further would be different even from airplanes and helicopters flying above. Satellites orbiting the earth give a citizen no warning or notice that he is under surveillance. Conversely, a person has a chance of seeing binoculars or other ground technology in use, and airplanes and helicopters can not only be seen flying overhead, but also have loud engines generally giving notice of their arrival over your home.

Approval of technology that is known to be in use in and around the general public appears to both protect existing precedent and to give form to a standard which might gage future interactions between technology and the Fourth Amendment. The adoption of such a standard, however, still presents a standard which does not proactively allow law enforcement or the average citizen to ascertain the balance point where the privacy

---

[97] *Kyllo*, 533 U.S. at 37 n. 3 (reviewing radar-based through-the-wall surveillance, a hand-held ultrasound system and a radar flashlight in development by the U.S. Department of Justice); *15324 County Hwy. E*, 219 F.3d 602, 604 (7th Cir. 2000) (holding that if thermal imagers or other technology some day become so sensitive that they can create a video image of everyone in a home and their exact activities, such a device would create significant Fourth Amendment concerns).

[98] *Dow Chem. Co.*, 476 U.S. at 238.

interests of the individual meets society's need to prevent crime. Further, while an in and around definition of general public use may protect existing precedent, close scrutiny of such a definition will show that the infrared camera in *Kyllo* was decided incorrectly under such a general public use definition. Finally, use of an in and around definition of general public use presents serious privacy implications when projected forward to emerging, highly intrusive technologies that are still under development.

### 2. *Kyllo*'s Thermal Imaging Camera Does Not Survive Scrutiny under a General Public Use Standard

While the Court in 2001 found thermal imaging to not be within general public use, at least one district court as early as 1992 described thermal imaging technology as "'off the shelf,' having been in general use for fifteen years."[99] In the nine years since that 1992 decision, the public has become familiar with seeing thermal images of distant battlefields on the evening news and has seen the use of thermal imaging cameras by law enforcement on several popular police reality television programs.[100]

Thermal imaging cameras have achieved many uses since the military developed the technology. Current commercial uses include detection of roof leaks, steam pipe leaks, cracks in high voltage transmission lines and overloaded transformers.[101]

Law enforcement found multiple uses for thermal imaging beyond searching private homes without a warrant. Thermal imaging has been used to enhance officer safety by locating hidden threats such as suspects, guard dogs and dangerous obstacles.[102] Thermal imaging allows night time search and rescue operations to cover a large area quickly with less manpower.[103] Thermal imaging has also been used in the air by law enforcement in high-speed vehicle pursuits to see vehicles driving without headlights and to detect recently driven vehicles in crowded parking lots or remote areas.[104] Finally, law enforcement officials along the border with Mexico have

---

[99] *U.S. v. Deaner*, 1992 U.S. Dist. LEXIS 13046 at *6 (M.D. Pa. July 27, 1992).

[100] Colbridge, *supra* n. 89.

[101] *Deaner*, 1992 U.S. Dist. LEXIS 13046 at * 6.

[102] John Mesenbrink & Doug Van Dover, ***Protecting Borders with Thermal Imaging***, 38 Security 8, 33 (Aug. 1, 2001) (available at 2001 WL 11592950).

[103] *Id.*

[104] *Id.*

found thermal imaging an effective tool in nighttime border patrol and fugitive searches.[105]

Fire departments make up perhaps the fastest growing market and use of thermal imaging equipment. Latest estimates show that ten percent of all fire departments in the United States are now equipped with thermal imaging devices and that number is growing daily.[106] Fire departments have found that with thermal imaging cameras firefighters can see potential victims in smoke filled rooms that normally would offer no visibility and the device allows firefighters to locate the hottest and most dangerous parts of a fire without actually entering the structure.[107]

Thermal imaging is now in limited use in both the animal and human medical fields.[108] With respect to humans, thermal imaging is being developed "to diagnose circulatory [problems] and nerve injuries, including migraines and toothaches."[109] In animals, the technology is being used to detect estrogen levels of animals in heat and to test bulls for fertility.[110] In horses, the thermal imager can detect possible "injection site reactions, abscessed implants and lameness that alters blood flow."[111]

The use of thermal imaging technology has moved from military to government to commercial use. The number of units in use continues to grow as new applications emerge and prices come down with competition. Geographically, more police, fire and commercial applications are expanding the geographic area in which this technology is being used. While commercial applications of thermal imaging get less media attention, purchase of thermal imaging cameras has received expanded media coverage in the areas of law enforcement and fire department purchases.[112]

Thermal imaging has received a tremendous amount of direct public exposure. Cities with as small as 15,000 residents have fire departments equipped with at least one thermal imaging camera.[113] One of the major

---

[105] *Id.*

[106] Dana E. Corbin, *Seeing is Believing*, 69 Occ. Health & Safety 8, 6067 (Aug. 1, 2000) (available at 2000 WL 10134994).

[107] *Id.*

[108] Assoc. Press, *Thermal Camera Helps Keep Track of Cattle's Health; Product for Public Use is Expected Within a Year*, St. Louis Post-Dispatch D9 (Dec. 24, 2000).

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *See* Jason Jett, *Following a Hot Trail–Special Camera Aids Police Investigations*, Star-Ledger (Newark N.J.) 025 (Aug. 27, 2000); Peter Marteka, *Firefighters Will Dedicate Thermal Imaging Systems to Contributors*, Hartford Courant (Conn.) B22 (Apr. 13, 2001); Lou Mumford, *Niles Gets Heat-Sensing Camera*, S. Bend Trib. (Ind.) A4 (June 3, 2000).

[113] *See* Valryn Bush, *Butler Twp. Firefighters Buy High-Tech Cameras*, Dayton Daily News (Ohio) Z56 (Oct. 26, 2000).

drawbacks to the use of thermal imaging has been the cost of the equipment. Many smaller or less affluent areas have trouble footing the $15,000-$25,000 price tag of these devices.[114] The answer to small city budgets and limited fire department resources in many cases has been to involve the public directly to raise the funds necessary.

Some states have set up grant programs to quickly get thermal imaging into more fire departments in their districts.[115] Grassroots fund raising campaigns, however, have been one of the most effective ways to pay for thermal imaging. Fire departments often get help in the form of direct donations from local business, civic organizations and the general public.[116] Not only are these groups and citizens directly involved in the fund raising and purchasing of the thermal imaging camera, the fire department often holds open houses at fire stations after the purchase to thank the public for its support and to give pubic demonstrations of the thermal imaging camera at work in their neighborhoods.[117]

Although thermal imaging technology is rarely actually used by the retail buying public, the general public has been widely exposed to both the dissemination and public use of this technology. The most similar technological device, which is approved for warrantless use by law enforcement to the thermal imaging camera may be night vision, goggles. Police and fire departments use both extensively. Both receive media attention. Neither has extremely wide distribution or actual numbers in use. Neither is normally detectable by citizens when being used. Neither is actually in general public use, but both are in use in the community by local government and private industry.

The use of night vision goggles is permitted without a warrant, however, and the use of the thermal imaging camera is forbidden. To remain consistent, the thermal imaging camera must be considered in general public use in the same manner as night vision goggles or the Court must find another way to distinguish the two technologies based on something other than the use of each technology in the general public. With the many uses of thermal imaging and the wide variety of people who come into direct contact with the use of thermal imaging technology, the Court in *Kyllo* failed to closely examine its own standard in determining what constitutes technology in general public use.

---

[114] Corbin, *supra* n. 106.

[115] Jett, *supra* n. 112.

[116] Marteka, *supra* n. 112.

[117] Marteka, *supra* n. 112; Mumford, *supra* n. 112.

### 3. The In and Around Definition of General Public Use Presents Serious Privacy Problems When Projected Against Emerging Highly Intrusive Technologies

While the thermal imaging camera in *Kyllo* was questioned on the basis of whether the technology had achieved general public use status, new technologies currently under development such as millivision and tempest monitoring present a much more serious problem when held to *Kyllo*'s new standard. The problem with these new technologies is not when they will cross over into general public use, but rather what to do with their incredibly intrusive capabilities once that crossover takes place.

Millivision wave technology uses electromagnetic radiation capable of seeing through most clothing, packaging and many wall materials while providing detailed images of the area scanned.[118] Suggested future uses of the technology include concealed weapon detection, surveillance and monitoring, contraband detection and situation assessment.[119] Cameras and scanners are currently in the development stage.[120]

Tempest monitoring is a technology under development that will allow a person several hundred yards away to view what is on the monitor of your computer and to show him exactly what you are viewing or writing on your computer screen.[121] No phone lines are needed for this technology, as the technology picks up the unique radio frequency waves generated by a computer monitor and reconstructs them on a distant monitoring device.[122] Under a *Kyllo* standard, homeowners would be forced to employ counter-technology to block intrusive scanning technology in general public use.

The result would seem to be a future home which resembles a fortress, armed with heat dampening walls to avoid thermal detection, counter-technology devices to prevent penetrating forms of ultrasound and electromagnetic waves, roofing materials incapable of being penetrated by satellite technology and scrambling technology to keep hackers and the public at large from reading the email on our computer screen.

As these technologies cross over into general public use, the average citizen will need to proactively protect his privacy interests and it is far

---

[118] Millivision, *About Millimeter Waves* <http://millivision.com:8071/mmw.html> (accessed Dec. 5, 2001).

[119] Millivision, *Security Applications* <http://millivision.com:8071/security.html> (accessed Dec. 5, 2001).

[120] Millivision, *Product Development* <http://millivision.com:8071/products.html> (accessed Dec. 5, 2001).

[121] Michael J. McCarthy, *The Pentagon Worries that Spies Can See Its Computer Screens*, Wall Street Journal A1 (Aug. 7, 2000).

[122] *Id.*

from clear how a general public use standard would or could be applied to such a situation. The standard articulated in *Kyllo* actually diminishes the average citizen's privacy rights by demanding that citizens now impossibly protect their privacy interests against highly intrusive technology as it crosses into the realm of general public use.

## IV. CONCLUSION

The *Kyllo* general public use standard further strains the tension between personal privacy and legitimate use of technology by law enforcement in the goals of preventing crime and protecting public safety. Future decisions regarding warrantless use of technology by law enforcement are impossible to predict from the *Kyllo* general public use standard.

Technology should be able to progress at the fastest level of distribution the market will allow, and neither the courts, law enforcement, nor the average citizen should have to keep measure of technological progress to determine when general public use occurs and when proactive steps need to be taken to protect individual privacy in the home.

"[T]he correct inquiry is whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[123] The *Kyllo* Court missed an opportunity to further define the proper balance between law enforcement, technology and the privacy interests of the homeowner. Given the incredible speed and inventiveness of the American entrepreneur, however, the Court is likely to soon get another opportunity to examine the issue in detail.

---

[123] *U.S. v. Ishmael*, 48 F.3d 850, 855 (5th Cir. 1995) (quoting *Oliver v. U.S.*, 466 U.S. 170, 183 (1984)).