



Volume 105 | Issue 1

Article 9


September 2002

Terrorism and Weapons Detection Technology: Reevaluating the Reasonable Expectation of Privacy after 11 September 2001

Michael A. Menzel Jr.

West Virginia University College of Law

Follow this and additional works at: <https://researchrepository.wvu.edu/wvlr>

 Part of the [Privacy Law Commons](#), and the [Terrorism Studies Commons](#)

Recommended Citation

Michael A. Menzel Jr., *Terrorism and Weapons Detection Technology: Reevaluating the Reasonable Expectation of Privacy after 11 September 2001*, 105 W. Va. L. Rev. (2002).

Available at: <https://researchrepository.wvu.edu/wvlr/vol105/iss1/9>

This Student Note is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact ian.harmon@mail.wvu.edu.

**TERRORISM AND WEAPONS DETECTION
TECHNOLOGY: REEVALUATING THE
REASONABLE EXPECTATION OF PRIVACY AFTER
11 SEPTEMBER 2001**

I.	INTRODUCTION	250
II.	DEVELOPING AND CATEGORIZING CONCEALED WEAPON DETECTION SYSTEMS.....	253
A.	<i>Concealed Weapon Detection Systems Currently Under Development.....</i>	253
B.	<i>Categorizing Weapon Detection Systems.....</i>	254
C.	<i>Illustrating the Effect of Resolution and Intrusion on Classifying Surveillance Technology</i>	256
III.	THE EVOLUTION OF FOURTH AMENDMENT SEARCH AND SEIZURE DOCTRINE	257
A.	<i>The Birth of the Fourth Amendment.....</i>	257
B.	<i>Pre-Katz Property Based Approach</i>	258
C.	<i>The Impact of Katz and Katz Progeny</i>	259
1.	<i>Katz v. United States</i>	259
2.	<i>Dow Chemical Co. v. United States</i>	260
3.	<i>Kyllo v. United States</i>	261
4.	<i>The Current Rule.....</i>	262
IV.	WHEN THE USE OF CONCEALED WEAPON DETECTION SYSTEMS IS CONSTITUTIONAL	263
A.	<i>Use of Weapon Detection Systems When There Is Probable Cause to Search.....</i>	264
B.	<i>Use of Weapon Detection Systems When There Is an Articulable Reasonable Suspicion the Suspect Is Engaged in a Crime of Violence or Is Armed.....</i>	266
1.	<i>Non-Terrorist Terry-Stop Situations</i>	266
2.	<i>Terry-Stops Where Terrorist Activity Is Alleged: An Automatic Terrorist Exception?.....</i>	268
C.	<i>Use of Weapon Detection Systems Without Probable Cause or Reasonable Suspicion</i>	271
1.	<i>Non-Administrative Searches: "Street Searches"</i>	271
2.	<i>Administrative Searches: Vehicle Checkpoints, Border Searches, Airports</i>	274

a. *Vehicle Checkpoints*.....274
 b. *Border Searches*275
 c. *Airports*.....275
 V. CONCLUSION276
 APPENDIX278

I. INTRODUCTION

“Change is good. Change is a necessary part of life. Change refreshes and challenges. We all welcome change. Like hell. Most of us hate change.”¹

Most of us hate change, yet even the most naïve recognize that changes regarding our civil liberties are inevitable following the terrorist attacks of September 11, 2001. Following the attacks of September 11th, news commentators throughout the United States were not inquiring into whether our civil liberties would be diminished, but rather, the ways the American public would have to barter civil liberties for safety. For example, an article published in *U.S. News and World Report* shortly after the attacks stated that “[b]efore September 11, government agencies and industry approached high-tech security devices warily, wondering whether the benefits outweighed the civil liberties and privacy concerns. Now the question they’re asking isn’t whether these devices should be used but how soon they can be in place.”² Another article in *U.S. News and World Report* stated that, following the attacks of September 11th, “[w]e all can expect to be scanned, probed, and sniffed by new devices at airports and in public buildings, gaining reassurance [of safety] at cost in dollars, convenience, and personal privacy.”³ An article published in *Business Week* shortly after the attacks reported,

Journalists, civil libertarians, and other professional alarmists cry “Big Brother” too frequently. But none of the privacy controversies of recent years – indeed, no event in modern history – has brought the prospect of Big Brother closer to reality than the World Trade Center horror. The thought that the same attackers might have access to biological weapons and other advanced technology forces us to reach for an equally powerful and futuristic arsenal with which to strike back. Suddenly, proposals are gaining legitimacy that were all but unmen-

¹ Roger Simon, *The New Normal*, U.S. NEWS AND WORLD REP., Nov. 12, 2001, at 14, 16.

² Dana Hawkins, *Guarding Liberties as Well as Lives*, U.S. NEWS AND WORLD REP., Oct. 8, 2001, at 56, 57.

³ Dana Hawkins & David LaGesse, *Tech vs. Terrorists*, U.S. NEWS AND WORLD REP., Oct. 8, 2001, at 56, 57.

tionable a month ago. Calls are being made for the establishment of databases of information about what citizens look like, where they go, and what they do; for the use of surveillance technology to monitor the nation's e-mail traffic; and for the imposition of a national identification card, to name a few. Many of these steps may well be necessary.⁴

An article in the *National Journal* reported that, after the events of September 11, “[p]rivacy will shrink. Boarding an airliner will be more like boarding El Al Israel: passenger-by-passenger interrogations; intrusive luggage and, sometimes, body searches; long delays; armed guards, armed sky marshals, maybe even armed flight attendants or pilots.”⁵ Regarding the effects of the September 11 attacks on the use of weapon scanning technology, a reporter for the *Evening Standard* noted that “[t]he fact that [QinetiQ’s thermal-imaging device, a weapon scanner currently employed as an alternative to a manual frisk in some airports,] strips its target so people appear almost naked has caused concern among civil rights watchers. But – with the events [of September 11th] in New York – such concerns may no longer seem so important.”⁶

Most of us hate change, but despite the unease associated with bartering civil liberties for safety, we must each, individually and collectively as citizens of the United States, consider the civil liberties we are willing to forego to live in a society where daily decisions are not dictated by terrorists abroad. As noted by Erwin Chemerinsky, “It is so important for the debate to get past the point where one side is saying, ‘We’ve got to give up civil liberties,’ and the other side is saying, ‘We cannot give up civil liberties . . .’ It has to be a much more nuanced discussion of what civil liberties are being compromised, under which circumstances, and for what gain.”⁷ Most of us hate change, yet change is coming, “[s]o amid vigilant new security and surveillance, we must work with consummate care to limit the damage to our freedoms.”⁸

With regard to civil liberties, many of the darkest moments in the history of the United States have fallen on the heels of military threats to American soil. Basic criminal rights were suspended for soldiers during the Civil War.⁹ During World War I, free expression was sharply curtailed by the Espionage

⁴ Mike France & Heather Green, *Security vs. Civil Liberties*, BUS. WK., Oct. 1, 2001, at 50, 50.

⁵ Stuart Taylor, Jr., *Thinking the Unthinkable: Next Time Could Be Much Worse*, 37 NAT’L J. 2801, 2805 (2001).

⁶ Peter Almond, *New Weapon Sees Through Terrorists*, EVENING STANDARD (London), Sept. 18, 2001, at 17.

⁷ France & Green, *supra* note 4, at 50.

⁸ Taylor, *supra* note 5, at 2806.

⁹ France & Green, *supra* note 4, at 50.

and Sedition Acts.¹⁰ Few blots on the history of the United States are as dark as that caused by the internment of Japanese Americans during World War II.¹¹ Dark moments can be justified if a dark today provides for a brighter tomorrow. However, there is little evidence that these dark moments did much to improve security within the United States.¹² Although news reports following the September 11th attacks are replete with references indicating the American people are prepared to accept reasonable reductions in civil liberties for concomitant gains in personal security, “we must combine pervasive surveillance with vigilant protection of privacy”¹³ All reductions in civil liberties must be justified by equal gains in personal security. The dark day of September 11th should not be made darker by unjustified reductions in civil liberties.

The fight against terrorism probably will be fought on many fronts, including changes in the enforcement of immigration laws, the enactment of new legislation expanding the wiretap capability of the federal government in terrorist investigations, and the development of biosensors capable of detecting biological weapons.¹⁴ However, one specific area where technological advancements have a manifest potential to increase personal security and reduce civil liberties is the development and deployment of sensory-enhancing electronic surveillance weapon detection devices; these newly created weapons scanners are the next generation of weapon detection technology.¹⁵

Weapon detection systems can be classified into one of four categories based on the level of resolution (i.e., the system’s ability to detect weapons and to discriminate weapons from other, non-contraband items) provided by the system and the level of the intrusiveness of the scan (i.e., the intimacy of details revealed about the person scanned). The four categories are derived from the dichotomous coupling of these two factors: low resolution, low intrusiveness (LRLI, e.g., security cameras); low resolution, high intrusiveness (“LRHI”; not

¹⁰ *Id.* at 51.

¹¹ *See id.*

¹² *See id.*

¹³ Taylor, *supra* note 5, at 2806.

¹⁴ *See, e.g.*, 8 U.S.C.S. § 1379 (2002) (requiring the “Attorney General and Secretary of State to . . . develop and certify a technology standard, including appropriate biometric identifier standards, that can be used to verify the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name.”); 8 U.S.C.S. § 1534 (2002) (noting that “an alien subject to removal under this title [8 U.S.C.S. §§ 1531 *et seq.*] shall not be entitled to suppress evidence [collected through electronic surveillance] that the alien alleges was unlawfully obtained.”); Charles W. Petit, *Catching a Whiff of Pestilence*, U.S. NEWS AND WORLD REP., Nov. 12, 2001, at 66 (discussing the deployment of “small, automated biosensor devices [in] . . . malls, airports, post offices, and subways” to detect toxins, virus and dangerous microbes in the air).

¹⁵ *See* Jason Lazarus, Note, *Vision Impossible? Imaging Devices—The New Police Technology and the Fourth Amendment*, 48 FLA. L. REV. 299 (1996).

developed);¹⁶ high resolution, low intrusiveness (“HRLI”; not developed, but, would be analogous with “canine sniff” drug detection systems);¹⁷ and high resolution, high intrusiveness (“HRHI”; e.g., BodySearch low dose X-ray imager, Millivision millimeter wave imager, and manual frisk).

In examining the evolution of weapon detection technology, Fox Butterfield noted that “new weapons detectors are expected to raise novel constitutional questions about police searches, and there are no exact precedents for the answers.”¹⁸ This note attempts to address some of these constitutional questions. Specifically, this note discusses the circumstances where it would be appropriate to employ weapons detection systems in three of these categories, the level of suspicion required by the security agency before use of each of these systems, and how the utility of each system broadens or narrows depending on circumstances, such as the location of the scan and the nature of the suspected criminal activity (e.g., drug trafficking vs. terrorism).

II. DEVELOPING AND CATEGORIZING CONCEALED WEAPON DETECTION SYSTEMS

A. *Concealed Weapon Detection Systems Currently Under Development*

Because of a perceived need to create new sources of revenue for defense technology companies following the end of the Cold War, beginning in the mid-1990’s, the federal government intensified federal funding of projects developing concealed weapon detection systems.¹⁹ The Department of Defense joined with the Department of Justice to transfer military technology used by the Department of Defense to the commercial market so that commercial products could be manufactured using this technology.²⁰ The goal was to make military technology available to local law enforcement agencies.

¹⁶ Systems in this category represent the “worst of both worlds.” They provide little information and are highly intrusive. Because low resolution, minimally intrusive systems and high resolution, moderately intrusive systems are available, no further consideration is given to weapon detection systems in this category.

¹⁷ A weapon detection system in this category would be analogous to a canine sniff search for narcotics. Raytheon Corporation’s electromagnetic pulse weapon detection systems detect only metallic weapons with recognized magnetic signatures. Despite these limits in their resolution, electromagnetic pulse weapon detection systems offer a relatively high level of resolution with minimal intrusiveness. Raytheon’s electromagnetic pulse weapon detection systems demonstrate the attributes of future weapon detection systems in this category. See Erik Milstone, *New Devices Let Frisks Go Undercover*, 82 A.B.A. J. 32; Fox Butterfield, *Justice Dept. Awarding Grants to Develop Gun Detectors*, N.Y. TIMES, Mar. 10, 1995, at C1.

¹⁸ Fox Butterfield, *New Devices May Let Police Spot People on the Street Hiding Guns*, N.Y. TIMES, Apr. 7, 1997, at A1.

¹⁹ Laura B. Riley, Comment, *Concealed Weapon Detectors and the Fourth Amendment: The Constitutionality of Remote Sense-Enhanced Searches*, 45 UCLA L. REV. 281, 285 (1997).

²⁰ *Id.*

In 1993, Janet Reno formally launched the transfer of military technology to law enforcement when she asked the Secretary of Defense to “assist the Department of Justice in ‘identifying and transferring military technologies useful to law enforcement.’”²¹ The Law Enforcement Technology Advisory Council noted that its top priority was the development of three concealed weapon detection systems including “one capable of being placed unobtrusively in school entrances; One [sic] capable of being mounted in and operated from a vehicle; and a handheld or portable version”²² Based on recommendations from the Law Enforcement Technology Advisory Council, the National Institute of Justice began awarding research grants to organizations and companies historically involved in defense development including “Raytheon Corporation of Portsmouth, Rhode Island, Millimetrix Corporation of Hadley, Massachusetts, and Idaho National Engineering Laboratory, a branch of the Department of Energy.”²³

Weapon detection systems currently under development include passive millimeter wave cameras, electromagnetic portals employing fluxgate magnetometers, tetahertz-wave weapons imagers, wide-band radar weapons detectors, combined millimeter wave/infrared cameras, and acoustic concealed weapon detectors.²⁴ An overview of current concealed weapon detection development supported by the United States Department of Justice can be viewed on the National Law Enforcement and Corrections Technology Center website.²⁵

B. *Categorizing Weapon Detection Systems*

Many law review articles address the intrusion of specific weapon detection systems on reasonable expectations of privacy.²⁶ Following the development of, or litigation over, the use of each new police surveillance technology, a plethora of legal diatribes have been published consisting of post hoc analyses of the intrusiveness of the newly developed surveillance technology and the resulting benefits in crime reduction or increased personal security. For

²¹ *Id.*

²² *Law Enforcement Technology, 1995: Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 104th Cong. 30 (1995) (statement of David G. Boyd, Director, Science & Technology Division of the National Institute of Justice); David C. Morrison, *Crime-Fighting 2001*, 26 GOV'T EXECUTIVE 42, 43 (1994).

²³ Riley, *supra* note 19, at 286.

²⁴ See The National Law Enforcement and Corrections Technology Center's Website, <http://www.nlect.org/> for more information about these weapon detection systems.

²⁵ The National Law Enforcement and Corrections Technology Center is a program within the United States Department of Justice. The address for the developing technology section of the National Law Enforcement and Corrections Technology Center's website is <http://www.nlect.org/techproj/>.

²⁶ See, e.g., Lazarus, *supra* note 15; Riley, *supra* note 19.

example, post hoc analyses of specific surveillance technologies have followed the development of wire taps,²⁷ electronic bugging devices,²⁸ spike mikes,²⁹ canine “sniffs,”³⁰ high resolution aerial photography,³¹ and forward-looking infrared radar.³² Because of standing requirements, courts may analyze the use of these systems only on a post hoc basis where a case or controversy exists.³³

Many weapon detection systems currently under development may not pass constitutional muster if used in ways currently intended. Resources should be diverted away from the development of weapon detection systems that, based on case precedent, will likely be adjudged to violate the Fourth Amendment.

The development of weapon detection systems should be guided by categorizing developmental and hypothetical systems based on each system’s intrusiveness and resolution. Weapon detection systems can be placed in one of four categories based on the dichotomous coupling of intrusiveness and resolution: LRLI, HRLI, LRHI, and HRHI.³⁴ The usefulness and the constitutionally permissible uses of detection systems can be broadly defined for each category. For example, no probable cause would be required to use weapon detection systems in the high resolution, low intrusiveness (not developed) or the low resolution, low intrusiveness (e.g., security cameras) categories.³⁵ However, although use of systems in both categories would be constitutionally permissible without probable cause,³⁶ HRLI systems would be more useful than systems in the latter category. In addition, although systems in the HRHI and the HRLI categories would be equally capable of detecting contraband, probable cause would be necessary only for the use of HI systems.

We can achieve three goals through categorizing detection systems based on resolution and intrusiveness. First, through categorizing detection systems, we can determine the specific circumstances under which each developmental system could be employed, as well as the level of suspicion needed to use detectors in each category. Second, categorizing detection systems allows

²⁷ *Olmstead v. United States*, 277 U.S. 438 (1928).

²⁸ *Goldman v. United States*, 316 U.S. 129 (1942).

²⁹ *Silverman v. United States*, 365 U.S. 505 (1961).

³⁰ *United States v. Place*, 462 U.S. 696 (1983).

³¹ *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986).

³² *United States v. Cusumano*, 67 F.3d 1497 (10th Cir. 1995), *vacated*, 83 F.3d 1247 (10th Cir. 1996) (en banc).

³³ *See* U.S. CONST. art. III, § 2; *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992).

³⁴ *See* Part I.; *supra* notes 16-17 and accompanying text.

³⁵ A HRLI weapon detection system would be analogous to a “canine sniff.” Like a “canine sniff,” the weapon detection system would only detect the presence of contraband (i.e., illegal weapons). Because HRLI systems would alert police only to the presence of contraband, use of the system would not invade constitutionally protected privacy interests.

³⁶ *See infra* notes 40-41 and accompanying text.

developers to determine the value or usefulness of each detection system in its constitutionally permissible roles. Most importantly, categorizing weapon detection systems based on intrusiveness and resolution allows for proactive analyses of the utility and constitutionality of hypothetical, undeveloped detection systems. Consideration of hypothetical detection systems can direct the development of less intrusive, higher resolution detection systems. In addition, consideration of the weapon detection systems in terms of resolution, which is directly related to the usefulness of the system in increasing personal security, and intrusiveness, which is directly related to how far the system evades our privacy rights, places the “give and take” nature associated with increasing personal security while protecting civil liberties in a more acute perspective.

We must assume that the reason HRLI weapon detection systems have not been developed is because the technology necessary to develop these systems does not currently exist. The events of September 11th suggest an immediate need for improved security. In toppling the World Trade Center Towers and ripping through the Pentagon, the attacks of September 11th destroyed more than buildings and crushed more than life; the attacks forever altered the pre-September 11th balance struck between personal security and civil liberties. Because non-intrusive weapon detectors capable of detecting plastic knives and other weapons used by terrorist in the September 11th do not exist, the courts and American people face the onerous task of re-balancing our immediate need for increased personal security and the privacy we are willing to exchange for this security.

C. *Illustrating the Effect of Resolution and Intrusion on Classifying Surveillance Technology*

The United States Supreme Court’s analysis in *Place* illustrates two important factors to be considered when classifying police surveillance technology: the intrusiveness and resolution of the search.³⁷ Although *Place* involved police surveillance for narcotics, not weapons, the holding of the case indicates the most important factors to consider when determining the reasonableness of a police surveillance method.³⁸

Although intrusiveness and resolution are related, analysis of both is necessary when evaluating the utility and danger imposed by a weapon scanner. In *Place*, the police, responding to a tip that Place might be involved in drug trafficking, stopped him in an airport. The police subjected Place’s luggage to a sniff search by a drug-sniffing dog. After the dog reacted positively to the lug-

³⁷ 462 U.S. 696 (1983).

³⁸ *Id.* at 705-07 (noting that “[t]he intrusion on possessory interests occasioned by a seizure of one’s personal effects can vary both in its nature and extent,” and holding that “the canine sniff is *sui generis*” because it is “so limited both in the *manner in which the information is obtained* and in the *content* of the information revealed”) (emphasis added).

gage, the police conducted a full search of it and discovered cocaine.³⁹ Because scanning Place's luggage with the canine nose did not require opening the luggage or viewing its contents, and because the scan alerted the police to the detection of only contraband, the level of the intrusiveness of the scan was low. In addition to being minimally intrusive, because the scan had a high probability of detecting drugs if drugs were present, and because the scan detected the presence of only contraband, the resolution of the scan was high. Because the "canine sniff" is minimally intrusive and only detects the presence of illegal contraband, the Court held that this type of scan was not a search under the Fourth Amendment.⁴⁰

The Court's holding in *Place* illustrates, through analogy, that future detection systems will pass constitutional muster for use in almost unlimited circumstances so long as the detection system only detects the presence of contraband.⁴¹ Weapon scanners with the properties of the canine sniff do not currently exist. Because of our need for improved weapon detection systems following the terrorist attacks of September 11th, we must consider the intrusiveness and resolution of existing and developmental weapon scanners, and the circumstances under which these systems may currently be employed.

III. THE EVOLUTION OF FOURTH AMENDMENT SEARCH AND SEIZURE DOCTRINE

A. *The Birth of the Fourth Amendment*

John Adams, in discussing the fervor surrounding the American Revolution, noted that the "child Independence" was born out of concern over writs of assistance and the unlimited authority these writs gave English soldiers to enter American homes and businesses to search for smuggled goods.⁴² One of the primary catalysts for the American Revolution was the use, by English soldiers, of general warrants to search homes without a prior showing of probable cause or reasonable suspicion.⁴³ With this oppression fresh in the minds of the drafters of the U.S. Constitution, the Fourth Amendment was written "to prevent the use of governmental force to search a man's house, his person, his papers, and his effects; and to prevent their seizure against his will."⁴⁴ The Fourth Amend-

³⁹ *Id.* at 698-99.

⁴⁰ *Id.* at 707.

⁴¹ *See id.*; *see also* *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (Stevens, J., dissenting) (noting that "sense-enhancing equipment that identifies nothing but illegal activity is not a search").

⁴² *Boyd v. United States*, 116 U.S. 616, 625 (1886).

⁴³ *See* *Olmstead v. United States*, 277 U.S. 438, 463 (1928); *see also* Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361, 362-63 (1920).

⁴⁴ *Olmstead*, 277 U.S. at 463.

ment provides 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.”⁴⁵ The language of the Fourth Amendment does not prohibit all searches – “only unreasonable searches and seizures . . . are forbidden.”⁴⁶ The text of the Fourth Amendment does not define what constitutes a search and what makes a search reasonable. The power of the Fourth Amendment hangs on the definition of “search” and “reasonable.” Courts continue to struggle with the definition of these two terms, and their meanings are ever evolving.

B. *Pre-Katz Property Based Approach*

Early jurisprudence utilized a property-based approach when analyzing Fourth Amendment search issues. Under this trespass doctrine, the Fourth Amendment was not violated unless there had been a warrantless search of a person’s “tangible material effects, or an actual physical invasion of his house ‘or curtilage.’”⁴⁷ In *Olmstead v. United States*, the Court noted that the Fourth Amendment only applied to “material things” or physical invasion of the home.⁴⁸ Because of the primitive nature of police surveillance technology prior to the twentieth century, this narrow interpretation of the Fourth Amendment was sufficient to shield citizens from most unwarranted governmental searches. However, by the mid-1900’s, courts were beginning to comment on potential conflicts between technological advancements in police surveillance and this narrow interpretation of the Fourth Amendment.⁴⁹ Use of the property-based trespass doctrine to analyze Fourth Amendment search issues permitted the police to use wiretaps⁵⁰ or electronic bugs⁵¹ without probable cause. The Court in *Berger v. New York*⁵² noted that Fourth Amendment jurisprudence was not keeping “pace with . . . advances in scientific knowledge.”⁵³

⁴⁵ U.S. CONST. amend. IV.

⁴⁶ *Boyd*, 116 U.S. at 641 (Miller, J., concurring).

⁴⁷ *Olmstead*, 277 U.S. at 466.

⁴⁸ *Id.* at 464.

⁴⁹ *Berger v. New York*, 388 U.S. 41 (1967).

⁵⁰ *Olmstead*, 277 U.S. at 466.

⁵¹ *Goldman v. United States*, 316 U.S. 129 (1942).

⁵² 388 U.S. 41 (1967).

⁵³ *Id.* at 49.

C. *The Impact of Katz and Katz Progeny*

1. *Katz v. United States*

The era of using a property-based approach in analyzing Fourth Amendment search issues came to a close with the Court's decision in *Katz v. United States*.⁵⁴ The Federal Bureau of Investigation ("FBI") suspected that Katz was using a public phone booth to conduct illegal wagering activity. The FBI attached an electronic listening device to the outside of a phone booth to monitor the content of calls Katz made from the booth. Even though the phone booth was a public area and the thing searched (i.e., the content of Katz' phone conversations) was not a tangible material effect, the Court held that monitoring phone conversations was a search.⁵⁵ In broadening its definition of search, the Court expressly overruled *Olmstead* and *Goldman v. United States*⁵⁶ with respect to their reliance on the property-based trespass doctrine. The rule that emanated from *Katz* is that the Fourth Amendment protects privacy interests, even outside the home, so long as the privacy interest passes a two-part test.⁵⁷ The first prong of the two-part test is the subjective prong; the person searched must exhibit an actual expectation of privacy.⁵⁸ The second, objective prong requires that the expectation of privacy be one society is willing to recognize as reasonable.⁵⁹ In applying this two-part test, Justice Harlan, in a concurring opinion, noted that Katz exhibited a subjective expectation of privacy when he entered the phone booth and shut the door behind him before placing his call and that "expectations of freedom from intrusion [when placing calls from phone booths] are recognized as reasonable."⁶⁰ Because the Court found that Katz exhibited a subjective expectation of privacy when placing his call from the phone booth and that his expectation of privacy was one the public recognized as reasonable, the Court held that monitoring the phone call was a search under the Fourth Amendment.⁶¹ *Katz* marked the supplanting of the trespass doctrine with the two-prong, subjective expectation/objective reasonableness test for analyzing issues involving searches and the Fourth Amendment.

⁵⁴ 389 U.S. 347 (1967).

⁵⁵ *Id.* at 353.

⁵⁶ 316 U.S. 129 (1942).

⁵⁷ *Katz*, 389 U.S. 347 (Harlan, J., concurring) (articulating two-part test).

⁵⁸ *Id.* at 361 (Harlan, J., concurring).

⁵⁹ *Id.*

⁶⁰ *Id.* (Harlan, J., concurring).

⁶¹ *Id.*

2. *Dow Chemical Co. v. United States*

In its holding in *Dow Chemical Co. v. United States*,⁶² the Court added an additional factor, “intimate details,” to be considered when determining what sorts of activities constitute a search. The Court’s holding in *Dow* suggests that as the intimacy of details revealed by the scan increases, the Court is more likely to hold that the expectation of privacy is one society considers reasonable.⁶³ The holding in *Dow* indicates the Court would consider use of high-resolution weapon detection systems currently available (e.g., passive millimeter wave and low-dose X-ray imagers) a search under the Fourth Amendment.

In *Dow*, the Environmental Protection Agency (“EPA”) took aerial photographs of a Dow chemical plant. Dow sought to have evidence revealed in the photographs excluded from trial because it alleged the aerial photography constituted an illegal search. The Court disagreed and held that because the EPA used a “conventional . . . commercial camera” rather than “some unique sensory device that . . . could penetrate . . . walls,” the aerial photography did not constitute a constitutionally proscribed search.⁶⁴

In determining if the aerial photography constituted an impermissible search, the Court looked at two factors: the availability of the surveillance equipment to the general public and the intimacy of the details revealed by the search.⁶⁵ Because the technology used in high-resolution weapon detectors (e.g., passive millimeter or low-dose X-ray imaging) is not available to the general public, the Court is more likely to find that the use of these systems constitutes a search.⁶⁶ In addition, the intimacy of detail revealed by high-resolution weapon detectors such as the BodySearch low dose X-ray imager and Millivision millimeter wave imager indicates the Court would find that a person’s expectation of privacy in the details revealed by these scans is reasonable and, therefore, that use of these systems constitutes a search under the *Katz* test.

⁶² 476 U.S. 227, 238 (1986).

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.* at 237-38.

⁶⁶ It is possible to “see through a person’s clothing with such accuracy that it can scan someone standing on the street and detect the diameter of a woman’s nipples, or whether a man has been circumcised.” Judy Jones, *Look Ahead to the Year 2000: Electronic Arm Of The Law Is Getting More High-Tech*, COURIER-J. (Louisville, KY), Oct. 19, 1999, available at LEXIS, News Library, COUJNL File. “Imaging devices might be capable of viewing extremely personal items such as a prosthetic limb, a woman’s sanitary napkin, a colostomy bag, or more unusual items.” Lazarus, *supra* note 15, at 311.

3. *Kyllo v. United States*

Many weapon detection systems currently in use or being developed rely on monitoring the amount and spatial patterns of radiation emitted from a person's body.⁶⁷ In *Kyllo v. United States*,⁶⁸ the government further argued that because its use of a thermal imaging device only detected "waste heat" emitted from the suspect's home and did not reveal intimate details about activities within the house, use of the thermal imager was not a search. The government argued that, like garbage left on the curb,⁶⁹ a person could not have a reasonable expectation of privacy in heat vented from the home. Because many weapon detection systems currently in development rely on monitoring "waste radiation" emitted from the suspect's body, an analogous argument could be made that because people do not have a reasonable expectation of privacy in "waste radiation" emitted from their body, use of scanning technology that monitors the amount and spatial patterns of radiation emitted from a body does not constitute a search. The Court's holding in *Kyllo* suggests this argument would fail.

In *Kyllo*, government agents used an Agema Thermovision 210 thermal imager to monitor the amount of infrared radiation emitted from one unit of a triplex where police suspected the tenant was using high-intensity lamps to grow marijuana.⁷⁰ The types of halide lamps used to grow marijuana indoors produce large amounts of heat that either escapes or is intentionally vented outside the home. When an object is scanned with a thermal imager, the relative levels of heat emitted from different portions of the object can be detected from the different shades of white, gray, and black produced on the scanner screen; white objects are hot, black are cool, and gray represents a temperature gradient between the two extremes.⁷¹ The type of thermal scanner employed in *Kyllo* detected only heat emitted from the triplex and did not reveal intimate details of activities taking place within the home.⁷² However, the Court held that "obtain-

⁶⁷ "All objects with temperatures above absolute zero naturally emit a broad spectrum of electromagnetic radiation, the details of which are determined by the material and the surface properties of the object, as characterized by its emissivity, and by its temperature. The apparent brightness of the object as viewed by a passive millimeter wave imager is a product of its physical temperature times its emissivity. A person at millimeter wavelengths is an especially good emitter. Metal objects are very poor emitters. Dielectric objects, such as plastics, ceramics, plastic explosives, powdered drugs, etc., have emission properties that are in between flesh and metals. Clothing is virtually transparent." *Reducing Gun Violence, 1994: Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 104th Cong. 1 (1994) [hereinafter *Gun Violence Hearings*] (statement of G. Richard Huguenin, President, Millitech [now Millimetrix] corporation), available at LEXIS, Legis Library, Cngtst File.

⁶⁸ 533 U.S. 27 (2001).

⁶⁹ *California v. Greenwood*, 486 U.S. 35 (1988).

⁷⁰ *Kyllo*, 533 U.S. at 29.

⁷¹ *Id.* at 29-30.

⁷² The thermal imager used in *Kyllo* "did not expose any intimate details of *Kyllo's* life," only

ing by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search"⁷³

The Court probably will use the same analytical framework used in *Kyllo* when analyzing the circumstances under which weapon detection systems that detect the presence of weapons by monitoring "waste emissions" produced by the body can be employed. The "waste radiation" and "waste sonic vibration" arguments with regard to weapons detectors are analogous to the "waste heat" argument made in *Kyllo*, which the Court made clear could not be reconciled with the holding in *Katz*.⁷⁴ Because the "waste emissions" detected by passive millimeter weapon detectors are so closely analogous to the "waste heat" monitored in *Kyllo*, and because people have similar reasonable expectations of privacy in their home and the intimate details of their bodies, it is unlikely the Court would find the "waste radiation" argument persuasive. In addition, unlike the thermal scanner employed in *Kyllo*, weapon detectors such as passive millimeter wave cameras reveal private, intimate details about the individual scanned.⁷⁵ In *Dow*, the Court noted that the intimacy of the details revealed is a factor to consider when determining if the use of the technology constitutes a permissible search.⁷⁶

The *Kyllo* Court indicated that one factor it relied on in determining that the thermal scan was a search was the *potential* for the sense-enhancing technology to reveal intimate details.⁷⁷ Because of the intimate details revealed by weapon detectors relying on "waste radiation" to produce an image of objects hidden beneath a person's clothing, and because the waste-energy argument has not previously prevailed, the Court will likely determine that the use of weapon detectors that rely on monitoring "waste radiation" constitutes a search under the Fourth Amendment.

4. The Current Rule

Despite the *Kyllo* decision, the holding in *Katz* remains the applicable rule regarding what constitutes a search under the Fourth Amendment. The *Katz* progeny helps illustrate factors the Court considers when determining (1) if

"amorphous 'hot spots' on the roof and exterior wall." *United States v. Kyllo*, 190 F.3d 1041, 1047 (9th Cir. 1999). *But see Kyllo*, 533 U.S. at 37 ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

⁷³ *Kyllo*, 533 U.S. at 28

⁷⁴ *See id.* at 34-36.

⁷⁵ *See supra* note 65.

⁷⁶ *Dow Chem. Co.*, 476 U.S. at 237-38.

⁷⁷ *Kyllo*, 533 U.S. at 38.

the person searched exhibited an actual expectation of privacy, and (2) if this expectation of privacy was one society was prepared to consider reasonable.⁷⁸

The Court in *Dow* did not address the “intimacy of detail revealed” and “availability of technology used” in terms of gradients. However, the holding in *Dow* suggests that as the intimacy of the detail revealed increases, and the availability of the technology used decreases, the Court is more likely to determine that the person has a reasonable expectation of privacy in the thing searched.

The Court’s holding in *Kyllo* helps fill gaps in the *Katz* rule. If a person voluntarily vents waste energy from her home, she has no subjective expectation of privacy in her waste heat.⁷⁹ However, if the sensory-enhancing technology provides information about activities occurring inside the home that could not otherwise have been obtained without physically entering the home, use of the technology constitutes a search.⁸⁰

Although the holdings of *Katz*, *Dow*, and *Kyllo* indicate that the use of all high-resolution weapon detection systems currently available constitutes a search, the Fourth Amendment does not bar all searches; only unreasonable searches are constitutionally prohibited. Issues courts are likely to face in the near future include (1) the circumstances under which the use of weapon detection systems is permissible, (2) if the events of September 11, 2001 changed the expectations of privacy society is willing to consider reasonable, and if so, (3) under what circumstances is society willing to permit the government to use weapon scanners without probable cause.

IV. WHEN THE USE OF CONCEALED WEAPON DETECTION SYSTEMS IS CONSTITUTIONAL

The constitutionality of the use of concealed weapon-detector systems depends on the circumstances under which each system is employed.⁸¹ Weapon detectors could be employed in numerous circumstances including (1) situations where the police have probable cause to search a suspect and use a weapons scanner in place of a manual frisk, (2) *Terry*-stop situations where the police have a reasonable articulable suspicion that the suspect is armed and dangerous and use a weapons scanner in place of a *Terry*-style patdown, and (3) in administrative-search situations, such as at airports and court houses, where the weapons scanner is used in place of magnetometers.

A potential fourth category would include the use of weapons detectors in non-administrative situations where police do not have probable cause to search and do not have a reasonable articulable suspicion that the subject is armed and dangerous. However, use of weapon scanners in these situations

⁷⁸ *Katz v. United States*, 389 U.S. 347 (1967).

⁷⁹ *Kyllo*, 533 U.S. at 27

⁸⁰ *Id.*

⁸¹ *Riley*, *supra* note 19, at 281.

would be constitutional only if scanning a subject with the scanner did not constitute a search under the Fourth Amendment. Although manufacturers of some weapon detectors suggest the detectors could be configured to work in a binary fashion (i.e., where they detected only contraband), this technology is not currently available.⁸² The Court most likely will find that use of all high-resolution systems currently available constitutes a search and will not permit the unrestricted use of these detectors.

A. *Use of Weapon Detection Systems When There Is Probable Cause to Search*

Although the Court has noted that “the police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure,” it has also held that “on-the-spot observations of the officer on the beat . . . historically has not been, and as a practical matter could not be, subjected to the warrant procedure.”⁸³ So long as it was not practicable to obtain a warrant prior to a search, courts commonly uphold warrantless manual frisks conducted by police officers who have probable cause to believe a crime has been committed and the person searched committed it.⁸⁴

Although courts commonly uphold warrantless manual frisks, the Supreme Court has noted that a manual frisk “is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly.”⁸⁵ A manual frisk often involves feeling “with sensitive fingers every portion of the prisoner’s body” and thoroughly searching the person’s “arms and armpits, waistline and back, the groin and area about the testicles, and entire surface of the legs down to the feet.”⁸⁶

Use of a highly-intrusive high-resolution weapons detector, like a passive millimeter scanner, should be permissible under circumstances where a manual frisk ordinarily would be used.⁸⁷ However, the indignity suffered by a

⁸² “[P]assive millimeter wave imagers do literally see through clothing In order to protect a person’s right to privacy, the actual image of the person being observed need only be displayed to an 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. A person with no suspicious object(s) could be cleared automatically with no operator intervention and without an image being displayed.” *Gun Violence Hearings*, *supra* note 67, at 1 (statement of G. Richard Huguenin, President, Millitech [now Millimetrix] corporation).

⁸³ *Terry v. Ohio*, 392 U.S. 1, 20 (1968).

⁸⁴ See, e.g., *United States v. Scott*, 270 F.3d 30, 40 (1st Cir. 2001); *United States v. Bayless*, 201 F.3d 116, 132 (2d Cir. 2000); *Laveto v. Lapina*, 258 F.3d 1156, 1164 (3d Cir. 2001); *United States v. Hopkins*, 268 F.3d 222, 225-26 (4th Cir. 2001).

⁸⁵ *Terry*, 392 U.S. at 17.

⁸⁶ L. L. Priar & T. F. Martin, *Searching and Disarming Criminals*, 45 J. CRIM. L.C. & P.S. 481 (1954).

⁸⁷ Low-dose X-ray images capable of detecting objects beneath people’s clothing are already

suspect scanned with a high-resolution weapon detector is comparable to, or less than, the indignity wrought by a manual frisk.⁸⁸ The indignity suffered by a suspect from having government agents view an image on which the outline of his scrotal area can be seen is no greater than the indignity suffered when the government agent has to “feel with sensitive fingers . . . the groin and area about the testicles.”⁸⁹

Where probable cause to search a suspect exists, electronic frisks via weapon detectors offer two advantages over manual frisks. As noted by Jeremy Travis, past director of the National Institute of Justice, “of the situation[s] cops face day in and day out, the greatest risk is approaching a subject who may be armed.”⁹⁰ The safety of the officer is greatly increased if the officer “know[s] in advance whether the individual is armed.”⁹¹ In addition to concerns regarding whether the suspect is armed, police face other risks, such as “the danger of being punctured by a hypodermic needle during a manual ‘patdown.’”⁹² One advantage of electronic frisks over manual patdowns is that electronic frisks allow police to determine if a suspect is armed before approaching or making contact with the individual. In addition, electronic frisks alert police to hidden dangers such as hypodermic needles hidden in the suspect’s hair or clothing so that these items can be removed if it is necessary to take the suspect into custody.

Another advantage of electronic frisks is that they can be conducted under less conspicuous circumstances than manual frisks. Manual frisks commonly involve having the suspect “stand[] helpless, perhaps facing a wall with his hands raised.”⁹³ As noted by the *Terry* Court, “it is simply fantastic” to argue that a manual frisk conducted under such circumstances is a “petty indignity.”⁹⁴ Although police presence would be obvious to bystanders during an electronic frisk, the suspect would not be forced to stand “spread eagle” against a wall with his hands on his head during the procedure and neither the suspect nor the police would have to suffer the dehumanizing humiliation associated

being used in place of manual frisks in some U.S. airports. Hawkins & LaGesse, *supra* note 3, at 56. “The BodySearch technology has already performed electronic strip-searches on nearly 800 international passengers arriving at eight U.S. airports in cities including New York and Washington. Customs inspectors let travelers deemed ‘suspicious’ choose between the scan and a pat down.” *Id.*

⁸⁸ See *supra* note 82 and accompanying text.

⁸⁹ Priar & Martin, *supra* note 86, at 481.

⁹⁰ Butterfield, *supra* note 18, at A1.

⁹¹ *Id.*

⁹² Max Glaskin, *Detector Frisks from a Distance*, SUNDAY TIMES, Feb. 26, 1995, at Features.

⁹³ *Terry*, 392 U.S. at 17.

⁹⁴ *Id.* at 16-17.

with having a government agent “feel with sensitive fingers every portion of the [suspect’s] body.”⁹⁵

The use of weapon detection systems could prove beneficial, both to suspects and to police officers, in circumstances where manual frisks traditionally would be employed. Because electronic frisks subject suspects to no greater intrusion than manual frisks, reduce risks in one of the most dangerous situations faced by police officers, and may reduce the indignity suffered by suspects subjected to manual frisks in public surroundings, the Court probably would permit the use of high-resolution weapon detectors in circumstances where police have probable cause to search a suspect.

B. Use of Weapon Detection Systems When There Is an Articulable Reasonable Suspicion the Suspect Is Engaged in a Crime of Violence or Is Armed

1. Non-Terrorist Terry-Stop Situations

The Fourth Amendment is not a “monolith.”⁹⁶ Since the Court’s holding in *Camara v. Municipal Court*,⁹⁷ it is clear that there are degrees of searches and that the meaning of “probable cause” depends on the context of the search. The *Camara* decision introduced a balancing approach to the Fourth Amendment. Because the *Camara* Court defined probable cause in terms of “reasonableness,” the *Camara* holding allowed certain types of searches on the basis of less than probable cause.⁹⁸

Following on the heels of *Camara*, the Court established a new category of “seizures” and “searches” in *Terry v. Ohio*.⁹⁹ In *Terry*, the Court held that a police officer may briefly detain an individual “for purposes of investigating possibly criminal behavior even though there is no probable cause to make an arrest” so long as the officer has an articulable reasonable suspicion that the individual is involved in criminal enterprise.¹⁰⁰ Based on the “reasonableness test” established in *Camara*, the Court held that it was reasonable for police to briefly detain an individual and engage in something less than a complete seizure based on suspicion that was less than “probable cause.”¹⁰¹ The Court also

⁹⁵ Priar & Martin, *supra* note 86, at 481.

⁹⁶ Anthony G. Amsterdam, *Perspectives On the Fourth Amendment*, 58 MINN. L. REV. 349, 388 (1974).

⁹⁷ 387 U.S. 523 (1967); JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE 138 (2000).

⁹⁸ DRESSLER, *supra* note 97, at 139.

⁹⁹ 392 U.S. 1 (1968).

¹⁰⁰ *Id.* at 22.

¹⁰¹ *Id.* at 21-22, 27.

held that if the officer had an articulable reasonable suspicion that the individual “presented a threat to the officer’s safety while he was investigating his suspicious behavior,” he could engage in a search of the suspect “limited to that which was necessary for the discovery of weapons which might be used to harm the officer or others nearby.”¹⁰² During this search the officer may patdown the outer clothing of the individual and may seize only items whose criminal nature is apparent.¹⁰³ This limited detention and limited search were later termed *Terry-stop* and *Terry-frisk*, respectively.

Terry-stops and *Terry-frisks* protect police officers during one of the most dangerous situations they face.¹⁰⁴ The dangers faced by police officers in *Terry-stop* situations often are as great as those where officers have probable cause to search a suspect. It is clear that electronic frisks offer the same advantages in *Terry-stop* situations as in searches where officers have probable cause to search or searches incident to arrest.

Although electronic frisks offer the same benefits to police in *Terry-stop* situations as they do in searches where officers have probable cause to search, the Court is unlikely to permit police to use highly intrusive high-resolution weapon detectors as a substitute for *Terry-frisks*. Unlike manual frisks, *Terry-frisks* are restricted to a light pat down of the suspect’s outer clothing. The intrusiveness of being scanned by a weapons detector such as the Millivision passive wave imager would be much greater than the intrusiveness associated with a *Terry frisk*.

In addition, a *Terry-frisk* is conducted for the purpose of finding weapons the suspect may use to harm the officer or others in the area; a *Terry-frisk* should not be used for the purpose of detecting contraband.¹⁰⁵ During a *Terry-frisk*, the officer is allowed to confiscate contraband other than weapons (e.g., drugs) only if the criminal nature of the item is apparent during the light pat-down of the suspect’s outer clothing.¹⁰⁶ Because contraband other than weapons also may be detected with most highly intrusive high-resolution weapon detectors, use of these systems during a *Terry-stop* would allow the police to detect items that a typical *Terry-frisk* would not discover.¹⁰⁷ Police officers would face

¹⁰² *Id.*

¹⁰³ *See id.* at 29.

¹⁰⁴ Butterfield, *supra* note 18, at A1.

¹⁰⁵ *Terry*, 392 U.S. at 26. The limited pat down “must be limited to that which is necessary for the discovery of weapons which might be used to harm the officer or others nearby.” *Id.* “The sole justification of the search in the present situation is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer.” *Id.* at 29.

¹⁰⁶ This is the “plain-feel” exception. *See Minnesota v. Dickerson*, 508 U.S. 366 (1993).

¹⁰⁷ Contraband detectable with passive millimeter wave imaging includes “[d]ry powders and/or liquids in plastic bags, vials, or other containers . . . in centimeter or larger sized packages.”

much greater temptation to manufacture articulable reasonable suspicion that a suspect was armed and dangerous if the police knew that they then could scan the suspect with a system that would alert them to the presence of contraband possessed by the suspect. The use of high-resolution weapon detectors in these circumstances would likely lead to an increase in the number of pretextual searches conducted by police.

Because high-resolution weapon detectors are more intrusive than *Terry*-frisks, allowing their use in *Terry*-stop situations would expose suspects to a greater than reasonable intrusion based only on an articulable reasonable suspicion. In addition, because use of weapon detectors in *Terry*-stops would likely lead to “fishing expeditions,” permitting police to use weapon detectors in *Terry*-stops probably would result in an increase in the number of people subjected to *Terry*-frisks.

2. *Terry*-Stops Where Terrorist Activity Is Alleged: An Automatic Terrorist Exception?

In *Florida v. J.L.*,¹⁰⁸ the Court considered whether bald and unilluminating assertions from an anonymous caller that an individual was unlawfully carrying a concealed weapon justified a *Terry*-stop and frisk. Typically, uncorroborated anonymous tips do not justify a *Terry*-frisk. In *J.L.*, the government argued for an automatic firearm exception. Under this exception, the police could stop and frisk someone under the *Terry* rule, based on an uncorroborated anonymous tip, if the informant suggested that the individual was illegally possessing a concealed firearm. In refusing to create an “automatic firearm exception” the court noted that “[f]irearms are dangerous, and extraordinary dangers sometimes justify unusual precautions,” however, the Court held that “an automatic firearm exception to [the] established reliability analysis would rove too far.”¹⁰⁹ The Court suggested that creating “[s]uch an exception would enable any person seeking to harass another to set in motion an intrusive, embarrassing police search of the targeted person simply by placing an anonymous call falsely reporting the target’s unlawful carriage of a gun.”¹¹⁰ However, the Court went on to state:

The facts of this case do not require us to speculate about the circumstances under which the danger alleged in an anonymous tip might be so great as to justify a search even without a showing of reliability. *We do not say, for example, that a report of a*

Gun Violence Hearings, *supra* note 67, at 1 (statement of G. Richard Huguenin, President, Millitech [now Millimetrix] corporation).

¹⁰⁸ 529 U.S. 266 (2000).

¹⁰⁹ *Id.* at 272.

¹¹⁰ *Id.*

*person carrying a bomb need bear the indicia of reliability we demand for a report of a person carrying a firearm before the police can constitutionally conduct a frisk.*¹¹¹

With these words, the Court in *J.L.* made it clear that while the level of intrusiveness of a search should be commensurate with the reliability of the information indicating the individual was involved in criminal enterprise, the level of suspicion required would be lower, and the required reliability of the information leading to that suspicion would decrease, as the extraordinary nature of the danger threatened increased. The Court's specific reference to bombs left its path open to create an "automatic terrorist exception."

An automatic terrorist exception could be improperly used to the same disastrous ends as an automatic firearm exception. However, because the ramifications of allowing terrorist activity to go unfettered so greatly outweighs the dangers of allowing an individual to unlawfully possess a firearm, the Court may hold that it is reasonable for police to conduct *Terry*-stops and frisks of individuals suspected of terrorist activities based on information provided by uncorroborated calls from anonymous informers.

In addition to permitting *Terry*-stops of suspected terrorists under circumstances where the reliability of an anonymous informer's tip would not be sufficient to justify a *Terry*-stop of an individual involved in a non-terrorist criminal enterprise, the automatic terrorist exception may also permit the Court to allow more intrusive searches of individuals suspected of terrorist activity. Interesting, in *J.L.* the Court stated that "extraordinary dangers sometimes justify unusual precautions."¹¹² With this statement, the Court made clear that the Fourth Amendment is not a monolith,¹¹³ that the protection provided by the Fourth Amendment, and the amount of suspicion needed to justify a search under the Fourth Amendment, exists on a gradient. Along this gradient, as the level of intrusiveness of a search increases, the requisite level of suspicion needed to justify a search also increases. Therefore, this statement suggests that the sliding scale of reasonableness identified in *Camara*, and clarified in *Terry*, also depends on the extraordinary nature of the danger threatened.

Based on the Court's reasoning pre-*J.L.*, the level of suspicion, and more importantly the reliability of the information upon which the suspicion is based, needed to strip search an individual would be much greater than the level of suspicion needed to pat down the individual's outer clothing. The Court's reasoning in *J.L.* indicates that the level of suspicion needed to pat down the outer clothing of an individual suspected of carrying a switchblade would be greater than the level of suspicion needed to pat down the outer clothing of an individual suspected of carrying a kilogram of C-4 plastic explosive (see Ap-

¹¹¹ *Id.* at 273-74 (emphasis added).

¹¹² *Id.* at 272.

¹¹³ See Amsterdam, *supra* note 96, at 388.

pendix, Figure 1A). If, as it suggests in *J.L.*, the Court is willing to alter the level of suspicion required, or the reliability of information upon which this information is based, in cases threatening “extraordinary dangers,” data that is moderately reliable should permit a more intrusive search to be conducted under circumstances threatening “extraordinary dangers” than under less threatening circumstances (see Appendix, Figure 1B). This line of reasoning suggests that although the Court should not permit the use of high-resolution weapon detectors under “normal” *Terry*-stop circumstances where the individual is suspected of being involved in non-terrorist criminal enterprise, because of the extraordinary danger posed by individuals suspected of terrorist activity, electronic frisks may be permitted in cases where there is evidence the individual is involved in terrorist activity.

In addition to the extraordinary dangers posed by terrorists, more intrusive searches of individuals suspected of terrorist activity may be justified based on the types of weapons commonly employed by terrorists. Whereas criminals involved in non-terrorist activities commonly carry concealed firearms that can be detected rather easily by magnetometers or patdowns of an individual’s outer clothing, terrorists involved in recent attacks in the United States have employed box cutters, plastic knives,¹¹⁴ and plastic explosives hidden in their shoes.¹¹⁵ These types of weapons are difficult to detect with magnetometers or typical *Terry*-style patdowns, but can be easily detected with the use of passive millimeter wave or low-dose X-ray imaging.¹¹⁶ Passive millimeter wave imaging can be used to detect “ceramic knives, low- or non-metal guns, non-metal grenades, . . . plastic explosives, [and] electronic devices such as ‘wires,’ tape recorders, explosive timers, or remote detonators.”¹¹⁷ Because of the “extraordinary dangers” threatened by terrorist activity, and because the types of weapons commonly employed by terrorists are difficult to detect in typical *Terry*-style patdowns, the Court may create an “automatic terrorist exception” allowing government agents to electronically frisk, during a *Terry*-stop, individuals suspected of terrorist activity.

¹¹⁴ Washington Whispers, *The Gun Angle*, U.S. NEWS AND WORLD REPORT, Nov. 12, 2001, at 4.

¹¹⁵ *Shoe-bomb Suspect Pleads Not Guilty to All 9 Charges*, THE DESERET NEWS, Jan. 19, 2002, at A02.

¹¹⁶ See Hawkins & LaGessee, *supra* note 3, at 56-57.

¹¹⁷ *Gun Violence Hearings*, *supra* note 67, at 1 (statement of G. Richard Huguenin, President, Millitech [now Millimetrix] corporation).

C. *Use of Weapon Detection Systems Without Probable Cause or Reasonable Suspicion*

1. Non-Administrative Searches: “Street Searches”

A primary concern surrounding the development of weapon scanning technology is that once the police have hand-held or vehicle mounted weapon detection systems, they will begin routinely scanning people walking along sidewalks, window shopping, or strolling in the local park, and that this scanning will be conducted without probable cause or a reasonable articulable suspicion that the individuals scanned have been involved in any sort of criminal enterprise. David A. Harris, a professor of law at the University of Toledo College of Law, noted that once hand-held weapon detectors are developed, “[n]othing is going to stop the police from scanning everybody.”¹¹⁸ According to Max Glaskin of the *Sunday Times*, the development of portable weapon detection systems means that “anyone, anywhere can be ‘frisked’ unknowingly, either by a fixed machine or one held by hand.”¹¹⁹ Reports from one of the developers of high-resolution weapon detection systems, G. Richard Huguenin, President of Millitech Corporation, do little to lessen these concerns. In his statement before a House of Representatives subcommittee, Mr. Huguenin commented that passive millimeter wave imaging offers the advantage of remote frisking suspects when a patrolman “does not wish to heighten tensions by having direct physical contact with a suspect.”¹²⁰ After reviewing these remarks, Mark Glaskin observed that police could further reduce potential tension and make their job safer by scanning suspects from “an unseen vantage point.”¹²¹ The potential for abuse is obvious.

The Court’s analysis in *United States v. Place*¹²² illustrates when, in non-administrative settings, weapon detection systems could be used without probable cause or reasonable articulable suspicion. The Court’s holding in *Place* illustrates the characteristics of the ultimate concealed weapon detection system.¹²³

In *Place*, the police responded to an anonymous tip that Place might be involved in drug trafficking. The police stopped Place at an airport and subjected his luggage to a “sniff search” by a drug-sniffing dog. The dog reacted

¹¹⁸ Milstone, *supra* note 17, at 32.

¹¹⁹ Glaskin, *supra* note 92, at Features.

¹²⁰ *Gun Violence Hearings*, *supra* note 67, at 1 (statement of G. Richard Huguenin, President, Millitech [now Millimetrix] Corporation).

¹²¹ Glaskin, *supra* note 92, at Features.

¹²² 462 U.S. 696 (1983).

¹²³ The hypothetical ultimate concealed weapon detection system would be a high resolution-low intrusiveness system that, like the canine sniff, detects only contraband. Such a system does not currently exist.

positively to Place's luggage, giving the police probable cause to conduct a thorough search of the bag. During the search, the police discovered cocaine.

Place argued that the cocaine the police discovered in his luggage was the fruit of an illegal search and should be excluded as evidence because the police subjected his luggage to the "canine sniff" without probable cause.¹²⁴ The court rejected Place's argument.

Although the police did not have probable cause to search Place when his luggage was subjected to the canine sniff, the cocaine the police discovered in his luggage did not have to be excluded because the canine sniff did not constitute a search under the Fourth Amendment. The Court noted that the canine sniff "does not require opening the luggage"¹²⁵ scanned by the dog, and the dog only responds to the presence of contraband. Because the canine sniff does not "expose noncontraband items that otherwise would remain hidden from public view, . . . the manner in which information is obtained [with the canine sniff] is much less intrusive than a typical search."¹²⁶ The Court held that because of the minimal intrusiveness of the canine sniff and because the canine sniff reveals the presence only of contraband, use of the canine sniff to detect narcotics in luggage does "not constitute a 'search' within the meaning of the Fourth Amendment."¹²⁷

Through analogy, *Place* suggests that, even without probable cause to suspect a person is carrying a concealed weapon or reasonable articulable suspicion that the individual is armed and dangerous, it would be constitutionally permissible to scan the person with a weapon detection system that only exposed the presence of illegal weapons. Because the detection system would reveal the presence of contraband only, being scanned by the system would not constitute a search under the Fourth Amendment.¹²⁸ Therefore, because the scan would not constitute a search, concealed weapons detected by the system would not be excluded as fruits of an illegal search.

An important factor to consider when analogizing the canine sniff to weapon detection systems is that, unlike concealed weapons, the legality of most "street drugs" is relatively uniform among states.¹²⁹ For example, the possession of cocaine is illegal in all fifty states. The use of a drug detection system capable of detecting only cocaine would not constitute a search anywhere in the United States because cocaine is contraband throughout the Union. In con-

¹²⁴ *Place*, 462 U.S. at 703-04.

¹²⁵ *Id.* at 707.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Kyllo v. United States*, 533 U.S. 27, 37 (2001). "[S]ense-enhancing equipment that identifies nothing but illegal activity is not a search." *Id.* at 47-48 (Stevens, J., dissenting) (emphasis added).

¹²⁹ A notable exception includes the legally prescribed use of marijuana for medicinal purposes in some states.

trast to the uniform illegality of cocaine possession throughout the United States, the legality of carrying concealed weapons varies among the fifty states.¹³⁰ Currently, it is legal to carry concealed firearms, provided the appropriate state permits are obtained, in thirty-one states.¹³¹ Assuming that a weapon detection system could be developed that detects the presence only of firearms,¹³² random scans with the system could be used only in the nineteen states where possession of concealed firearms is illegal. Probable cause or reasonable articulable suspicion would be needed to scan suspects with the detection system in the thirty-one states where it is legal to carry concealed firearms.¹³³

The Fourth Amendment would not proscribe the use of weapon detection systems revealing the presence only of contraband. However, weapon detection systems capable of detecting only contraband do not currently exist. The weapon detection systems that have recently become available (e.g., Body Search low dose X-ray imager) or are currently under development (e.g., Millivision millimeter wave imager) have the greatest potential for more effective weapon detection – but also are highly intrusive.

Because weapon detection systems that are currently available reveal the presence of items other than contraband, they cannot be categorized as dichotomous search systems like the canine sniff discussed in *Place*. Until dichotomous weapon detection systems are developed, weapon detectors can not be used to scan individuals in non-administrative settings where the police do not have probable cause that the individual has committed a crime or a reasonable articulable suspicion that they are armed and dangerous.

¹³⁰ *Gun-Detection Devices Ripped As Too Intrusive*, CHATTANOOGA FREE PRESS, Apr. 8, 1997, at A3.

¹³¹ *Id.*

¹³² Metal detectors currently in use detect all metal items; detection is not limited to firearms. The resolution of these systems is low. Although some companies, such as InVision Technologies, Inc., are developing passive magnetic sensing technology capable of recognizing the magnetic moments, or “signatures,” of specific weapons, allowing the system to “discriminate between guns and harmless clutter objects such as keys and eye glasses,” these systems are not currently available. *InVision Technologies Subsidiary Accelerates Development of New Weapons Detection Technology, Enters Technology Licensing Agreement*, BUS. WIRE, Apr. 30, 1999, LEXIS, News Library, Business Wire File.

¹³³ This only applies to use of the weapon detection system in random “street” scans. This caveat does not apply to use of the weapon detection system in an administrative search context. For example, because concealed firearms are illegal in all commercial airports, the system could be used to scan for concealed firearms in airports, even in the thirty-one states where concealed firearm possession is legal.

2. Administrative Searches: Vehicle Checkpoints, Border Searches, Airports

a. Vehicle Checkpoints

Case precedent reveals that weapon detection systems could not be used at vehicle checkpoints that were established primarily to detect ordinary criminal activity.¹³⁴ The use of vehicle checkpoints to detect criminal activity has been a matter of intense debate.¹³⁵ The Supreme Court has approved of the use of suspicionless highway checkpoints for three objectives: (1) detecting illegal aliens,¹³⁶ (2) inspecting each driver's license and vehicle registration,¹³⁷ and (3) conducting sobriety tests.¹³⁸

In *City of Indianapolis v. Edmond*,¹³⁹ the Court recently considered the constitutionality of the use of a drug-sniffing dog to detect contraband at a license and vehicle registration checkpoint. The Court held that use of the drug-sniffing dog at the registration checkpoint violated the Fourth Amendment and noted that vehicle checkpoints cannot be established to detect ordinary criminal activity.¹⁴⁰

The Court's holding in *Edmond* clearly indicates that the Fourth Amendment bars the use of high resolution, highly intrusive weapon detection systems to randomly scan drivers at vehicle checkpoints.¹⁴¹ More importantly however, the Court's holding in *Edmond* indicates that the Fourth Amendment proscribes the use of dichotomous, high resolution, low intrusiveness weapon detectors analogous to the canine sniff at vehicle checkpoints.

Although case precedent indicates that weapon detection systems could not be used to detect ordinary criminal activity at vehicle checkpoints, the Court noted in *Edmond* that "there are circumstances that may justify a law enforcement checkpoint where the primary purpose would . . . , but for some emer-

¹³⁴ *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).

¹³⁵ *See, e.g., Edmond*, 531 U.S. 32; *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976).

¹³⁶ *See Martinez-Fuerte*, 428 U.S. at 562.

¹³⁷ In *Delaware v. Prouse*, 440 U.S. 648 (1979), the Supreme Court suggested that vehicle checkpoints could be established to inspect the driver's license and registration as long as all oncoming traffic was stopped and questioned. Subsequent to the Court's decision in *Prouse*, lower courts have upheld general vehicle registration checkpoints as constitutional. *See* 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 10.1-.02, at 676-78, 682-85 (3rd ed. 1996).

¹³⁸ *Sitz*, 496 U.S. at 453-55.

¹³⁹ 531 U.S. 32 (2000).

¹⁴⁰ *Id.* at 40-42.

¹⁴¹ *See id.*

agency, relate to ordinary crime control.”¹⁴² In defining such a circumstance, the Court stated that “the Fourth Amendment would almost certainly permit [a] . . . roadblock set up to thwart an imminent terrorist attack.”¹⁴³ Based on the Court’s holding in *Edmond*, use of weapon detection systems at a vehicle checkpoint may be constitutionally permissible as long as the checkpoint is an “appropriately tailored roadblock” established based on probable cause to believe that a terrorist attack is imminent and that establishment of the checkpoint will aid in thwarting the attack.¹⁴⁴

b. *Border Searches*

The Court’s holding in *United States v. Ramsey*¹⁴⁵ indicates that Fourth Amendment protection virtually disappears at international borders. People may be stopped and searched at international borders without a warrant. In addition, border patrol agents may search individuals crossing international borders without probable cause to believe the individual has committed a crime and without reasonable articulable suspicion that the individual is armed and dangerous.¹⁴⁶ No “individualized suspicion of wrongdoing” is required for searches or seizures conducted at international borders.¹⁴⁷

High-resolution, highly intrusive weapon detection systems could be employed at international borders and could be used to randomly scan individuals entering the country. No individualized suspicion of wrongdoing would be required to conduct border searches with existing weapon detection systems or systems currently under development.

c. *Airports*

Airports, like international borders, present unique situations with regard to the Fourth Amendment. In *Florida v. J.L.*,¹⁴⁸ the Supreme Court noted that it did not hold “that public safety officials in quarters where the reasonable expectation of Fourth Amendment Privacy is diminished, such as airports . . ., cannot conduct protective searches on the basis of information insufficient to justify searches elsewhere.” In addition, in *Ramsey*, the Court clearly indicated that the exceptions to the Fourth Amendment that applied at international bor-

¹⁴² *Id.* at 44.

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ 431 U.S. 606 (1977).

¹⁴⁶ *Id.* at 616.

¹⁴⁷ DRESSLER, *supra* note 97, at 283.

¹⁴⁸ 529 U.S. 266, 274 (2000) (internal citations omitted).

ders, also applied at “functional equivalents” of international borders.¹⁴⁹ The Court noted that “border-search doctrine, suggests no distinction . . . stemming from the mode of transportation across [the] borders” of the United States.¹⁵⁰

The Court’s holdings in *J.L.* and *Ramsey* suggest that airports where international flights arrive will be treated as borders with respect to search and seizure doctrine. Under this analysis, if necessary, passengers at airports could be scanned with high resolution, highly intrusive weapon detection systems currently available.

V. CONCLUSION

The National Institute of Justice says that Millivision scanners “are intended to be used only in places such as airports, courts and prisons or to search suspects who may be frisked under *Terry* standards.”¹⁵¹ Based on analysis of case precedent, this may overstate the constitutionally permissible use of high resolution, highly intrusive weapon detection systems like Millivision scanners.

Case precedent clearly indicates that high resolution, highly intrusive weapon detection systems could be used to search suspects in all circumstances where the police have probable cause to conduct a search and in all circumstances where a manual frisk would be permitted (e.g., search incident to arrest). The use of weapon detection systems in these circumstances may reduce the risk of injury both to police officers and to suspects. In addition, because the use of a weapon detector does not require the suspect to stand “spread eagle” with his hands on his head, weapon detectors can reduce the humiliation and anxiety associated with being frisked in public.

Although newly developed weapon detectors may be substituted for frisks in circumstances where a manual frisk would be appropriate, the high level of intrusion associated with the use of these types of scanners makes it unlikely that the Supreme Court would permit police to use them in place of ordinary *Terry*-frisks. In recent decisions regarding search and seizure, the Supreme Court left itself room to create a “terrorist exception.” Under the “terrorist exception,” police would be permitted to use high resolution, highly intrusive weapon detection systems in *Terry*-frisk circumstances. However, in order for the search to fall under the “terrorist exception,” the police must have a reasonable articulable suspicion that the suspect is armed, dangerous, and involved in terrorist activity.

Without probable cause to search or a reasonable articulable suspicion that a suspect is armed and dangerous, high resolution, highly intrusive weapon detectors can be used only in administrative searches. The Court’s holding in *Place* suggests that if a dichotomous weapon detection system could be devel-

¹⁴⁹ 431 U.S. at 622.

¹⁵⁰ *Id.*

¹⁵¹ Milstone, *supra* note 17, at 32.

oped that would detect only contraband, individualized suspicion would not be required for its use. Although the Court's recent holding in *Edmond* makes this conclusion less certain, it is clear that as a weapon detection system's resolution increases, intrusiveness decreases, and the violence associated with the type of criminal activity monitored increases, the Court will be less likely to determine that use of the system violates the Fourth Amendment.

With regard to administrative searches, the Court's holding in *Edmond* indicates that use of currently developed weapon detection systems in conjunction with roadblocks would constitute an impermissible search. In addition, *Edmond* suggests that even if a perfectly dichotomous weapon detection system were developed, its use at vehicle checkpoints may violate the Fourth Amendment. However, use of even highly intrusive weapon detectors may be permitted under circumstances where, in reaction to credible information indicating terrorist activity is afoot, the police establish an appropriate roadblock tailored to detect that activity.

Because of the reduction in Fourth Amendment protections at international borders and airports, administrative searches at these locations can be highly intrusive and can be conducted without individualized suspicion. Associated with the sovereign's right to protect itself, high resolution, highly intrusive weapon detection systems can be employed at borders and in airports to detect illegal activity.

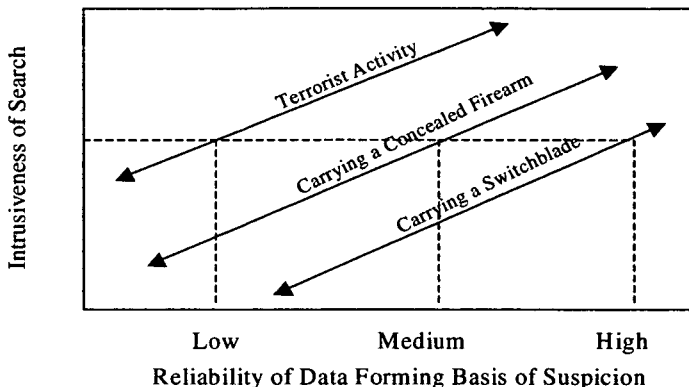
Existing and development weapon detection systems have the potential to work both good and evil. Because of the types of weapons currently employed by terrorists (e.g., plastic knives and shoes with the soles replaced by explosives), it is impossible to imagine a weapon detection system capable of detecting all instruments of death, while leaving personal items like artificial limbs, colostomy bags, implants, and intimate items hidden from the government eye. Use of current and developmental weapon detection systems offer the promise of greater personal and national security and the simultaneous loss of civil liberties. Unfortunately, the gain of one will inevitably mean some loss of the other. The attacks of September 11th demand that we re-balance civil liberties with personal and national security. Although most of us hate change, the re-balancing has already begun. It is only through knowledgeable consideration and retrospection that we can recall the past, determine the civil liberties we are willing to forego and the security we are willing sacrifice to protect our individual freedoms, and shape the future.

*Michael A. Menzel, Jr.**

* J.D. Candidate May 2003, West Virginia University College of Law; Ph.D. Candidate May 2003, Forest Resource Science, West Virginia University, Division of Forestry; M.S., Wildlife Biology, University of Georgia, 1998; B.S., Forest Resources, University of Georgia, 1995. I thank my wife, Jennifer, for her untiring support and my daughter, Emma, for her interminable patience.

APPENDIX

A



B

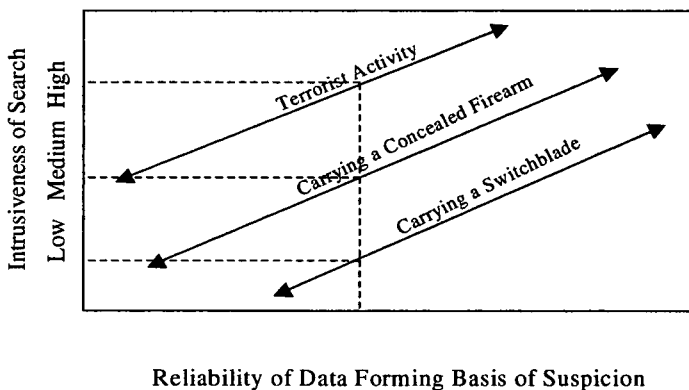


Figure 1. Figure A illustrates the effect of the level of danger posed from a suspected activity (i.e., terrorist activity v. carrying a switchblade) on the reliability of data needed before a moderately invasive search can be conducted. The lower the level of danger posed by the suspected activity, the higher the reliability of data required for a search of a constant intensity. Figure B illustrates that by extrapolation, the Court's holding in *Florida v. J.L.*, 529 U.S. 266 (2000) indicates that for a constant level of reliability of data, the level of search intensity permitted during a Terry frisk would increase with the increasing level of danger posed by the suspected activity.