NOTE

BAD INTENT OR JUST A BAD DAY? FOURTH AMENDMENT IMPLICATIONS RAISED BY TECHNOLOGICAL ADVANCES IN SECURITY SCREENING

Lindsey Gil[*]

I. INTRODUCTION

People rarely think just about work when they enter their offices each day. The human mind is able to juggle a wide array of worries and concerns at any given moment. In an age of wireless communication and digital media, people are easily accessible and in turn, easily reminded of those very worries and concerns. In this modern world, it is rare for any person to categorize himself as free from cares and stress for a prolonged period of time.

Now imagine entering your workplace, your mind full of worry about a big project you must complete by the day's end. You walk through your office's newest security measure for the first time – a machine that resembles, to put it bluntly, a metal detector on steroids. While you are standing in the machine, a security attendant begins to ask you a series of questions ranging from "Are

[*] J.D., Boston University School of Law, 2010; B.A. Economics and Public Relations, *summa cum laude*, Syracuse University, 2007.

you carrying any weapons at this time?" to "Do you intend to commit any illegal acts inside this building today?" This does not feel like a typical security measure, so your anxiety level begins to rise. Instead of being allowed to pass through the machine and proceed to your office, you are asked to submit to a second scan. Within the next few minutes you gradually become alarmed as after the second scan you are brought into a private room where you are questioned by security officials to ascertain whether or not you are a part of a plot to hurt people inside your office building.

Although this example might seem slightly exaggerated, this situation has become a very real possibility with the invention of the government's newest security-scanning technology: MALINTENT. As the recent attempted bombing of a Detroit-bound jet by Umar Farouk Abdulmuttallab on Christmas Day shows, the threat of terrorist violence is still ever-present and the Department of Homeland Security (DHS) is scrambling to brief building owners and airlines on how to best prevent potential attacks.[1] MALINTENT reflects DHS's commitment to seeking out new technologies to counter national security threats.[2] Although MALINTENT scans may be effective in spotting potential terrorists, they raise serious concerns in the areas of personal liberty and privacy. Specifically, it is unclear whether the use of MALINTENT technology violates Fourth Amendment protections.

This Note examines the Fourth Amendment issues raised by the use of this new scanning system. Part II describes the technology behind MALINTENT and how MALINTENT scans are used to detect individuals with criminal intentions. Additionally, Part II also examines some of the general concerns that accompany the use of this technology. Part III evaluates the MALINTENT technology through the lens of the Fourth Amendment to determine whether the way in which the technology scans an individual constitutes a search and whether that search is lawful. Part IV suggests MALINTENT will be found to be a Fourth Amendment search and that such a search will likely be allowed under the administrative search exception to the warrant requirement.

II. BACKGROUND

A. The Technology Behind MALINTENT

MALINTENT is a new security system developed by the Human Factors Division, a department within DHS's Directorate for Science and Technology.[3]

---

[1] *See Christmas Day Bomb Scare Prompts Review of Airline Security*, PBS.ORG., Dec. 28, 2009, http://www.pbs.org/newshour/bb/terrorism/july-dec09/airport1_12-28.html.

[2] Department of Homeland Security: Science & Technology, http://www.dhs.gov/files/scitech.shtm (last visited Feb. 3, 2010).

[3] *See* Liz Hazelton, *The Airport Security Scanner That Can Read Your Mind*,

At its mechanical level, MALINTENT is a mobile walk-through corridor that contains sensors and imagers that that can read body temperature, heart rate, respiration, eye movement and other biometric indicators, without any actual physical contact.[4] The purpose of this test is to assess nonverbal cues provided by biometric data to determine whether the person passing through the system intends to harm others.[5] To put it simply, this technology claims to be able to spot a person with "malintent or the intent or desire to cause harm," much like an "x-ray for bad intentions."[6]

MALINTENT operates like the walk-through metal detectors (magnetometers) commonly used in airports and courthouses. A person walks through the MALINTENT portal and is asked several control questions by an interviewer while in the portal.[7] MALINTENT's sensors then record that person's biometric data, which is transmitted to computers that develop a "risk assessment" for the person in question.[8] When the sensors pick up data from an individual that is not consistent with a person with "neutral" intentions, the sensors transmit warning data to analysts in a nearby mobile unit the size of a trailer.[9] Those analysts can then choose whether or not to "flag" the entrant.[10] When an analyst chooses to flag an entrant, that entrant is pulled aside both for questioning and to undergo an additional scan within the MALINTENT portal, which includes micro-facial scanning.[11] This second scan is able to recognize seven primary emotions and emotional cues, as well as minute muscle movement, which can indicate criminal intent.[12] By 2010, the MALINTENT system will also include equipment that analyzes all body movement (not just

DAILYMAIL, Sept. 24, 2008, http://www.dailymail.co.uk/sciencetech/article-1060972/The-airport-security-scanner-read-mind.html.

[4] *See Malintent Will Make You Sweat*, TECHTREE.COM, Sept. 26, 2008, http://www.techtree.com/India/News/Malintent_Will_Make_you_Sweat/551-93658-582.html; *see also* ROBERT P. BURNS, U.S. DEPT. OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 3-4 (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf.

[5] *See Malintent Will Make You Sweat*, *supra* note 4.

[6] *Body Scanner Capable of Detecting "Hostile Intent"*, IMPACTLAB.COM, Sept. 24, 2008, http://www.impactlab.com/2008/09/24/body-scanner-capable-of-detecting-hostile-intent/; Allison Barrie, *Homeland Security Detects Terrorist Threats By Reading Your Mind*, FOXNEWS.COM, Sept. 23, 2008, http://www.foxnews.com/story/ 0,2933,426485,00.html.

[7] *See* Humphrey Cheung, *Homeland Security Testing 'Mind-Reading' Checkpoints*, TGDAILY.COM, Sept. 24, 2008, http://www.tgdaily.com/content/view/39464/108/.

[8] *Id.*

[9] Barrie, *supra* note 6.

[10] *Id*.

[11] *See* Hazelton, *supra* note 3.

[12] *Id.*

facial movement), as well as an eye scanner and pheromone-reader.[13] If an individual passes through the MALINTENT portal without being flagged or the second scan does not confirm the first scan's results, all the information collected about the flagged individual is erased.[14] If, however, the second scan confirms the first scan's results, which suggest a possible security concern, police officers can question, arrest or remove the individual with "criminal intent" from the area before any harm or crime occurs.

One clear benefit of the MALINTENT technology is its ability to utilize racially neutral flags in its scans. MALINTENT's "multi-modal behavioral and physiological sensing technologies" allow for "culturally neutral indicators of mal-intent."[15] Thus, this scanning technique eliminates the racial profiling inherent in many other security procedures. Critics of the use of ethnic, racial or religious profiling to identify potential terrorists have long called for security systems that focus on criminal behavior rather than the aforementioned characteristics.[16] In the airline context, criminal behavior that could be used to detect potential terrorists includes buying a one-way ticket with cash and checking no luggage, behavior exhibited both by Umar Farouk Abdulmuttallab and Richard Reid, the suspected December 2001 shoe-bomber.[17] Similarly, MALINTENT Project Leader Bob Burns states that another advantage of this new security system is that it does not track individuals or make judgments about them, but "analyzes you against baseline stats when you walk in the door" and assesses individuals only with regard to their behavior in the present situation.[18] Burns' statements, however, have not been validated as DHS representatives have yet to explain the exact procedure used to flag an individual after a first or second MALINTENT scan. Although it is implied that the MALINTENT system will register some sort of warning based on a scan's results, there is no information regarding what role, if any, a security analyst will play in deciding to flag an individual.

MALINTENT's creators predict that the technology will be the security

[13] Barrie, *supra* note 6; *see also* Cheung, *supra* note 7.

[14] *See* Barrie, *supra* note 6; *see also* Cheung, *supra* note 7; Hazelton, *supra* note 3; *'Pre-crime' Detector Shows Promise*, NEWSCIENCTIST.COM, Sept. 23, 2008, http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html.

[15] *Draper Labs Awarded $2.6 Million Contract by DHS*, SECURITYINFOWATCH.COM, Feb. 6, 2009,http://www.securityinfowatch.com/root+level/1289487.

[16] *See* Arsalan Iftikhar, *Why Profiling Doesn't Work*, CNN.COM, Jan. 5, 2010, http://www.cnn.com/2010/OPINION/01/05/iftikhar.profiling.does.not.work/index.html?iref=allsearch. Criticizing the use of racial profiling, Iftikhar points out that "by targeting only certain passengers for additional screening, 'blind spots' can be easily identified and duplicitously exploited by violent extremists wishing our country harm." *Id.*

[17] *See id.*

[18] Hazelton, *supra* note 3.

screening of the future and intend to use it at airports, border crossings, sporting events and other security checkpoints.[19] The technology used to develop the MALINTENT system is known as "'Future Attribute Screening Technology' – or FAST – because it is designed to get passengers through security in two to four minutes, and often faster," which is one of the reasons it is well suited for security scanning at large venues.[20] Additionally, MALINTENT is different from other attempts to use large-scale biometric scanning technology because traditional biometric tests focus only on identifying known terrorists, while "FAST technologies focus strictly on real-time psycho physiological/behavioral patterns in an attempt to prevent the unknown terrorist from gaining successful access to his or her desired location."[21] DHS representatives further claim that this technology is so precise it can recognize the difference between a terrorist and someone who is merely experiencing a high level of stress, as well as the difference between a person who is sweating heavily due to nerves and one who naturally sweats heavily.[22] If MALINTENT is truly as effective as its creators promise, the possibilities for the use of this technology to prevent terrorist attacks or expose members of terrorist cells in the United States are endless.

B. Government Tests of MALINTENT

As of the writing of this Note, DHS has conducted only one public test of MALINTENT, which took place on September 18, 2008 in the D.C.-Maryland area.[23] Participants in the test thought they were entering a building to attend a technology expo when, in reality, they were walking through the MALINTENT system.[24] Over one hundred and forty-four test subjects unknowingly participated.[25] Of those one hundred and forty-four test subjects, twenty-three were selected by Homeland Security to act as "civilian accomplices" in the test and were given a disruptive device to carry into the building, thereby creating the criminal purpose MALINTENT technology is designed to recognize in individuals.[26] Participants standing in the MALINTENT portals were asked control questions by interviewers in order to evaluate their biometric responses.[27] Control questions included, "Do you plan to detonate an explosive at the expo today?" and "Do you plan to illegally

[19] *See*, *e.g.*, *id.*

[20] Barrie, *supra* note 6.

[21] *Draper Labs Awarded $2.6 Million Contract by DHS*, *supra* note 15.

[22] *See* Barrie, *supra* note 6.

[23] *See id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* Cheung, *supra* note 7.

record any information at the expo today?"[28] Although the results of the test are classified, DHS Undersecretary for Science and Technology Administration Jay Cohen called the test a "home run."[29] Furthermore, DHS spokesman John Verrico stated that although DHS is still in the early research stages of development, the project is looking "promising" and tests are running at about "seventy-eight percent accuracy on malintent detection and eighty percent on deception" detection.[30]

C. Early Criticism of MALINTENT

Project Leader Bob Burns claims that MALINTENT will "restore a sense of freedom" that citizens have not experienced since September 11, 2001.[31] Critics, however, argue that MALINTENT creates a world where "thought crime" might actually be a reality. Bloggers and personal privacy advocates all across the United States have taken to the web to express their concerns about this type of technology.[32] Frequent comparisons are made between MALINTENT and the "crimethink" system used in George Orwell's novel Nineteen Eighty-Four or to the technology used in Tom Cruise's 2002 movie, Minority Report.[33] Bloggers and their commenters seem especially concerned about the impact this technology will have on the general public's freedoms, which is best summarized by one individual's allusion to a quote by Benjamin Franklin: "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[34]

Orwellian comparisons aside, many critics have major concerns about the reliability of the MALINTENT technology. Specifically, bloggers question the use of control questions in evaluating an individual's biometric responses – a method used in current polygraph tests that are considered by many to be unreliable and largely inadmissible in court proceedings.[35] Critics have also expressed concerns regarding the propensity for this technology to generate a

---

[28] *Id.*

[29] Barrie, *supra* note 6.

[30] *Body Scanner Capable of Detecting "Hostile Intent"*, *supra* note 6.

[31] Barrie, *supra* note 6.

[32] For an example of some of the blog-based discussions regarding MALINTENT technology, see Bruce Schneier, *Thoughtcrime*, SCHNEIER ON SECURITY, Sept. 25, 2008, http://www.schneier.com/blog/archives/2008/09/thoughtcrime.html.

[33] *See* Kevin Underhill, *DHS Says Scanners Successfully Detect "Mal-Intent,"* LOWERINGTHEBAR.COM, Nov. 19, 2008, http://www.loweringthebar.net/2008/11/dhs-testing-hos.html.

[34] *See* Posting of Mentor to Ryoung5367's blog, http://www.wral.com/golo/blogpost/3598960 (Sept. 24, 2008, 9:58 a.m. EST).

[35] *See* Underhill, *supra* note 33.

large percentage of false positives.[36] Although MALINTENT project representatives claim the technology is so sensitive that it can tell the difference between a terrorist and a person who is experiencing a high level of stress, it is unclear whether in practice such a claim is true. As MALINTENT will likely be used in airports and courthouses, two areas which commonly see individuals with high stress levels, the risk of false positives is a legitimate worry. Because MALINTENT is designed to aid in national security efforts, however, its creators have largely not released information that addresses many of these apprehensions. Even available information about MALINTENT, however, reveals some areas of concern. In particular, MALINTENT is designed to register a highly subjective emotional and mental state. It is uncertain whether directing someone to smuggle something into an arena or to think like a terrorist, which is what DHS representatives told civilian accomplices to do during MALINTENT's only public test, would truly produce the type of physiological reaction present in a potential terrorist.

Similarly, it is unclear how the technology will account for specific medical or psychological disorders in individuals that may affect their biometric or behavioral responses. As false positives must be investigated just as stringently as other threats to determine whether an actual security risk exists, the presence of false positives undermines the MALINTENT system by devoting scarce security resources away from actual threats.[37] The severity of such a drawback depends largely on how many false positives the system identifies. As noted, currently available data suggests that the MALINTENT system is running at about seventy-eight percent accuracy level regarding malintent detection.[38]

Additionally, critics also argue this technology is an invasion of privacy because it "catalogs vital signs for non-medical reasons."[39] John Verdi of the Electronic Privacy Information Center characterizes the MALINTENT system as a "medical exam conducted without permission" and describes it as "substantially more invasive" than current security screening measures in use at airports across the United States.[40] Furthermore, this type of technology will

[36] *See, e.g.*, Hazelton, *supra* note 3 (posting of Rich Edwards, Sept. 24, 2008); *see also Homeland Security's Big Brother 'Malintent' Program on Fast Track*, PHANTOMSANDMONSTERS.WETPAINT.COM, Dec. 18, 2009, http://phantomsandmonsters.wetpaint.com/page/Homeland+Security's+Big+Brother+'Malintent'+Program+On+Fast+Track.

[37] *See* Fred H. Cate, *Government Data Mining: The Need For A Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 475 (2008).

[38] *See Body Scanner Capable of Detecting "Hostile Intent"*, *supra* note 6.

[39] *Fighting Terrorism Through Clairvoyance*, THE TRAVELER NEWSLETTER (Assist America, Inc., Princeton, N.J.), 3d Q. 2008, http://www.assistamerica.com/traveler/travelervol26.htm.

[40] Underhill, *supra* note 33. Current screening technology used in most airports is not

capture the clothing-less form of many Americans suspected of no wrongdoing, as it also involves full body scanning.[41] Although Amy Kudwa, a DHS spokeswoman, claims that no information gathered about a person will be stored after the scan, critics have pointed out problems with that claim.[42] First, storage of a scan's results will likely be necessary when a scan leads to an arrest or questioning. The government, however, has released no information as to how the information from a MALINTENT scan will be stored or used in situations that result in an individual's arrest, seizure or prosecution. Secondly, the government will likely have to collect a wide range of biometric data in order to train the system to differentiate between neutral responses and responses that should merit a second scan.[43] This will require either large-scale testing by consent to collect this type of information or it will be initially necessary to store information gained from those scanned by the system in order to improve the effectiveness of this technology.

Finally, the basis of MALINTENT's technology – the science of biometrics – has faced criticism when used in national security initiatives. The effective use of biometrics depends largely on the collection of a wide range of physiological and psychological data from a large number of people in order to develop "valid predictive models."[44] This poses a problem in national security settings because the government likely does not have enough information regarding the biometric responses of terrorists during their attacks in order to create an effective predictive model for recognizing a potential terrorist on the basis of biometrics.[45] The development of a predictive model to recognize terrorists is further complicated by the fact that terrorists and terrorist attacks rarely follow a set pattern. Such attacks are often planned to avoid any of the behavioral or physiological triggers that form the basis for a biometric predictive model.[46]

As the above criticisms illustrate, the MALINTENT technology has the propensity to infringe on an individual's Fourth Amendment rights. It is

even sophisticated enough to show the contours of the body or reveal foreign objects. *See* John Schwartz, *The Debate Over Full Body Scans vs. Invasion of Privacy Flares Anew After Incident*, N.Y. TIMES, Dec. 29, 2009, http://www.nytimes.com/2009/12/30/us/30privacy.html.

[41] *See* Schwartz, *supra* note 40. The use of full body scanning in itself is not always thought to be highly reliable as such machines have limits in that they cannot detect objects stowed in bodily orifices or concealed within the folds of an obese person's flesh. *See id.*

[42] *See* Catherine Elsworth, *New Airport Screening "Could Read Minds"*, TELEGRAPH.CO.UK., Sept. 23, 2008, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3069960/New-airport-screening-could-read-minds.html.

[43] *See* Posting of Mentor, *supra* note 34.

[44] Cate, *supra* note 37, at 473-74.

[45] *See id.* at 474.

[46] *See id.* at 474, 477-78.

therefore necessary to conduct a further analysis of this technology within the framework of the Fourth Amendment to determine whether such infringements actually occur. On its most basic level, the Fourth Amendment prohibits unlawful search and seizure and attempts to protect a citizen's privacy and liberty interests.[47] The Fourth Amendment in practice, however, is much more complex than this simplified interpretation. In assessing the broad impact of the Fourth Amendment, the Court has outlined a series of rules and standards that affect the behaviors and practices of law enforcement officers. In order to effectively conduct a Fourth Amendment analysis, however, it is best to keep the basic interpretation in mind. Thus, in considering whether a situation may implicate a person's Fourth Amendment rights, one should first consider a question that goes to the very heart of the Fourth Amendment: has a search occurred?

III. MALINTENT AND THE FOURTH AMENDMENT

A Defining a Search

1. Plain View Doctrine

A search within the meaning of the Fourth Amendment requires a physical intrusion into a constitutionally protected area, which can include both bodies and attire.[48] MALINTENT scans, although they gather information about some of the interior workings of the body, are solely exterior scans, which may not constitute physical intrusions in the traditional sense.[49] Additionally, the biometric data gathered from these scans disclose information that, theoretically, a person would be able to observe using his or her senses. As many of the biometric responses that can cause the MALINTENT system to flag an entrant can be observed visually, like perspiration rate, eye movement and respiratory rate, these scans may require analysis under the plain view doctrine.

The plain view doctrine emerged from *Coolidge v. New Hampshire*, in which the Court held that under certain circumstances, as long as the officers remain within the bounds of the original search, the police may seize evidence in plain view without a warrant.[50] Although this doctrine appears to presuppose a "search," later interpretations of the *Coolidge* decision by the

[47] *See* U.S. CONST. amend. IV.

[48] *See* Silverman v. United States, 365 U.S. 505, 512 (1961).

[49] With the emergence of sense-enhanced technology, however, standards defining a search within the meaning of the Fourth Amendment are evolving – a concept which will be examined later in this note.

[50] Coolidge v. New Hampshire, 403 U.S. 443, 467-68 (1971).

Court validate a warrantless search and seizure if the police officer, standing in a lawfully permitted position, is able to see the incriminating evidence in plain view.[51] The primary justification for this doctrine is that in situations where incriminating evidence is in plain view, the protections provided by the warrant process are unnecessary.[52] The plain view doctrine now also extends to certain other senses, such as hearing and smell, both of which can justify a warrantless search and seizure.[53]

Under the plain view doctrine, a police officer's basic observations do not constitute a search. Similarly, if a person is validly stopped, it is not a search for an officer to visually examine the entire exterior of that person.[54] Such an observation does not constitute a search because what a person willingly exposes to the public eye is not a privacy interest protected by the core of the Fourth Amendment.[55] Thus, it can be argued that because the MALINTENT scanning technology does assess certain factors that are apparent to the human eye, aspects of these scans may fall under the plain view doctrine and, therefore, may not constitute a search within the meaning of the Fourth Amendment. The boundaries of what is considered in plain view, however, are not precisely defined. Here, MALINTENT measures minute variations in biometric data and assesses several biometric factors, some apparent to the naked eye and some not, in order to determine whether to flag a person.[56] As MALINTENT assesses these factors together and uses sense-enhancing technology to obtain some of the data, it is arguable whether these scans should truly fall under the plain view doctrine and avoid categorization as a search.

The plain view doctrine does have certain limitations. One such limitation applies when the evidence in plain view requires advanced scrutiny to aid an investigation. Some courts have found that the examination of publicly exposed information, which requires additional analysis to be of investigative

[51] *See* Horton v. California, 496 U.S. 128, 136-37 (1990).

[52] *See Coolidge*, 403 U.S. at 467-68.

[53] *See id.* at 468 ("[I]ncontrovertible testimony of the senses" may provide probable cause for seizure of evidence); *see also* Texas v. Brown, 460 U.S. 730, 739 (1983) (noting "that if, while lawfully engaged in an activity in a particular place, police officers perceive a suspicious object, they may seize it immediately").

[54] *See generally The Supreme Court: 1992 Term – Leading Cases*, 107 HARV. L. REV. 144, 165 (1993).

[55] *See* California v. Ciraolo, 476 U.S. 207, 215 (1986); United States v. Knotts, 460 U.S. 276, 281 (1983) (noting that "[one] traveling . . . on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"); Unites States v. Dionisio, 410 U.S. 1, 14 (1973) (observing that "like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear" and for that reason, he has no reasonable privacy expectation as to his voice).

[56] *See* BURNS, *supra* note 4, at 4.

value, does not constitute public knowledge under the plain view doctrine because it extends past the boundary of what is easily observable by the human eye.[57] Thus, there appears to be a fine line between what is considered an investigative technique utilizing publicly exposed information and what is considered a search. One example of a case emphasizing this fine line is *Cupp v. Murphy*.[58] In *Cupp*, the Court found that scraping the fingernails of a voluntarily present murder suspect was a search, notwithstanding a police officer's observation of dried blood on the suspect's fingertips.[59] Because the evidence that was in plain view required further testing to confirm criminal behavior, the taking of that evidence constituted a search.[60] A parallel argument could be made with regard to MALINTENT. MALINTENT scans measure very subtle and often invisible biometric responses. Those responses, standing alone, may not provide an indication of the type of criminal thoughts MALINTENT is designed to detect. Instead, it is often only when those independent biometric responses are considered together that criminal behavior is suggested. As MALINTENT requires a computer to analyze the interplay of several biometric factors, this additional step may take MALINTENT scans out of the realm of the plain view doctrine. Under this reasoning, it is arguable that MALINTENT is properly characterized as a Fourth Amendment search.

2. Sense-Enhanced Searches

In this high technology age, the criteria used to define a "search" under the Fourth Amendment are constantly evolving. The Supreme Court has found that certain investigatory techniques, including dog sniffs and aerial surveillance (both often categorized as sense-enhancing technology) do not constitute searches and thus do not implicate Fourth Amendment concerns.[61] This reasoning is based largely on the idea that an individual has no reasonable expectation of privacy for things the individual exposes to the eyes of the public, much like the rationale behind the plain view doctrine discussed above, even if sense-enhancing technology is required for the observation.[62] Subsequent courts have found that the examination of publicly exposed information using some forms of sense-enhancing technology, especially if it requires additional testing or analysis to be of investigative value, is not public

[57] *See* Molly Bruder, *Say Cheese! Examining The Constitutionality of Photostops*, 57 AM. U. L. REV. 1693, 1704-05 (2008).

[58] *See* Cupp v. Murphy, 412 U.S. 291 (1973).

[59] *See id*. at 294-95.

[60] *See id.*

[61] *See* Bruder, *supra* note 57, at 1703-04; s*ee also* Florida v. Riley, 488 U.S. 445, 449-50 (1967) (holding that surveillance from a helicopter is not a search); United States v. Place, 462 U.S. 696, 706-07 (1983) (holding that a dog sniff of a suitcase is not a search).

[62] California v. Ciraolo, 476 U.S. 207, 215 (1986).

knowledge under the plain view doctrine as it extends past the boundary of what is easily observable by the human eye.[63] Thus, there appears to be minimal difference between what is considered an investigative technique utilizing publicly exposed information and what is considered a search.[64]

As MALINTENT uses sensors to employ a form of sense-enhancing technology, one must determine whether the technology records information exposed to the eyes of the public or whether the use of such technology is so invasive that it qualifies as a search. As mentioned above, enhanced naked eye perception is typically not a search.[65] Recent trends in court decisions, however, suggest that whether sense-enhancing technology constitutes a search depends less on the type of technology involved and more on what that technology reveals.[66] This trend has likely emerged from the decision in *Katz v. United States*, in which the Court focused its concern not on the tools used by the government to obtain information, but on the object of the government's efforts.[67] In *Katz*, the Court held that the government's use of wiretap technology was illegal because it sought information to which the Court believed the individual had a justifiable expectation of privacy.[68] Hence, the Court based its decision on the type of information revealed, not the technology used to uncover it.

A case illustrating this trend is *Kyllo v. United States*. In *Kyllo*, police officers attempted to determine if suspects were growing marijuana in their home through the use of a thermal imaging machine, which revealed whether heat lamps required for the growth of marijuana in such an environment were being used.[69] The officers conducted the thermal scans and then presented the scan results to a magistrate in a warrant application.[70] On appeal, the Supreme Court ruled that the use of the thermal scan was unconstitutional.[71] The Court

[63] *See* Bruder, *supra* note 57, at 1704-05.

[64] Additionally, claiming that something is "knowingly exposed to the public" is not a general way to get around labeling something as a search. It has been suggested that a person exposes to the public only what "reasonably curious persons" might observe and that such a person would not likely engage in "continuous tailing . . . for a long distance or time." Therefore, "long-term visual surveillance may result in a search subject to Fourth Amendment warrant requirements." Note, *Tracking* Katz*: Beepers, Privacy and the Fourth Amendment*, 86 YALE L.J. 1461, 1494 & n.145 (1977).

[65] *See* United States v. Allen, 675 F.2d 1373, 1380 (9th Cir. 1980).

[66] *See Place*, 462 U.S. at 705-06 (holding that use of a drug-sniffing canine does not constitute a search because it detects only the location of contraband without interfering with lawful activities).

[67] *See* United States v. Cusumano, 67 F.3d 1497, 1501-02 (10th Cir. 1995).

[68] *See* Katz v. United States, 389 U.S. 347, 351-52 (1967).

[69] *See* Kyllo v. United States, 533 U.S. 27, 29 (2001).

[70] *Id.* at 30.

[71] *Id.* at 40.

found that using sense-enhancing technology that is not in general public use to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search."[72] The *Kyllo* Court reached this conclusion not only due to the unique privacy interests linked to one's home, but also because the investigative technique in question involved discovering information that was not publicly exposed and fell within an individual's reasonable expectation of privacy.[73] The Court has distinguished *Kyllo* from other cases using sense-enhancing technology, like the use of drug-sniffing dogs in *Illinois v. Caballes*,[74] by stating that the latter methods provide greater privacy protections as they "only reveal the location of drugs, while keeping private all lawful activities."[75] In *Kyllo*, however, the thermal imaging device allowed officers to observe both lawful and unlawful activities taking place in the house, which made the use of the device an illegal search.

In examining sense-enhancing technology based on the type of technology used, it does not appear that the courts have reached a consensus as to when the use of specific types of technology will constitute a search. Most courts have held that the use of drug-sniffing dogs does not constitute a search, though a minority have held the reverse under certain circumstances, noting that that the canine nose is able to smell things a police officer's nose cannot.[76] One area in particular where courts have come out on both sides of the issue is the use of beepers or global positioning technology to track criminal suspects.[77] In cases where the warrantless use of this sense-enhancing technology has been upheld, courts usually base their reasoning on the fact that the defendants were traveling on public streets and could have been monitored by visual surveillance, and thus had knowingly exposed themselves to public scrutiny.[78]

Other courts, however, have not accepted that argument. In *State v.*

---

[72] *Id.* at 34.

[73] *See id.*

[74] *See* Illinois v. Caballes, 543 U.S. 405 (2005).

[75] James Fisher, *What Price Does Society Have to Pay for Security? A Look At the Aviation Watch Lists*, 44 WILLAMETTE L. REV. 573, 596 (2008).

[76] *Compare* United States v. Place, 462 U.S. 696 (1983) *with* People v. Evans, 65 Cal. App. 3d 924 (1977) (holding that the use of drug-sniffing dogs during a traffic stop was a violation of the defendant's Fourth Amendment rights).

[77] *Compare* United States v. Knotts, 460 U.S. 276 (1983) (upholding the warrantless monitoring of a defendant through a beeper in the defendant's car) *with* United States v. Karo, 468 U.S. 705 (1984) (holding that the warrantless monitoring of a defendant through a beeper in a private home was invalid).

[78] *See Knotts*, 460 U.S. at 285 (holding that because the defendant was traveling on public streets and could have been observed through visual surveillance, the warrantless use of a beeper to track the defendant did not violate the defendant's Fourth Amendment rights).

Campbell, the Oregon Supreme Court invalidated the use of a transmitter to track a suspect's movements and rejected the argument that electronic surveillance is no different than visual surveillance, emphasizing that "any device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom."[79] The *Campbell* court criticized the state's argument that the transmitter was "simply a device for 'enhancing' visual observation in the manner of moderate power binoculars or camera lenses."[80] Specifically, the court cited the state's own assertion that the use of this transmitter was necessary to track the defendant because police were unable to follow him through traditional visual surveillance.[81] In fact, it was only by using the transmitter that the police were able to find the defendant's automobile "some forty miles from where they expected to find it" and were able to do so without using traditional tracking methods, like "looking for footprints, broken branches, etc."[82] Thus, in *Campbell*, the court held that just because information is "legitimately available" through one means does not imply it can be "obtained through any other means without engaging in a search."[83]

As technology is continually evolving, this area of law is in a constant state of flux. Based on current case law, however, it is unclear whether a MALINTENT scan would be considered a search or not. If one looks at the case law emerging from courts, considering the use of beepers or global positioning technology, one may find that MALINTENT scans are likely searches as the scans may reveal health information that falls within an individuals' objectively reasonable expectation of privacy, an argument that mirrors the court's reasoning in *Kyllo*. Similarly, it is unclear whether the MALINTENT system simply enhances the senses a person possesses or replaces them, another issue that may affect the legality of the technology in question. Because MALINTENT records minute biometric responses and measures them against each other, it seems unlikely that a person would be able to collect this type of data, or at least interpret it, without the MALINTENT technology. Thus, using similar reasoning to that found in the court's decision in *Campbell*, one may be able to argue that these scans constitute a search as MALINTENT is not simply enhancing a person's senses, but replacing them. This reasoning, however, has not always been judged to be compelling by most courts as a clear majority has held that the use of drug-sniffing dogs, which may be able to smell things humans cannot (thereby

[79] *See* State v. Campbell, 306 Or. 157, 171-72 (1988).

[80] *Id.* at 166.

[81] *See id.*

[82] *Id.*

[83] *Id.*

replacing one's sense of smell), is not a search.

In contrast, one may also argue that because many of the biometric factors measured by MALINTENT can be observed visually, these scans are really just enhancing what the naked eye can perceive and thus do not constitute a search. This claim is based largely on the reasoning that if an individual knowingly exposes certain traits to the public, like the sound of the individual's voice, law enforcement officials should be able to use technology to analyze those traits. Additionally, the court's decision in *Kyllo* may also support a determination that MALINTENT scans are not a search. It can be argued that much like dog sniffs, MALINTENT scans reveal only illegal intentions, while ignoring lawful ones, and an individual's privacy interests are not impacted by the exposure of illegal intentions. MALINTENT's record of false positives, however, may impact the effectiveness of this last argument.

B. MALINTENT as a Search

If a MALINENT scan is found to constitute a search, one must then consider whether that search is lawful in light of the Fourth Amendment. Under the Fourth Amendment, a warrant is required before police officers can conduct a search and seizure.[84] "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[85] A search and seizure is unlawful only if it is conducted without a warrant and infringes on a person's privacy interest.[86] A privacy interest, however, must be reasonable to earn Fourth Amendment protection and exists only when two requirements are met. First, the petitioner must have a personal, subjective expectation of privacy in the place in question. Second, the expectation of privacy must be one that society wishes to recognize as reasonable.[87] The court will extend a privacy interest only if the interest serves a valuable social goal.[88] One's privacy interest is not tied to a specific location and therefore what a person intends to preserve as private, even in a public area, may be protected by the Fourth Amendment.[89]

1. Privacy Interests

As MALINTENT is designed as a security system, it is nearly certain that a warrant will not accompany most uses of the technology. In the absence of the protections provided by a warrant, it must be determined whether these scans

[84] *See* Katz v. United States, 389 U.S. 347, 357 (1967).

[85] Florida v. Riley, 488 U.S. 445, 462 (1989) (quoting Schmerber v. California, 384 U.S. 757, 767 (1966)).

[86] *See* Minnesota v. Carter, 525 U.S. 83, 88 (1998).

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

[88] *See*, *e.g.*, Minnesota v. Olson, 495 U.S. 91, 99-100 (1990).

[89] *See Katz*, 389 U.S. at 351-52.

violate a personal and socially accepted expectation of privacy. If MALINTENT does violate a person's privacy interests, it constitutes an unlawful search unless it falls under one of the many exceptions to the warrant requirement, which will be discussed later in this section.

Under the first prong of the *Katz* test, a person must possess a subjective privacy interest for a warrantless search to be unlawful.[90] Although a person may not always have a valid privacy interest in those aspects of his person he exposes to the public eye, a valid privacy interest likely exists for much of the biometric information collected by MALINTENT.[91] Information such as heart rate, perspiration rate, and full body scan images may represent data most people would consider "private."[92] Thus, as *Katz* requires a subjective privacy interest, it is highly possible that such an interest is present in many people's minds when they consider medical information. The second prong of the *Katz* test requires a showing that such a privacy interest is one that society is willing to recognize as reasonable.[93] Because the government has enacted many statutes to protect a person's medical data, it is likely that a privacy interest in this area is also objectively reasonable.[94]

For a warrantless search to be invalid, one must show a violation of one's privacy interest. Here, as suggested by the Eleventh Circuit in *United States v. Vega-Barvo*, an invasion of one's privacy interest is typically linked to the intrusiveness of the search in question.[95] Typically, the more intrusive a search, the more reasonable the suspicion must be to justify the search.[96] Internal body searches in particular are considered highly intrusive.[97] The intrusiveness of a search should have a direct correlation to the indignity suffered by one undergoing the search.[98] The *Vega-Barvo* court outlined three factors which can help to measure the indignity created by a search: "(1)

[90] *Id.* at 361.

[91] *See* Whalen v. Roe, 429 U.S. 589, 605 (1977) (requiring the use of safeguards in government databases to protect individuals submitting their health information). This case is one of the first to suggest that there is a right to informational privacy within the Fourth Amendment.

[92] It is important to note that a subjective belief in privacy is not determinative, but is necessary under the *Katz* test.

[93] *See Katz*, 389 U.S. at 361.

[94] One such example is The Freedom of Information Act of 1966, which exempts personally-identifiable health information from public dissemination by the federal government. 5 U.S.C. § 552(b)(6) (2000).

[95] *See* United States v. Vega-Barvo, 729 F.2d 1341, 1344 (11th Cir. 1984).

[96] *See* United States v. Himmelwright, 551 F.2d 991, 995 (5th Cir. 1977).

[97] *See Vega-Barvo*, 729 F.2d at 1345.

[98] *See id.* ("[T]o determine the level of intrusiveness of a search, we must focus on the indignity of the search."); *see also id*. at 1349 (a strip search requires reasonable suspicion based on articulable facts) (citing *Himmelwright*, 551 F.2d at 995).

physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force."[99] Although factors one and three may not directly apply to the way in which a MALINTENT scan is conducted, factor two does represent an important concern because MALINTENT scans visually expose intimate body parts and also expose intimate medical information. According to the *Vega-Barvo* court, the "embarrassment caused by the exposure of intimate body parts is often a determinative factor in the constitutionality of . . . searches."[100] Based on these factors, as well as many people's reasonable belief that their medical information is private, MALINTENT scans may violate a person's privacy interest and represent an invalid search without a warrant.[101]

2. Administrative Search Exception

There are several exceptions to the requirement of a warrant for a lawful search. One such exception, which MALINTENT scans may fall under, are administrative searches. Administrative searches are lawful, warrantless searches that are not held to the same standard of probable cause or reasonable suspicion required for a typical search in an investigation by law enforcement officials.[102] These searches are exempt from the warrant requirement because they are conducted as part of a regulatory scheme with a defined administrative goal, rather than as part of a criminal investigation targeted at a specific individual.[103] For a search to be considered a lawful administrative search, however, the intrusion created by the search must be minimal and the interest served by the search must be both significant and legitimate.[104]

The administrative search exception developed because in certain contexts it may be impractical to require some level of individualized suspicion or warrant to conduct a search.[105] Thus, in these situations, if the government's need for a search or need to gather certain information outweighs a person's privacy interest, the search falls under the administrative search exception.[106] As these types of searches are conducted without individualized suspicion, most courts have held that law enforcement must show circumstances that make developing individual suspicion unfeasible or impractical and that a less

[99] *Id.* at 1346.

[100] *Id.* at 1347.

[101] This assumes the use of MALINTENT technology is found to be a search.

[102] *See* People v. Dukes, 580 N.Y.S.2d 850, 851-52 (Crim. Ct. 1992).

[103] *See* United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973).

[104] *See* Thomas P. Crocker, *Overcoming Necessity: Torture and the State of Constitutional Culture*, 61 SMU L. REV. 221, 266 (2008); *see also Dukes*, 580 N.Y.S.2d at 852.

[105] *See* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665-66 (1989).

[106] *Id.*

restrictive search alternative is not available.[107] Additionally, as these searches do not require a warrant or individualized suspicion, they may be subject to abuse. One way to prevent such abuse is to require procedures to ensure against arbitrary search selections. For this reason, courts must carefully consider, on a case by case basis, the amount of discretion an officer conducting an administrative search possesses.[108] Thus, to uphold an administrative search as valid, courts require a showing that a search resulted due to the application of standardized procedures involving neutral criteria.[109]

In assessing the lawfulness of a proposed administrative search, the court conducts a balancing test in which it weighs the "degree of the intrusion" against the "severity of the danger posed."[110] The "degree of the intrusion" caused by an administrative search is analyzed by evaluating the discretion given to the person conducting the search, the circumstances in which the search takes place, the duration of the search, the presence of possible safeguards to protect a person's privacy and the liberty interest of the person being searched.[111] Furthermore, in its balancing test, the court will also consider the "effectiveness of the procedure used in achieving its stated goal."[112] If a court finds that the risk of danger outweighs the intrusion caused by a search and that the intrusion is both minimal and narrowly circumscribed, the court will likely find that the search is lawful.[113]

One area where administrative searches are often conducted is airports.[114]

---

[107] *See* Delaware v. Prouse, 440 U.S. 648, 654-655 (1979) (citing United States v. Brignoni-Ponce, 422 U.S. 873, 881-83 (1975)); *see also* Nat'l Treasury Employees Union, 489 U.S. at 665-6. *But see* United States v. Martinez-Fuerte, 428 U.S. 543, 557 (1976) (holding the need for a less restrictive alternative did not need to be incorporated into the court's assessment of the validity of an administrative search).

[108] *See* Camara v. Municipal Court, 387 U.S. 523, 532-533 (1967).

[109] *See id.*

[110] People v. Dukes, 580 N.Y.S.2d 850, 852 (Crim. Ct. 1992); *see also Camara*, 387 U.S. at 536-37 (holding under the balancing theory, the court will consider whether the practice at issue has a long history of judicial and public acceptance, is essential to achieve acceptable results and involves a relatively limited invasion of privacy).

[111] *See*, *e.g.*, Crocker, *supra* note 104 at 266; *see also* New Jersey v. T.L.O., 469 U.S. 325, 337-342 (1985); *Prouse*, 440 U.S. at 654-55 (holding that if a search allows an officer to have too much discretion, it is not a valid administrative search).

[112] Gutierrez v. State, 22 S.W.3d 75, 83 n.7 (2000) (citing Brown v. Texas, 443 U.S. 47, 50-51 (1979)).

[113] *See* United States v. Sharpe, 470 U.S. 675, 689 (1985) (Marshall, J., concurring).

[114] It is important to note a difference in the justification for airport searches of those arriving from international flights. As these searches are conducted at national borders, they implicate the national security interest in protection from external, foreign threats. *See* United States v. Ramsey, 431 U.S. 606, 619 (1977). Additionally, Section 482 of the Tariff Act of 1930 gives customs officials the right to conduct searches and seizures at borders

The use of a magnetometer (or x-ray) a person passes through to board a plane has been judged by a majority of courts to constitute a search under the Fourth Amendment.[115] Airport security measures, however, fall under the administrative search doctrine due to their routine nature and absence of arbitrariness, as they are applied to all attempting to travel by air, and because of their very important goal – to "deter potential hijackers from even attempting to bring weapons on a plane."[116] The use of a magnetometer in such a setting is thought by courts to be a minimal intrusion because a magnetometer does not "annoy, frighten or humiliate those who pass through it" even though its use does constitute a search.[117] These types of searches at airports are considered reasonable, however, only if the search is "no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives and . . . is confined in good faith to that purpose."[118] Another factor which supports the lawfulness of these searches is that most travelers have advance warning that searches of these types will occur.[119]

Although courthouses face different security risks than airplanes, courts assessing the constitutionality of security measures in courthouses have found that protecting the public from risks of violence in government buildings is also a "compelling governmental interest."[120] Thus, some courts have upheld the use of "blanket suspicionless searches calibrated to the [potential] risk" at the entrances to courts and certain government buildings.[121] In finding such searches permissible, courts have cited the purpose of these administrative searches, which is to "locate and retrieve any weapons or other items that

where they suspect the carrying of merchandise subject to duty or imported contrary to law. 19 U.S.C.S. § 482 (2002).

[115] *See* United States v. Albarado, 495 F.2d 799, 806 (2d Cir. 1974); *see also* People v. Firtschler, 364 N.Y.S.2d 801, 805-06 (Sup. Ct. 1975) (holding that the use of x-ray technology constitutes a search under the Fourth Amendment because the machine's primary purpose is to locate items where there is normally an expectation of privacy).

[116] *Albarado*, 495 F.2d at 804 (holding that although airport searches sometimes lead to the discovery of contraband that the searches were not invented to discover, that does not affect the administrative nature of the searches or their constitutionality).

[117] *Id.* at 806.

[118] United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007) (citing United States v. Davis, 482 F.2d 893, 913 (9th Cir. 1973)).

[119] *See, e.g.*, United States v. Edwards, 498 F.2d 496, 499, 501 (2d Cir. 1974).

[120] People v. Rincon, 177 A.D.2d 125, 127 (N.Y. App. Div. 1992).

[121] Chandler v. Miller, 520 U.S. 305, 323 (1997); *see also* Legal Aid Society of Orange County v. Crosson, 784 F. Supp. 1127, 1130 (S.D.N.Y. 1992) (holding that the limited warrantless searches of individuals entering government buildings is lawful as long as it is "part of a general practice and not for the purpose of securing evidence for criminal investigations.").

would pose a danger to others," rather than to gather evidence for a criminal investigation, as a determinative factor.[122]

If MALINTENT scans are found to be searches, this exception to the warrant requirement is the most compelling argument for the scan's validity. In examining the MALINTENT technology in terms of the factors outlined in the aforementioned balancing test, it seems likely that a court would find this technology falls under the administrative search exception. MALINTENT technology is designed to be exceptionally fast, which removes any concern over the duration of the scans. Additionally, MALINTENT technology is designed to function much like current security measures at airports: every building entrant must walk through the MALINTENT portal to enter a building, which removes any concern over arbitrariness or abuse of discretion. Similarly, as the scanning sensors move over the exterior of the body and any information gathered about an entrant that is not flagged by the computer system is destroyed, it does not seem that this technology qualifies as overly intrusive in the face of the compelling government interest in preventing terrorist attacks and other crimes. Based on the above analysis, it is likely that MALINTENT scans would be allowed under the administrative search exception in certain forums.[123]

3. Consent-Based Searches

It is also possible that MALINTENT scans will fall under the consent exception to the warrant requirement. If a person consents to a search, law enforcement officials are not required to obtain a warrant to continue with the search.[124] In past cases, the government has relied on this argument, in addition to the administrative search exception, to justify the presence of magnetometers at airport security checkpoints.[125] In cases examining the lawfulness of airport security measures, the government has typically reasoned that in making the decision to fly, an individual is consenting to the accompanying security measures and the presence of such measures should not

[122] People v. Spalding, 776 N.Y.S.2d 765, 769 (Crim. Ct. 2004).

[123] This technology may be allowed at public buildings or public events where the government has a compelling need to enact stringent safety measures. But, it is doubtful such a need would be found at most private institutions, and thus unlikely that the administrative search exception would justify the use of MALINTENT technology there.

[124] *See* Florida v. Bostick, 501 U.S. 429, 438 (1991).

[125] *See, e.g.*, United States v. Edwards, 498 F.2d 496, 501; *but see* United States v. Ruiz-Estrella, 481 F.2d. 723, 727, 728-29 (2d Cir. 1973) (evidence that defendant was unaware of his right to refuse consent by not boarding a flight is probative in determining whether consent to the search was freely given; lack of explicit communication of passengers' freedom to leave if they do not wish to be searched is relevant evidence).

come as a surprise.[126] Thus, if a person does not want to submit to these security measures, he or she can choose other modes of transportation.[127]

Consent alone, however, is not enough. The court must also find that that consent is voluntary, which is largely a question of fact to be determined by "the totality of all circumstances."[128] Knowledge of the right to refuse is typically one factor that is considered in determining whether consent was voluntary, but it is not necessarily determinative of voluntary consent.[129] Additionally, not every court has found consent to be a valid justification for magnetometer searches. In *United States v. Albarado*, the Second Circuit held that in forcing a traveler to submit to a search in order to use air transportation, that submission is the product of coercion and does not constitute implied consent.[130] The approach used by the *Albarado* court, however, is not commonly endorsed in cases of this nature.

A similar consent argument was used to justify magnetometer searches in court houses. In *Gibson v. Texas*, Gibson, an attorney, argued that the security measures at his local court house violated his Fourth Amendment rights because he was forced to submit to the security measures or give up the practice of law.[131] Although the Texas court found that in entering the court house Gibson consented to the searches, the court held that Gibson's consent was "qualified" or constituted implied consent.[132] In its analysis of the legality of Gibson's implied consent, the court considered such factors as:

> notice of the impending search; voluntary conduct in consenting to the search; [whether] the search was justified by a vital interest; [whether] the search was reasonably effective in securing the interests at stake; [whether] the search was only as intrusive as necessary to further the interests justifying the search; and [whether] the search curtailed the unbridled discretion in the searching officers.[133]

---

[126] *See Edwards*, 498 F.2d at 501; *see also Spalding*, 776 N.Y.S.2d at 770 (the presence of magnetometers at the airports constitutes adequate notice to individuals of an impending search if they choose to travel by air, and they may walk away if they do not consent to such search).

[127] *See* United States v. Davis, 482 F.2d 893, 913 n.59*; see also Spalding*, 776 N.Y.S.2d at 770.

[128] *Edwards*, 498 F.2d at 504 (Oakes, J., concurring) (citing Schneckloth v. Bustamonte, 412 U.S. 218, 223 (1973)).

[129] *See Schneckloth*, 412 U.S.at 249 (holding that consent was given voluntarily even absent a showing of actual knowledge of the right to refuse consent).

[130] *See* United States v. Albarado, 495 F.2d 799, 806-07 (2d. Cir. 1974); *see also* United States v. Kroll, 481 F.2d 884, 886 (8th Cir. 1973).

[131] *See* Gibson v. Texas, 921 S.W.2d 747, 756 (Tex. App. 1996).

[132] *Id.* at 757.

[133] *Id.* at 758.

In its analysis, the *Gibson* court cited in particular "the high social value that society properly attaches to assuring that a courthouse is a place in which rational reflection and disinterested judgment will not be disrupted by intimations of violence" in finding that Gibson gave qualified consent.[134]

It is likely that the use of MALINTENT scans is justified under the theory of qualified or implicit consent. In most situations, building entrants will likely have advance warning of MALINTENT scans or see the scanning portals upon entering a building. Thus, an entrant's decision to proceed into the building and through the portals could represent consent to the scans, as long as such consent was shown to be voluntary. Additionally, as MALINTENT portals will likely be used as part of a security screening process in public buildings, the scans serve a "vital interest" and are a part of a routine practice, both of which are factors that weigh in favor of the legality of consent according to the *Gibson* court. The only possible problem with using consent to establish the legality of MALINTENT scans involves constitutional issues. It is possible that one could argue consent is coerced in these situations as a person must choose between his or her constitutional right to privacy and another constitutional right, such as freedom to travel or a right to a trial, as one must pass through these scanners to board a plane or enter a courtroom. This argument has not been successful in regards to the use of magnetometers and x-rays at airports. It is therefore doubtful such an argument could prevent the use of MALINTENT scans.

C. MALINTENT as an Investigatory Stop

It is possible, based largely on some of the arguments outlined above, to argue that MALINTENT does not constitute a search within the meaning of the Fourth Amendment. If MALINTENT does not qualify as a search, it is likely that it does qualify as an investigatory stop. One must then evaluate whether an investigatory stop of this nature is constitutional.[135]

The elements of a constitutionally valid investigatory stop were defined in 1968 by the Court in *Terry v. Ohio*.[136] In *Terry*, the Supreme Court held that the Fourth Amendment's prohibition on unreasonable search and seizure is not violated when a police officer briefly stops a suspect and searches him as long

---

[134] *Id.* at 759 (citing Ryan v. County of DuPage, 45 F.3d 1090, 1095 (7th Cir. 1995)); *see also* Downing v. Kunzig, 454 F.2d. 1230, 1232 (6th Cir. 1972) (holding that due to outbreaks of violence in government buildings the state has a valid interest in providing security measures to ensure the safety of employees and the public in government buildings).

[135] *See* U.S. CONST. amend. IV.

[136] *See* Terry v. Ohio, 392 U.S. 1, 34 (1968) (White, J., concurring) (nothing in the constitution prevents a police officer from stopping a suspect in a public place and asking him questions).

as the officer has reasonable suspicion that the suspect has committed or is about to commit a crime.[137] Thus, a *Terry* stop is neither a search nor a seizure, but an initial investigatory stop. The *Terry* court established that the reasonable suspicion necessary for a valid investigatory stop must be based on "specific and articulable facts that, taken together with rational inferences from those facts" justify the intrusion caused by the stop.[138] The inquiry is one into the "totality of the circumstances" in each case.[139] Under *Terry*, to determine whether reasonable suspicion existed at the time of the stop, courts must evaluate the reasonableness of an investigatory stop "in light of the particular circumstances" surrounding the stop.[140] Reasonable suspicion is a less demanding standard than probable cause, but requires, at its minimum, that an objective justification exists for stopping a particular individual.[141] The objective existence of reasonable suspicion is most typically evidenced through the officer's knowledge that a crime has been committed and his personal observations.[142] This standard prevents police officers from stopping suspects based on an "inchoate and unparticularized suspicion or 'hunch.'"[143] The Court's decision in *Terry* is based largely on the recognition that a balance needs to exist between an individual's right to be free from unreasonable search and seizure and the interests of law enforcement officers, both in terms of an officer's safety in the line of duty as well as an officer's need to deescalate a situation and obtain relevant evidence.[144]

If an investigatory stop is valid under the standards established in *Terry*, an

---

[137] *Id.* at 31.

[138] *Id.* at 21; *see also* United States v. Elmore, 482 F.3d 172, 183 (2d Cir. 2007) (finding an investigatory stop valid because the use of an informant created reasonable suspicion); United States v. Atchley, 474 F.3d 840, 848-49 (6th Cir. 2007) (finding an investigatory stop valid because the informant's tip, and the defendant's nervous behavior and apparent lies when police questioned him, created reasonable suspicion); United States v. Samuels, 493 F.3d 1187, 1192-93 (10th Cir. 2007) (finding an investigatory stop valid because a reliable informant's tip and subsequent observations by the officer of behavior consistent with drug buy created reasonable suspicion); United States v. Martinez, 486 F.3d 855, 862, 863 (5th Cir. 2007) (holding an investigatory stop was not valid because the government did not show the informant was reliable and officers did not verify allegations of criminal activity, so there was no evidence supporting a reasonable suspicion).

[139] *See Elmore*, 482 F.3d at 183; *see also Atchley*, 474 F.3d at 848-49.

[140] *Terry*, 392 U.S. at 21.

[141] *See Warrantless Searches and Seizure*, 37 GEO. L.J. ANN. REV. CRIM. PROC. 39, 42-43 (2008); *see also* Illinois v. Wardlow, 528 U.S. 119, 123 (2000).

[142] *See Terry*, 392 U.S. at 21-22 (under the objective standard, one must determine whether the police officer's observations and knowledge warrant a reasonable belief that an investigative stop is appropriate).

[143] *Id.* at 26.

[144] *Id.* at 21-22.

officer is also allowed to conduct a limited pat-frisk of the person stopped.[145] The pat-frisk, however, is restricted in scope and must be confined to what is reasonably necessary to discover weapons.[146] If an officer happens to find contraband on a lawfully stopped person while conducting a frisk, however, the officer is not compelled to ignore that contraband.[147]

The procedures associated with the use of the MALINTENT system may constitute an investigatory stop. MALINTENT aids security personnel by flagging building or event entrants that may intend to commit violence in certain venues. If MALINTENT operators decide after both an initial and secondary MALINTENT scan that an individual poses a security threat, that person is pulled aside for further questioning.[148] If MALINTENT screens constitute an investigatory stop, one must consider whether the results of the scan establish the requisite reasonable suspicion for a valid investigatory stop under *Terry*.

MALINTENT's scanning portal is comparable to metal detectors commonly used at airports and other facilities for purposes of determining how the results of such scans affect an articulable suspicion analysis. In *United States v. Epperson*, the defendant attempted to bring a concealed weapon onto an airplane.[149] A United States Marshal found the weapon after Epperson walked through a metal detector and the detector gave an abnormal reading.[150] Before his trial, Epperson moved to have the gun excluded by claiming that the metal detector constituted an unreasonable search under the Fourth Amendment because the search was made without a warrant.[151] The Fourth Circuit found that the passing through the metal detector constituted a warrantless search, but held the search to be reasonable under the *Terry* stop exception.[152] In reaching this decision, the *Epperson* court relied largely on the reasoning used in *Terry* to justify the creation of the *Terry* stop exception to the warrant requirement for a search.[153] Specifically, the *Epperson* court cited the *Terry* Court's

---

[145] *See id.* at 31 (Harlan, J., concurring).

[146] *Id.* at 31-32; *see also* Sibron v. New York, 392 U.S. 40, 65 (1968) (holding that an officer exceeded the scope of such a pat-frisk in that he made "no attempt at an initial limited exploration for arms" but instead "thrust his hand into Sibron's pocket").

[147] *See* Michigan v. Long, 463 U.S. 1032, 1050 (1983).

[148] *See* Barrie, *supra* note 6.

[149] United States v. Epperson, 454 F.2d 769, 770 (4th Cir. 1972).

[150] *Id.*

[151] *Id.*

[152] *Id.* ("[T]hat is the very purpose and function of a magnetometer: to search for metal and disclose its presence in areas where there is a normal expectation of privacy."); *id.* at 772 (referencing Terry v. Ohio, 392 U.S. 1 (1968)).

[153] *See id.* at 771 (referencing *Terry*, 392 U.S.); *see also* United States v. Davis, 482 F.2d 893, 905-06 n.32 (1973) (where the court, in evaluating airport search cases, stated that

conclusion that the *Terry* stop exception was necessary to ensure the protection of officers from concealed weapons and that such protection could extend to others in danger as well.[154]

There are two major concerns with classifying scans, like magnetometer scans, as *Terry* stops. First, as established earlier in this Note, most courts consider these types of scans to be searches that are justified under either the consent or administrative exceptions to the warrant requirement.[155] Second, observing an individual setting off a metal detector lacks a major requirement of a *Terry* stop: particularized, reasonable suspicion.[156] As the officer only had a brief opportunity to observe the suspect in *Epperson*, there was likely not enough time for the officer to determine particularized suspicion that the defendant might be attempting to commit a crime. Instead, the officer's only knowledge about the defendant was that the defendant set off the metal detector, which does not immediately suggest criminal activity per se. Epperson's criminal intentions did not become apparent until after an additional "search" was performed. Thus, the argument can be made that the results of magnetometer scans do not provide enough information to form the particularized basis for reasonable suspicion necessary for a *Terry* stop.

It can be further argued that MALINENT scan results are even less likely to provide the reasonable suspicion necessary for a valid *Terry* stop than the results of a magnetometer scan. For one, although metal detectors can be set off for benign reasons, in theory, metal detector scans are designed only to seek out weapons. MALINTENT scans, however, are designed to record biometric data. It is only when all the data is analyzed together that a person may be flagged based on his or her results, and asked to submit to a second scan or questioning. And similar to metal detectors, MALINTENT scans too can be set off for completely benign reasons and are currently running only at a seventy-eight percent accuracy level. Even then, the scan reveals only the possibility of criminal intentions, rather than suggesting the person in question is carrying a weapon or a bomb. Thus, it may be more likely that the results of a magnetometer scan, which provide concrete evidence that a person possesses a concealed, unidentified metal object, creates a higher level of reasonable suspicion than measuring a person's biometric responses to control questions.

"[m]ost . . . have relied upon *Terry*'s stop-and-frisk rationale or general 'reasonableness' to uphold searches (including magnetometer scanning) of either the prospective passenger's person, or his carry-on luggage . . .").

[154] *See Epperson*, 454 F.2d at 770-71 (citing *Terry*, 392 U.S. at 27).

[155] *See supra* Part III.B.ii.; *see also* United States v. Haynie, 637 F.2d 227, 230 (4th Cir. 1980) (holding that the use of x-ray devices to reveal the shape of object inside a package constituted a search within the meaning of the Fourth Amendment).

[156] *See* United States. v. Arvizu, 534 U.S. 266, 273 (2002) (court must determine whether an officer has a "particularized and objective basis" for reasonable suspicion for a lawful investigatory stop).

One must also consider whether using MALINTENT scans to justify investigatory stops provides the requisite objective and particularized basis for reasonable suspicion. Here, although biometric information gathered by a scan is analyzed by a computer, the final decision on whether to flag an individual belongs to a security analyst, which introduces a subjective element into these stops. Additionally, many of the factors typically used to argue that a stop is "objective" in traditional *Terry* stop cases are not present here: scanners are not directly observing suspicious behavior, only physiological responses to control questions, and no crime has yet been committed to put an individual's behavior into context. Similarly, it is doubtful that the suspicion generated by a MALINTENT scan is truly particularized. Limited information is available on the protocol used to flag individuals and how certain health conditions will affect the accuracy of the scans. Thus, if someone with a disorder like asthma is always going to be flagged based on their biometric responses, can these scans really be considered to result in particularized suspicion? And finally, it is unlikely that the biometric aspects of these scans could be used to justify a frisk during a *Terry* stop. As discussed above, frisks are only allowed during these investigatory stops so that an officer can ensure his or her safety, and in some contexts, the safety of those around him by determining whether the stopped person has a weapon.[157] Here, if only a person's physiological responses suggest that he or she might have some sort of criminal intentions, it is unlikely that an officer would be justified in conducting a pat-frisk. Thus, setting off a scan on the basis of one's biometric responses, which could be completely benign and do not necessarily pose a direct risk, should not constitute the same amount of reasonable suspicion as setting off a metal detector because one is carrying an unidentified metal object, which could be a weapon.

Furthermore, although most cases involving the use of scanning technology similar to MALINTENT arise out of scans that have occurred at airports, there are certain special considerations that are involved in airport security that may not carry over into other forums. Airports are distinctive because if a person is able to get a bomb or gun past airport security, that person is uniquely positioned to harm a large number of people.[158] Thus, in the face of such danger, most searches will be found to be reasonable as long as they are

[157] *See Terry*, 392 U.S. at 31-32 (Harlan, J., concurring).

[158] *See* United States v. Bell, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, C.J., concurring) ("When the risk is the jeopardy of hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplanes, the danger *alone* meets the test of reasonableness, so long as the search is conducted in good faith for the purpose of preventing hijacking or like damage and with reasonable scope and the passenger has been given advance notice of his liability to such a search so that he can avoid it by choosing not to travel by air.").

conducted in good faith and are no more intensive than necessary to detect weapons or explosives.[159] In support of this idea, the court in *Epperson* found the stop and search valid under the *Terry* analysis only because its purpose was for "discovering weapons and preventing air piracy," and not for "discovering weapons and precriminal events."[160] In addition to the *Epperson* court, at least one other court observed that "[a]t this point in time when airplane hijacking is at a crisis level, such an expectation, to be free from the limited intrusion brought about by the screening process utilized in the boarding area of the airports, is not justifiable under the circumstances."[161]

In attempting to understand where MALINTENT scans fall within the standards set out by the *Terry* Court, it is also helpful to examine investigatory stops in the context of sobriety checkpoints. Much like a traditional stop and frisk, sobriety checkpoints aim to discover and apprehend those committing a crime, which in this case is the crime of driving while intoxicated. In assessing whether a sobriety checkpoint is lawful, courts have turned to a balancing test established in *Brown v. Texas*.[162] Under the three-prong test used by the Court in *Brown*, to determine whether a checkpoint stop was lawful a court must balance the state's interest in preventing accidents caused by drunk drivers, the effectiveness of sobriety checkpoints in achieving that goal, and the level of intrusion on an individual's privacy caused by the checkpoint.[163]

In determining the intrusion on a person's privacy and liberty caused by a sobriety checkpoint, courts look at several factors. One such factor is the duration of the stop and the level of investigation that occurs during the stop.[164] There are no bright-line rules, however, to measure the appropriateness of a stop's length or the level of investigation involved, which has resulted in differing interpretations of this factor's application.[165] Courts will also consider the manner in which a sobriety checkpoint is conducted. To be lawful, sobriety checkpoints must be conducted in a manner designed to eliminate arbitrary selection of motorists and to minimize causing anxiety or fright among motorists.[166] Thus, it is important that these checkpoints are conducted by police officers in uniform so that motorists are able to recognize

---

[159] *See id.; see also* United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007) (quoting United States v. Davis,482 F.2d 893, 913 (9th Cir. 1973)).

[160] United States v. Epperson, 454 F.2d 769, 771 (4th Cir. 1972).

[161] Shapiro v. State, 390 So. 2d 344, 347 (Fla. 1980).

[162] *See* Brown v. Texas, 443 U.S. 47, 50 (1979).

[163] *See id.* at 50-51*; see also* Illinois v. Lidster, 540 U.S. 419, 427 (2004) (quoting *Brown*, 443 U.S.).

[164] *See* Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 452 (1990).

[165] *See id.*

[166] *See id.* at 452-53 (noting that sobriety checkpoints are thought to be better than roving patrols which are subjective and generate fright).

a visible sign of authority, so as to minimize alarm.[167] Additionally, arbitrary selection is thought to be removed from the process by establishing rules that require either the stopping of all motorists or the selection of motorists to stop based on neutral criteria. Finally, the location and timing chosen for a checkpoint must be selected in a regularized manner and some courts require advance notice of the checkpoints.[168] In assessing checkpoints in general, police officers must be sure to select a valid, objective purpose for their checkpoints. Often, if officers attempt to use a single roadblock for multiple purposes, the court will consider it overly intrusive and thus unlawful under the Fourth Amendment.[169]

Many of the factors that must be present for a lawful sobriety checkpoint are also present for initial MALINTENT scans. Locations will likely be chosen for these portals based on a special need for security at such locations, like sports arenas. Although individuals may not receive advance notice of the portal's placement, it is likely that upon entering a building a person will see the portals, much like a person is able to see a magnetometer, and then has the choice to continue into the building or leave. Furthermore, as each person entering the building will have to submit to a scan, it ensures there is no arbitrary selection of individuals for the initial scans and based on MALINTENT's creators' statements, the scans should take only two to four minutes. Finally, as MALINTENT scans will likely be conducted by security personnel, there will probably be a similar showing of authority as there is at sobriety checkpoints, which will minimize any fear an individual might experience upon seeing the portals. The only factor which may prove problematic is the intensity of the search, as some people may consider MALINTENT scans to be highly intrusive, while others may not.

In applying the *Brown* balancing test, many courts have found that intrusions on a person's liberty and privacy interests caused by the checkpoint are minimal as the stops are typically brief and the related investigation is of negligible intensity.[170] However, if an officer wants to conduct more extensive field sobriety test, the officer likely needs the level of reasonable suspicion also necessary for a valid *Terry* stop to do so.[171] This poses an interesting parallel that must be kept in mind in analyzing MALINTENT scans. Though, like sobriety checkpoints, the initial scan may be lawful due to its short duration, generally minimal intrusion, and the manner in which it is conducted, to warrant a second scan, much like additional field sobriety tests, an officer must

[167] *See id.*

[168] *See* Orr v. People, 803 P.2d 509, 512 (Colo. 1990); *see also* People v. Rister 803 P.2d 483, 485 (Colo. 1990); State v. Garcia, 500 N.E.2d 158, 161 (Ind. 1986).

[169] *See* State v. DeBooy, 996 P.2d 546, 551 (Utah 2000).

[170] *See Sitz*, 496 U.S. at 451-52.

[171] *See id.* at 451.

have reasonable suspicion that the person in question has committed or will commit a crime. As established above, although the initial MALINTENT scans may be lawful, it is not yet clear whether an elevated heart rate, respiration rate and perspiration level, even when evaluated together, will provide a strong enough basis to establish objectively reasonable suspicion for additional scanning and questioning.

D. MALINTENT as a Seizure

MALINTENT technology also raises concerns regarding whether the results of a MALINTENT scan constitute probable cause for a constitutionally valid seizure. If a building entrant is flagged by a MALINTENT analyst, it is likely that that entrant will be asked, or forced, to submit to an additional and possibly more invasive scan as well as questioning by security guards. It is at this point one must decide whether the second scan or questioning constitutes an investigatory stop, which is valid on the basis of reasonable suspicion, or a seizure, which requires the presence of probable cause to be lawful.[172] Although a stop may initially meet the criteria of a valid investigatory stop, an investigatory stop turns into a seizure when a reasonable person would not feel free to terminate an encounter with the police.[173]

Before determining whether a seizure is lawful, one must first establish if a seizure has transpired. In this case, whether or not additional MALINTENT scans or the questioning of flagged individuals represents a seizure depends largely on how the MALINTENT screening process is put into practice by DHS. Of particular concern will be how operators approach an individual who has been flagged by analysts and attempt to convince that individual to submit to questioning. If building entrants are asked, and not forced, to accompany MALINTENT operators or security guards for questioning, case law suggests a court may not find that a seizure occurred because the entrants have voluntarily submitted to the questioning.[174] Even then, however, a court would have to examine the circumstances closely to definitively determine whether an individual could interpret an operator's actions to be an order, which then suggests any further scanning or questioning is a seizure.[175] Upon certain

---

[172] *See*, *e.g.*, Terry v. Ohio, 392 U.S. 1, 25-26 (1968); *see also* United States v. Quinn, 815 F.2d 153, 156 (1st Cir. 1987).

[173] *See* United States. v. Wallace, 429 F.3d 969, 974 (10th Cir. 2005) (no seizure occurred when an officer questioned the driver because there was no show of authority that would indicate to a reasonable person that he was not free to leave); *see also* United States v. Swindle, 407 F.3d 562, 572-73 (2d Cir. 2005) (driver was not "seized" when police officers activated patrol car lights, even if a reasonable person would feel obligated to pull over, because there was no physical force preventing him from continuing).

[174] *See* United States v. Mendenhall, 446 U.S. 544, 555-56 (1980).

[175] *See id.* at 554-55.

shows of authority, even when a person is asked to voluntarily follow a police officer's request, the particulars of the situation may suggest that a reasonable person would not feel free to refuse the request.[176] If a person does not feel free to refuse such a request, a seizure has likely occurred.[177]

Courts will also consider the location where additional questioning or scanning takes place in determining whether a seizure has occurred. If the questioning takes place in another, public part of the building, rather than an isolated room, the court may find that a seizure has not occurred.[178] Conversely, if an individual is asked to accompany security guards to a private area of the building for questioning, it is highly possible that individuals will feel that they have no choice but to comply and the circumstances may indicate a de facto arrest, and thus a seizure, has occurred.[179] The fact that such a request for additional questioning is made in a building where free movement is generally restricted is not enough to transform a stop into a seizure.[180]

If the court does find that a seizure occurred, it must then determine whether the seizure was lawful. For a seizure to be lawful, probable cause must exist for the seizure.[181] Probable cause is the amount of information that would warrant a prudent person's belief that the defendant committed a crime.[182] The probable cause necessary for a valid seizure must satisfy the same standard of proof required to make a lawful arrest.[183] If, based on a factual analysis of the circumstances, a court finds that a seizure has occurred without probable cause, any evidence obtained from that seizure would not be admissible in a court proceeding.[184] Absent a warrant, information gathered from a seizure is considered "fruit of the poisonous tree" and is not admissible in further legal action.[185]

Here, it is unlikely that a second scan of a person flagged by MALINTENT

---

[176] *See* United States v. Faulkner, 450 F.3d 466, 470 (9th Cir. 2006) (seizure occurred when a forest ranger stopped the defendant's vehicle at checkpoint because a reasonable person would not have felt free to leave due to show of authority through uniform, firearm, official government vehicle, stop sign, and orange cones).

[177] *See id.*

[178] *See* United States v. Williams, 365 F.3d 399, 404-05 (5th Cir. 2004).

[179] *See* United States v. Zapata, 18 F.3d 971, 975 (1st Cir. 1994) (quoting Berkemer v. McCarty, 468 U.S. 420, 441 (1984) in discussing de facto arrests).

[180] *See* United States v. Smith, 423 F.3d 25, 30-31 (1st Cir. 2005) (no seizure occurred when officers requested a man's identification and the physical environment may have restricted his freedom of movement).

[181] *See* Terry v. Ohio, 392 U.S. 1, 37 (1968).

[182] *See* Draper v. United States, 358 U.S. 307, 339 (1959).

[183] *See* United States v. Quinn, 815 F.2d 153, 156 (1st Cir. 1987).

[184] *See* United States v. Mosley, 454 F.3d 249, 269 (3d Cir. 2006).

[185] *Id.*

constitutes a seizure. Even if it does, it is unlikely that a court would find that seizure to be unlawful. Individuals who set off metal detectors are usually compelled to submit to a second scan using a hand-held metal detector, which courts have found either to be a valid search and seizure or a valid *Terry* stop.[186]

Possible seizure concerns are raised, however, when an individual who is flagged by a MALINTENT scan is asked to submit to additional questioning. It is unclear whether the results of the MALINTENT scan would constitute probable cause for a seizure, if asking a flagged individual to submit to further questioning does in fact constitute a seizure. Such an analysis must be applied in a case by case manner as a person's individualized reaction to MALINTENT personnel can greatly affect a court's analysis as to whether probable cause for a seizure existed.[187] Generally, however, this inquiry must involve an assessment of how new technology will be used in a probable cause analysis to determine the validity of a seizure. As MALINTENT scans are currently only running at about seventy-eight percent accuracy in detecting criminal intentions, it is unlikely that, were a seizure to occur, the results of a MALINTENT scan, without more, would constitute probable cause to validate the seizure.[188]

Without further testing of the MALINTENT technology and the science of biometrics in this context, it would be difficult to argue that the results of this scan provide the concrete proof necessary for probable cause. Additionally, in the interest of national security, the government has provided a limited amount of information about MALINTENT so as to avoid manipulation of its system. Although computers analyze an individual's biometric data, the final decision on whether to flag someone rests in the hands of security analysts operating the system. Without information about the protocol followed in choosing which individuals to flag for further scanning or questioning, one cannot eliminate the

[186] *See* United States v. Bui, 15 F.3d 1090, No. 92-50566, 1994 WL 6609 (9th Cir. Jan 10,1994); *see also* United States v. Davis, 482 F.2d 893, 912 (9th Cir. 1973) (warrantless airport security checks are valid administrative searches, so long as they are limited to searches for guns, explosives, or other dangerous devices that may jeopardize airport safety).

[187] *See* Kolender v. Lawson, 461 U.S. 352, 366 n.4 (1983) (Brennan, J., concurring) ("[S]ome reactions by individuals to a properly limited *Terry* encounter, . . . such as flight, may often provide the necessary information, in addition to that which the officers already possess, to constitute probable cause.").

[188] *See* Florida v. Royer, 460 U.S. 491, 499 (1983) (in investigating a person who is "no more than suspected of criminal activity, the police may not . . . seek to verify their suspicions by means that approach the conditions of arrest"). In *Royer*, the defendant was brought into a separate room for questioning, believed he was being detained, and had his luggage and identification seized, all of which the court found to constitute a de facto arrest. *Id.*

possibility of subjectivity in choosing which individuals to flag. This weakens the argument in favor of probable cause on the basis of these scans. Thus, in determining which building entrants to question, MALINTENT is not directly comparable to metal detectors, which provide objective data that a person is carrying a concealed, unidentified metal object, providing a stronger basis for arguing that further questioning or scanning of the individual is necessary.

IV. CONCLUSIONS

MALINTENT technology is a combination of traditional security screening techniques and the latest scientific advances in the area of biometrics. When DHS places MALINTENT portals at select locations, they will represent the first security measure of this type in wide-spread use.[189] As this technology is so novel, few prior court decisions are able to give an accurate idea of how MALINTENT will be assessed under the Fourth Amendment.

It is likely, however, based on reviewing prior court decisions regarding the use of related technology, that MALINTENT will be found to be a search and will be allowed under the administrative search exception to the warrant requirement. Although the way in which MALINTENT scans are conducted is not highly invasive, their results reveal private medical data. The United States' current commitment to protecting an individual's right to keep his or her medical data private suggests that courts will likely find that MALINTENT scans do infringe on a person's privacy interests.[190] Furthermore, as these scans will likely be used in public buildings and areas where there is a vital need to prevent individuals from entering with weapons or criminal intentions, MALINTENT scans seem to fall directly within the administrative search exception.[191]

However, based on the current information released on MALINTENT, if a court were to find that through its use of sense-enhancing technology it did not constitute a search, it is likely that the results of an initial MALINTENT scan would not create the requisite reasonable suspicion necessary for a valid *Terry* stop. Thus, MALINTENT scans are either a search under the administrative exception and are lawful, or, if classified as a non-search, are an unlawful basis for conducting an investigatory stop. This creates an interesting contrast as non-searches are typically thought to be less invasive than traditional searches, and thus infringe less on a person's Fourth Amendment rights. For this reason, there are more stringent protections of personal privacy during searches as

[189] *See* Schwartz, *supra* note 40 (currently, full-body imaging machines, the security measure most comparable to MALINTENT, are only used in nineteen airports in the United States. The Transportation Security Administration has released plans, however, to purchase 150 additional full-body imaging machines.).

[190] *See* The Freedom of Information Act, 5 U.S.C. § 552(b)(6) (2000).

[191] *See* People v. Rincon, 177 A.D.2d 125, 127 (N.Y. App. Div. 1992).

compared to investigatory stops. It is rather ironic that under such a scenario, MALINTENT scans could satisfy the stricter personal protections necessary for a valid search, but not for a *Terry* stop. Furthermore, if MALINTENT scans do not constitute searches, it is highly likely that those scanned by MALINTENT and flagged for additional questioning will have been seized without ever having been searched.

If MALINTENT scans are found to be lawful searches, one must then consider what protocol should be established for their use in order to protect the American people from both terrorists and invasions of their privacy.[192] Although these searches may be valid according to the requirements of the Fourth Amendment, they may also represent a step towards surrendering one's civil liberties for increased national security. For such a tradeoff to be successful, the American people must have "trust and confidence in the government."[193]

One way to establish that level of trust is through the release of information. National security concerns aside, the government needs to make available additional information regarding the accuracy of MALINTENT scans and the way in which information gathered from the scans will be stored and used in criminal proceedings. This will allow both the courts and the American people to make fair determinations regarding the use of this technology.[194] Medical information is thought to be private information and some people may have concerns on how this information will be used and gathered during MALINTENT scans. Additionally, to allude to Orwell's work once more, most people will likely be uncomfortable with the idea that a machine can read their private thoughts and that the results of this machine can be used against them in court. One way to help assuage these fears is through a statute. As the Electronic Communications Privacy Act of 1986 illustrates, Congress can pass statues that regulate nearly every use of technology by law enforcement officials.[195] A statute which lays out the exact procedure for conducting

[192] *See* Fisher, *supra* note 75 at 593 ("[T]he government cannot be allowed to hide behind national security as a means to reach an unconstitutional end. While the government is faced with a monumental task of protecting our nation against an enemy that has blended into American society, the Constitution must still control.").

[193] Timothy M. Ravich, *Is Airline Passenger Profiling Necessary?*, 62 U. MIAMI L. REV. 1, 46 (2007).

[194] Release of information about MALINTENT scans may weaken their effectiveness, but is necessary to ensure that transparent testing is conducted. *See id.* at 36 (noting that national security information that is unknown publicly cannot be tested transparently for its accuracy).

[195] For example, in the Electronic Communications Privacy Act of 1986 (EPCA), Congress established regulations governing the use of pen registers and tap and trace devices by law enforcement officials. Under the regulations listed in the EPCA, the government does not need a warrant in order to use these devices, but does need to obtain a

MALINTENT scans and for the use of the scans' results may help to soothe the public's fear of this technology and ensure a standardized and fair procedure for operating the system so as to maximize protection of an individual's rights. The creation of such a statute is especially important in this context as it is unlikely that a prosecution that hinges on the use of this technology will reach the requisite judicial level to be considered binding precedent on the lawfulness of the MALINTENT technology.

Americans hold dear their rights to privacy and liberty under the Fourth Amendment. That being said, individuals have different opinions on just how much of those rights they are willing to give up in return for greater levels of national security. Although initially MALINTENT scans seem to satisfy the requirements of a lawful search, only actual use of this technology will determine whether this proposition is true. MALINTENT may prove to be the government's most accurate and effective method of preventing terrorism and other crimes. But even in light of that benefit, the American people should still be on guard to ensure encroachments on their personal liberty do not occur. Justice Brandeis captured this best in his opinion in *Olmstead v. United States*:

> [I]t is . . . immaterial that [an] intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[196]

court order, which may be issued on a lesser showing of probable cause needed for a warrant as described by the statute. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511(2)(h)(i) (2008).

[196] Olmstead v. United States, 277 U.S. 438, 479 (1928).