

1-1-2009

The TSA's New X-Ray Vision: The Fourth Amendment Implications of Body-Scan Searches at Domestic Airport Security Checkpoints

Tobias W. Mock

Follow this and additional works at: <http://digitalcommons.law.scu.edu/lawreview>



Part of the [Law Commons](#)

Recommended Citation

Tobias W. Mock, Comment, *The TSA's New X-Ray Vision: The Fourth Amendment Implications of Body-Scan Searches at Domestic Airport Security Checkpoints*, 49 SANTA CLARA L. REV. 213 (2009).

Available at: <http://digitalcommons.law.scu.edu/lawreview/vol49/iss1/5>

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

THE TSA'S NEW X-RAY VISION: THE FOURTH AMENDMENT IMPLICATIONS OF "BODY-SCAN" SEARCHES AT DOMESTIC AIRPORT SECURITY CHECKPOINTS

Tobias W. Mock*

INTRODUCTION

The Transportation Security Administration is currently testing a new form of airport screening technology that renders a virtual naked image of the human body.¹ This so-called "body-scan" technology is earmarked to become the centerpiece of the "checkpoint of the future," replacing walk-through metal detectors as the primary means of detecting personally concealed weapons and contraband.²

The technology is emerging as a result of widespread deficiencies in present-day search capabilities.³ Since the events of September 11, 2001, government accountability auditors have successfully bypassed security checkpoints with

* Technical Editor, *Santa Clara Law Review*, Volume 49; J.D. Candidate, Santa Clara University School of Law, B.S., Boston University. I would like to thank Santa Clara University legal writing instructor Patricia Rauch, and my father, Wayne Mock, for their helpful comments.

1. Leslie Miller, *Feds Want See-Through Security*, CBS NEWS, June 26, 2003, <http://www.cbsnews.com/stories/2003/06/26/tech/main560541.shtml>.

2. *One Year Later: Have TSA Airport Security Checkpoints Improved?: Hearing Before the H. R. Comm. on Oversight and Gov't Reform*, 110th Cong. 9 (2007) (statement of Gregory D. Kutz, Managing Director, and John W. Cooney, Assistant Director, Forensic Audits and Special Investigations, United States Government Accountability Office), [hereinafter *Kutz Testimony*] available at <http://oversight.house.gov/documents/20071114175647.pdf>; Eileen Sullivan, *Full-Body Scan at Airports Could Replace Walk-Through Metal Detectors*, ABC NEWS, Oct. 11, 2007, <http://abcnews.com/US/wireStory?id=3716778>.

3. See OFFICE OF THE INSPECTOR GENERAL, U.S. DEPT. OF HOMELAND SECURITY, OIG NO. 04-37, AUDIT OF PASSENGER AND BAGGAGE SCREENING PROCEDURES AT DOMESTIC AIRPORTS 3-4 (2004) [hereinafter OIG AUDIT], http://www.dhs.gov/xoig/assets/mgmt/rpts/OIG_04-37_0904.pdf.

weapons and explosives at an alarming rate.⁴ While weaknesses exist across all areas of airport security, outdated technology has been identified as a primary culprit, with traditional walk-through metal detectors (magnetometers) leading the way.⁵

Although recognized by government officials as a potential remedy for these failures, the intrusive nature of body-scan technology implicates significant privacy concerns for the millions of domestic airborne travelers.⁶ Accordingly, this comment will attempt to reconcile the competing values of privacy and security in the context of modern-day airport searches, with particular consideration given to the appropriate role, if any, that body-scan technology should play in the future. Whether the technology should be used as a part of the mandatory search procedures that are conducted as a matter of course or as a subsequent search procedure after a passenger elicits a certain degree of suspicion requires careful consideration of the competing interests presented by the technology.⁷

Part I of this comment examines the current state of domestic airport security, including an assessment of current airport checkpoint procedures and capabilities and an introduction to the technology behind body-scan x-rays.⁸ Part II identifies and reconciles the various judicial justifications for airport searches,⁹ while part III identifies the particular Fourth Amendment issue that the technology presents in the context of routine airport searches.¹⁰ Finally, given the judicial framework and particularly invasive nature of the technology, part IV endorses using body-scan searches in the *secondary* search layer as an alternative to pat-down searches; a manner that appropriately considers the competing interests of privacy and security.¹¹

4. See *id.*; see also *Kutz Testimony*, *supra* note 2, at 4.

5. See *OIG AUDIT*, *supra* note 3, at 2.

6. See *id.* at 3, 4 n.5.

7. It is important to note that this comment does not address the specific issue of whether TSA's definition of "arousal of suspicion" is constitutionally justified.

8. See discussion *infra* Part I.A–D.

9. See discussion *infra* Part II.

10. See discussion *infra* Part III.

11. See discussion *infra* Part IV.

I. BACKGROUND: MODERN AIRPORT SECURITY

Domestic airport security has undergone significant transformation since the events of 9/11.¹² Among the many changes include advances in technology, systems, and processes, and an increased focus on accountability.¹³ Despite these measures, it is clear that significant weaknesses persist.¹⁴

While these new technologies and processes develop, courts continue to disagree over how to reconcile the various layers of airport security with the Fourth Amendment protection against unreasonable searches and seizures.¹⁵ Although the plain language of the Fourth Amendment sets forth “reasonableness” as a general benchmark,¹⁶ significant uncertainty exists as to how the government should proceed in implementing new technologies without sacrificing the constitutional rights of American travelers.

A. *The Transportation Security Administration*

Congress acted swiftly to federalize airport security after the 9/11 attacks.¹⁷ The Aviation and Transportation Security Act (the “ATSA”) transferred operational control of airport security from the private sector to the Transportation Security Administration (the “TSA”), an entity created under the ATSA.¹⁸ The ATSA initiated a “fundamental change in the way [the government] approaches the task of ensuring the safety and security of the civil air transportation system.”¹⁹

Since its creation in November 2001,²⁰ the TSA has assumed control of security in at least 315 of the nation’s more than 420 commercial airports, hired and trained a screening workforce,²¹ and deployed thousands of explosive

12. See *United States v. Aukai*, 497 F.3d 955, 960–61, 962 n.6 (9th Cir. 2007).

13. See discussion *infra* Part I.

14. See discussion *infra* Part I.C.

15. See, e.g., *United States v. Hartwell*, 296 F. Supp. 2d 596, 602 (E.D. Pa. 2003), *aff’d*, 436 F.3d 174 (3d Cir. 2006). See generally U.S. CONST. amend. IV.

16. U.S. CONST. amend. IV.

17. OIG AUDIT, *supra* note 3, at 1.

18. *Id.*

19. *United States v. Aukai*, 497 F.3d 955, 960 n.6 (9th Cir. 2007) (quoting H.R. REP. NO. 107-296, at 53–54 (2001) (Conf. Rep.), *reprinted in* 2002 U.S.C.C.A.N. 589, 590).

20. OIG AUDIT, *supra* note 3, at 1.

21. Richard J. Webber, *The Partial Reprivatization of Airport Security*

detection systems and x-ray devices to remedy perceived security weaknesses at airport checkpoints.²² Following the direction of the 9/11 Commission,²³ the TSA seeks to carry out a “layered” security system with a “broad range of interlinked measures that are flexible, mobile, and unpredictable.”²⁴ Although airport security under the TSA is multifaceted,²⁵ checkpoint screening is the primary method of identifying potential threats.²⁶

B. Passenger Screening

The ATSA authorizes mandatory checkpoint screening by the TSA.²⁷ The three primary elements of the passenger screening process are human capital, procedures, and technology.²⁸ Though independent, the three elements are designed to interact with one another to create a comprehensive security system.²⁹

1. Human Capital: Transportation Security Officers

Human capital performs an essential function in the checkpoint screening process. Accordingly, transportation security officers (“TSOs”) are required to complete a minimum of forty hours of classroom training and sixty hours

Screening: *First Steps*, 40 THE PROCUREMENT LAW. 15, 18 (2005).

22. *Kutz Testimony*, *supra* note 2, at 5.

23. *One Year Later: Have TSA Airport Security Checkpoints Improved?: Hearing Before the H. R. Comm. on Oversight and Government Reform*, 110th Cong. 4 (2007) (statement of Kip Hawley, Assistant Secretary, Transportation Security Administration) [hereinafter *Hawley Testimony*], available at <http://oversight.house.gov/documents/20071115110733.pdf>.

24. *Id.* at 1. For example, the TSA cites its overnight implementation and subsequent modification of standard operating procedures in response to the threats posed by liquid explosives following the uncovering of the UK bomb plot in August 2006. *Id.* at 4. See also *Kutz Testimony*, *supra* note 2, at 4.

25. *Kutz Testimony*, *supra* note 2, at 4. Other “layers” include “intelligence gathering and analysis, checking passenger manifests against watch lists, and employing undercover air marshals.” *Id.* See also discussion *infra* Part I.B.

26. *Kutz Testimony*, *supra* note 2, at 4. In 2006, the TSA screened 708,400,522 passengers and intercepted 13,709,211 prohibited items at security checkpoints. Transportation Security Administration, Research Center: Screening Statistics, http://tsa.gov/research/screening_statistics.shtml (last visited Aug. 30, 2008).

27. *United States v. Aukai*, 497 F.3d 955, 960 n.6 (9th Cir. 2007) (citing H.R. REP. NO. 107-296, at 53-54 (2001), *reprinted in* 2002 U.S.C.C.A.N. 589, 590).

28. *Kutz Testimony*, *supra* note 2, at 2.

29. See *Hawley Testimony*, *supra* note 23, at 1-2.

of on-the-job training prior to certification.³⁰ Additionally, security officers must meet annual recertification standards, including a standard operating procedures knowledge test, an image certification test, and a practical skills demonstration.³¹

TSO officers follow a standard operating procedure during passenger screening that includes aspects of procedure and technology.³² Standard primary search mechanisms include the use of walk-through magnetometers for passenger screening as well as x-ray baggage searches.³³ Passengers who repeatedly alarm walk-through or hand-held metal detectors or otherwise alert TSO officers of potential wrongdoing are subject to secondary searches.³⁴ The TSA standard operating procedures manual describes the process that officers must follow during these secondary searches, which includes, for purposes of our discussion, the use of a pat-down search.³⁵

2. Present-Day Primary Screening

Primary screening searches refer to the routine searches performed on each individual regardless of the level of suspicion aroused.³⁶ Primary screening mechanisms include

30. *Id.* at 5. Officer training is ongoing after certification, as the TSA annually allocates funds for three million hours of TSO recurrent training. *Id.* Additionally, the TSA online learning center ("OLC") makes available over 350 general training and development courses for TSO use. *Department of Homeland Security Appropriations, FY 2005: Hearings Before the Subcomm. on Homeland Security of the Senate Comm. on Appropriations, 108th Cong.* 367 (2005) (statement of Admiral David Stone, Acting Administrator, Transportation Security Administration) [hereinafter *Stone Testimony*], available at http://globalsecurity.org/security/library/congress/2004_h/040323-stone.htm.

31. *Stone Testimony, supra* note 30, at 367. Additional officer testing is carried out in the threat image protection ("TIP") program, which employs software that superimposes images of prohibited items on the x-ray screen during actual operations to determine whether the officer is able to identify the object. *Id.* at 368.

32. *Kutz Testimony, supra* note 2, at 4.

33. *Id.*

34. *See id.* at 5; *see also* discussion *infra* Part I.B.3.

35. *Kutz Testimony, supra* note 2, at 5. Secondary searches also include the use of explosive trace detection ("ETD") swabbing, which detects explosive vapors and residue. *Id.* Security officers collect samples by rubbing swabs on carry on objects or clothing and place the swab in the ETD machine, and the machine analyzes the sample for traces of explosive materials. *Id.* at 5 n.7.

36. *See Hawley Testimony, supra* note 23, at 3; *see also* United States v.

most notably the physical searches performed at the screening checkpoint with magnetometers and baggage scanning machines.³⁷ In addition to physical searches, however, the TSA employs various other interlinked measures that include efforts to detect behavioral abnormalities in passengers, increase visibility of officer teams,³⁸ and screen passengers against lists of high-risk individuals.³⁹

The TSA's Visible Intermodal Prevention and Response ("VIPR") teams are broadly deployed to increase the visible presence of security personnel.⁴⁰ The teams are comprised of TSO officers, Federal Air Marshals, and law enforcement, and are used in areas away from checkpoints to detect potential threats.⁴¹ Many of these individuals are trained in an advanced observational screening tool to detect potential wrongdoing.⁴²

Screening Passengers by Observational Techniques, or "SPOT," is a program designed by behavioral expert Mark G. Frank⁴³ that uses objective criteria to determine when individuals are trying to disguise emotion.⁴⁴ Trained officers observe passengers and look for both obvious and subtle suspicious behavioral indicators, like a particular vocal timbre, gestures, and facial movements.⁴⁵ The officers consult a list of approximately thirty questionable behaviors, each of

Aukai, 497 F.3d 955, 957 (9th Cir. 2007).

37. See *Kutz Testimony*, *supra* note 2, at 4.

38. *Hawley Testimony*, *supra* note 23, at 3.

39. Transportation Security Administration, What We Do: Secure Flight Program, http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm (last visited Aug. 30, 2008) [hereinafter Secure Flight Program].

40. See *Hawley Testimony*, *supra* note 23, at 3.

41. *Id.*

42. See Jonathan Karp & Laura Meckler, *Which Travelers Have 'Hostile Intent'? Biometric Device May Have the Answer*, WALL ST. J., Aug. 14, 2006, available at http://online.wsj.com/public/article/SB115551793796934752-2hgveyRtDDtssKozVPmg6RAAA_w_20070813.html?mod=tff_main_tff_top.

43. Press Release, Nat'l Sci. Found., New Technologies Could Make Airport Screening More Effective and Less Cumbersome (Oct. 24, 2006), available at http://www.nsf.gov/news/news_summ.jsp?cntn_id=108133. Frank received his Ph.D. in social psychology from Cornell and completed post-doctoral work in the psychiatry department at the University of California at San Francisco; he has published numerous articles on facial expressions and interpersonal deception. *Id.*

44. Karp & Meckler, *supra* note 42.

45. *Id.* An example of an obvious behavioral indication is wearing an extremely large jacket in warm weather. *Id.*

which is assigned a numerical score.⁴⁶ When the score exceeds a predetermined sum, an officer will approach the individual for further questioning.⁴⁷ At that point, approximately eighty percent of individuals are dismissed without further intrusion.⁴⁸ However, if the conversation arouses further suspicion, the passenger may be subject to a secondary search.⁴⁹ The program began in Boston shortly after 9/11,⁵⁰ and as of August 2006, was in use at twelve major airports.⁵¹

Additionally, acting on a key recommendation by the 9/11 Commission,⁵² Homeland Security is currently developing "Secure Flight," a program designed to conduct uniform prescreening of passenger information against government watch lists.⁵³ Currently, prescreening is conducted by the individual airlines, which, according to the TSA, results in unnecessary "inconsistencies and misidentifications."⁵⁴

Under Secure Flight, the TSA will receive basic passenger information, such as name and itinerary, through airline reservation systems and will then screen the information against government watch lists.⁵⁵ Depending on whether the individual is on the "no fly list," or "selectee list," the individual will either be prevented from boarding the aircraft or selected for secondary screening, respectively.⁵⁶

While the program continues to raise privacy concerns,⁵⁷

46. *Id.*

47. *Id.* Although the particular line of questioning pursued by SPOT officers has not been addressed by the court, "routine" questioning of passengers at airport checkpoints does not amount to custodial interrogation. *United States v. Hartwell*, 296 F. Supp. 2d 596, 606 (E.D. Pa. 2003), *aff'd*, 436 F.3d 174 (3d Cir. 2006).

48. Karp & Meckler, *supra* note 42.

49. *Id.* Despite the objective criteria used by the program, Gregory T. Nojem of the ACLU has criticized SPOT for potentially allowing impermissible criteria, such as race, to become a factor. *Id.*

50. *Id.*

51. *Id.* As of August 2006, the program had identified about one hundred people who were trying to smuggle drugs, use fake identification, or commit other crimes, but none who were attempting a terrorist attack. *Id.*

52. Secure Flight Program, *supra* note 39.

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. *Secure Flight Compared to Predecessor Program CAPPS II*, AMERICAN CIVIL LIBERTIES UNION, Mar. 29, 2005, <http://www.aclu.org/privacy/spying/15304res20050329.html>.

the TSA claims that it will provide a more equitable and consistent matching process than the current airline-operated system.⁵⁸ Accordingly, Secure Flight, scheduled to go online in 2008, seeks to streamline the screening process, thereby reducing the number of false positive tests.⁵⁹

Along similar lines, the TSA and private industry operate a registered traveler program that provides expedited security screening for those who volunteer to undergo a security threat assessment.⁶⁰ Once qualified as a registered traveler, an individual has access to enhanced customer service, discounts, and reduced waiting times at security checkpoints.⁶¹ The program is intended to offer heightened security to frequent travelers by encouraging participating entities to implement new technologies for use in the program.⁶²

3. *Present-Day Secondary Screening*

Approximately fifteen percent of domestic airline passengers are subject to secondary “pat-down” searches.⁶³ According to the TSA, a number of circumstances can justify secondary screening, including random selection, a failed walk-through or hand-held magnetometer search, and where a passenger otherwise raises a “red flag,” by, for example, purchasing a one-way plane ticket or alerting a government

58. Secure Flight Program, *supra* note 39.

59. *Id.*

60. Registered Traveler Interoperability Pilot Program, 73 Fed. Reg. 44275, 44276 (July 30, 2008), available at http://www.tsa.gov/assets/pdf/registered_traveler_interoperability_pilot_program_73_fr44275.pdf. To enroll in the registered traveler program, applicants provide biographic and biometric data to participating airports and airlines as well as TSA approved service providers. *Id.* The applicant's identity is checked against terrorist related watch-lists maintained by TSA. *Id.*

61. *Id.* Participants include several airports and air carriers such as the San Francisco International Airport, Orlando International Airport, Air France, and British Airways, among others. Transportation Security Administration, Our Approach: Registered Traveler Overview, <http://www.tsa.gov/approach/rt/index.shtm> (last visited Aug. 30, 2008).

62. Registered Traveler Interoperability Pilot Program, *supra* note 60.

63. Sara Kehaulani Goo, *Airport Pat-Down Protocol Changed: Women Complained that Security Checks Were Humiliating*, WASH. POST, Dec. 23, 2004, at E01. Other secondary search procedures beside pat-downs, such as detailed baggage inspections, are not relevant for purposes of this discussion, which is limited to search procedures conducted on individuals themselves, rather than on their personal belongings or luggage.

watch list.⁶⁴

Since 2001, the TSA has implemented stricter and more extensive secondary search procedures at airport checkpoints, including modifications to the pat-down search protocols.⁶⁵ Present day pat-down search procedures are often described as overly invasive and draw significant complaints from the traveling public.⁶⁶ While the searches are conducted on a same-sex basis, pat-downs require contact with sensitive parts of the body, including the chest and thighs.⁶⁷ Furthermore, screening officers conducting the search may, under certain circumstances, expand the scope to even *more* intimate and sensitive parts of the body, such as under and in-between a woman's breasts.⁶⁸

While in recent years the TSA has slightly scaled back pat-down searches,⁶⁹ many travelers continue to describe the searches as invasive and humiliating.⁷⁰ In response to hundreds of reported complaints from passengers, the TSA is currently developing potentially less-intrusive technologies and procedures to replace pat-downs.⁷¹

4. *Advances in Technology and Search Procedures*

The TSA employs modern technology in addition to walk-through and handheld magnetometers and baggage x-ray systems.⁷² Explosive detection systems ("EDS"), and explosive trace detection ("ETD") devices are widely used to detect potential threats.⁷³ For example, General Electric-

64. Transportation Security Administration, Research: Frequently Asked Questions, <http://www.tsa.gov/research/privacy/faqs.shtml> (last visited Aug. 30, 2008). For commentary on the government watch list programs, see Ryan Singel, *How to Get Off a Government Watch List*, WIRED, Apr. 16, 2007, available at <http://www.wired.com/politics/onlinerights/news/2007/04/watchlist2>.

65. Jessica D. Lew, *Secondary Screening Procedures for Airports: Putdowns for Pat-downs*, 19 LAWORLD: INT'L BUS. BRIEFING 1, 2 (2005), available at <http://www.makdap.com.au/docs/LAWorld%20Vol%2019.pdf>.

66. *Id.* ("Many women have reported rough, rude, and humiliating manhandling, and sometimes even overtly sexual groping by security officials.")

67. William Saletan, *Digital Penetration: Invasion of the Naked Body-Scanners*, SLATE, Mar. 3, 2007, <http://www.slate.com/id/2160977/pagenum/all>.

68. Goo, *supra* note 63.

69. *See id.*

70. *Id.*

71. *Id.*

72. *Stone Testimony*, *supra* note 30, at 368.

73. *See id.* Use of EDS and ETD devices are identified as the key to

manufactured "EntryScan" devices are capable of detecting explosives and narcotics by emitting puffs of air around the passenger in order to dislocate and detect traces of various substances.⁷⁴ The technology is currently used both randomly and as a secondary search mechanism.⁷⁵

Looking to the future, the TSA is taking a proactive approach to developing screening technology and search procedures.⁷⁶ As of 2004, the TSA and Department of Homeland Security were actively funding over 200 research and development projects related to transportation security.⁷⁷ In addition to body-scan technology, current projects include bottled liquid scanners, advanced technology x-rays, automated explosive detection systems,⁷⁸ and biometric devices, among others.⁷⁹ The TSA is also actively adjusting search procedures and officer development programs in response to threats and perceived vulnerabilities.⁸⁰ Despite these efforts, however, government audits of security checkpoints have uncovered numerous weaknesses and are currently forcing the TSA to re-evaluate all aspects of its aviation security programs.⁸¹

C. *Exposed Security Weaknesses*

Widespread government audits of security checkpoints

compliance with the 2005 statutory requirement for full electronic screening of checked baggage. *Id.*

74. Press Release, Transportation Security Administration, Tampa International Airport is TSA Test Bed for Explosives Trace Detection Portals (Aug. 3, 2004), *available at* http://www.tsa.gov/press/releases/2004/press_release_0474.shtm.

75. *Id.*

76. *Hawley Testimony*, *supra* note 23, at 6. "TSA concurs with the final [GAO] suggestion to continue to develop and deploy new technology." *Id.*

77. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO NO. 04-890, TRANSPORTATION SECURITY R&D: TSA AND DHS ARE RESEARCHING AND DEVELOPING TECHNOLOGIES, BUT NEED TO IMPROVE R&D MANAGEMENT 3 (2004), *available at* <http://www.gao.gov/new.items/d04890.pdf>. In 2004, TSA allocated 79.5% of its \$159 million R&D budget for aviation-related security projects, while Homeland Security allocated 71.9% of its \$87 million R&D budget in a similar manner. *Id.* at 4 tbl.1. Other federal agencies such as the Department of Transportation and NASA also have funded transportation security. *Id.* at 4.

78. *Hawley Testimony*, *supra* note 23, at 6.

79. Karp & Meckler, *supra* note 42.

80. *Hawley Testimony*, *supra* note 23, at 1. The TSA frequently modifies its screening program based on a number of factors, including passenger feedback, risk based planning, and internal review. *Kutz Testimony*, *supra* note 2, at 4.

81. *Kutz Testimony*, *supra* note 2, at 9.

have been underway since 9/11.⁸² The results have exposed a security system that is unable to detect modern terrorist weapons.⁸³ While opportunities for improvement exist across all aspects of security, there is a general consensus regarding the need to enhance detection capabilities through implementation of new technology.⁸⁴

1. *Areas of Vulnerability at Security Checkpoints*

The Department of Transportation's Office of the Inspector General tested security checkpoints at the direction of President Bush between November 2001 and July 2002.⁸⁵ The tests indicated several areas of vulnerability in officer training, equipment and technology, procedures, and management.⁸⁶ As a result, the TSA created the Office of Internal Affairs and Program Review ("OIAPR"), which developed criteria to evaluate security systems nationwide.⁸⁷

In 2003, Homeland Security implemented its own undercover tests to assess the detection capabilities of airport security systems.⁸⁸ The tests included hundreds of investigations at different categories of airports and concluded in November 2003.⁸⁹ Officials administering the tests met with OIAPR prior to and after the tests to obtain and review security directives and modify standard operating procedures.⁹⁰ Recommendations included increased recurrent training for security officers, more attentive management to "ensure effective, vigilant, and courteous screening,"⁹¹ and

82. *Id.* at 1; see, e.g., OIG AUDIT, *supra* note 3.

83. See *Kutz Testimony*, *supra* note 2.

84. OIG AUDIT, *supra* note 3, at 4. The U.S. Government Accountability Office highlighted three areas in need of improvement: technology, procedure, and human resources. *Kutz Testimony*, *supra* note 2, at 1-2.

85. OIG AUDIT, *supra* note 3, at 1.

86. *Id.* at 1-2.

87. *Id.* at 2.

88. *Id.* Testing was completed at fifteen airports and included undercover agents attempting to pass security checkpoints with various prohibited items. *Id.*

89. *Id.* "Commercial airports are categorized based on the number of annual enplanements. The nation's busiest airports are termed Category X airports while airports with fewer enplanements are categorized as Category I, Category II, or Category III." OIG AUDIT, *supra* note 3, at 2 n.2.

90. *Id.* Homeland Security also visited the transportation security lab in New Jersey to discuss their test methodology and learn about the technology in use at various airports. *Id.*

91. *Id.* at 5.

development and implementation of new technology.⁹²

Homeland Security completed a second round of aviation security screening tests between November 2004 and February 2005.⁹³ Although TSA had taken steps to follow previous recommendations, the report stated that “the lack of improvement since [its] last audit indicat[ed] that significant improvement in performance may not be possible without greater use of technology.”⁹⁴ This conclusion was based in part on the fact that a majority of the failures occurred notwithstanding the diligent and proper performance of the screening officers.⁹⁵ Based on this finding, Homeland Security recommended that the TSA “aggressively pursue the development and deployment of innovations and improvements to aviation security technologies, particularly for checkpoint screening.”⁹⁶ Homeland Security specifically recommended giving preference to body-scanning devices “that will enable the screening workforce to better detect both weapons and explosives.”⁹⁷

2. TSA Security Audits

In response to these audits, TSA created the Aviation Screening Assessment Program (“ASAP”) to expand covert testing and provide statistics to further develop security systems.⁹⁸ Over a six-month period beginning in April 2007, ASAP performed thousands of covert tests designed to assess threats, including those specifically posed by liquid and other non-metal explosives.⁹⁹ Additionally, the TSA itself conducts

92. *Id.* at 1–4. Technology discussed in the report include multi-view x-ray systems for baggage screening, backscatter x-ray, and the TIP program. *Id.* at 3–4.

93. OFFICE OF THE INSPECTOR GENERAL, U.S. DEPT. OF HOMELAND SECURITY, OIG NO. 05-16, FOLLOW-UP AUDIT OF PASSENGER AND BAGGAGE SCREENING PROCEDURES AT DOMESTIC AIRPORTS 1 (2004), available at http://www.dhs.gov/xoig/assets/mgmt/rpts/OIG_05-16_Mar05.pdf.

94. *Id.* at 2.

95. *Id.* (“A ‘pass’ occurred if the object was identified by screening personnel and prevented from being carried into the sterile area through the screening checkpoint or being put into the baggage system downstream from the checked baggage screening location. A ‘fail’ occurred when the object was not detected at the screening checkpoint, or the checked bag was cleared for flight.”).

96. *Id.*

97. *Id.* at 3.

98. *Hawley Testimony*, *supra* note 23, at 7.

99. *Id.* Testing methodology was based in large part on the threat posed by the British bomb plot:

over a thousand covert tests for improvised explosive devices (“IEDs”) and improvised incendiary devices (“IIDs”) and 70,000 electronic image tests every day.¹⁰⁰

The TSA has remained secretive about the specific results of these audits.¹⁰¹ However, the Government Accountability Office was particularly forthcoming in a November 15, 2007 preliminary report detailing the result of a series of tests performed by the Office.¹⁰² The report showed that investigators were successful in passing through security checkpoints with components for “several” IEDs and IIDs.¹⁰³

Our tests clearly demonstrate that a terrorist group, using publicly available information and few resources, could cause severe damage to an airplane and threaten the safety of passengers by bringing prohibited IED and IID components through security checkpoints. Given our degree of success, we are confident that our investigators would have been able to evade transportation security officers at additional airports had we decided to test them.¹⁰⁴

The preliminary report led to immediate action from the TSA, setting in motion a plan to develop and implement a technologically advanced “checkpoint of the future.”¹⁰⁵

The discovery of this bomb plot, in which terrorists allegedly sought to detonate [IEDs] in airplanes as they crossed the Atlantic Ocean, caused TSA to substantially modify its screening procedures—all liquids, gels, and aerosols with some exceptions were banned from being carried through passenger screening checkpoints and onto aircraft until the plot was further investigated.

Kutz Testimony, supra note 2, at 1.

100. *Hawley Testimony, supra* note 23, at 7. TSA Administrator Kip Hawley claims that tests are conducted at “every checkpoint, every shift, everyday, [at] every one of our four hundred fifty some airports.” Bob Orr, *GAO: Bomb Parts Snuck Past Airport Checkpoints*, CBS NEWS, Nov. 14, 2007, <http://www.cbsnews.com/stories/2007/11/14/eveningnews/printable3502791.shtml>.

101. *See Kutz Testimony, supra* note 2, at 1 n.1, 2, 2 n.3.

102. *Id.* at 1. The tests were completed at nineteen unspecified airports. *Id.*

103. *Id.* at 2. The particular device components and methods of concealment are classified. *Id.*

104. *Id.* at 9–10.

105. *Id.* at 9. The Government Accountability Office issued a more comprehensive report on the tests, along with recommendations to the TSA, in July 2008. *Aviation Security: An Update (2008): Hearing Before the Subcomm. on Aviation of the H. Comm. On Transportation and Infrastructure*, 110th Cong. (2008) (statement of Cathleen A. Berrick, Dir. of Homeland Security and Justice Issues, Gov't Accountability Office), [http://transportation.house.gov/Media/File/Aviation/20080724/GAO_Cathleen%](http://transportation.house.gov/Media/File/Aviation/20080724/GAO_Cathleen%20Berrick%20Statement%207-24-08.pdf)

D. The “Checkpoint of the Future”: Body-Scanning Technology

The TSA’s investment in threat detection technologies has increased significantly with the emergence of liquid and other modern explosive devices such as those uncovered in the British terrorist plot of 2006.¹⁰⁶ The non-metallic properties of these emerging threats have rendered magnetometers obsolete and left the TSA scrambling for answers.¹⁰⁷

The technologies at the forefront of this effort are two kinds of “whole-body” scanning machines that utilize “backscatter” x-ray and “millimeter wave” technologies, respectively, to detect items concealed under layers of clothing.¹⁰⁸ While utilizing different technologies, both machines penetrate clothing but not skin, allowing the screening officer to view an image of the human form along with hidden items of “unusual density.”¹⁰⁹

1. Backscatter X-ray

Backscatter x-ray technology uses narrow, low-intensity x-rays that deflect off human skin to display an image of the human form.¹¹⁰ The technology offers a distinct security advantage over magnetometers, which cannot detect many of the substances used in modern explosive devices.¹¹¹ The

20Berrick_7_24_08%20AvHrng%20on%20Aviation%20Security.pdf.

106. See Michael Chertoff, Editorial, *We Must Remain Flexible*, USA TODAY, Aug. 15, 2006, at 9A, available at http://www.usatoday.com/news/opinion/editorials/2006-08-15-chertoff-security_x.htm.

107. Saletan, *supra* note 67; see also Transportation Security Administration, Our Approach: Mythbusters, http://www.tsa.gov/approach/mythbusters/liquids_ban.shtm (last visited Aug. 30, 2008).

108. See Transportation Security Administration, Our Approach: Whole Body Imaging, http://www.tsa.gov/approach/tech/body_imaging.shtm (last visited Sept. 11, 2008).

109. Saletan, *supra* note 67.

110. Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, Feb. 23, 2007, http://www.tsa.gov/press/releases/2007/press_release_02232007.shtm. The level of x-ray exposure from backscatter machines is equivalent to approximately fifteen minutes of exposure to naturally occurring radiation, such as sunlight. *Id.*

111. See Miller, *supra* note 1. For example, Rep. John Mica pointed out that Richard Reid, convicted of trying to blow up a trans-Atlantic jetliner after

machines have been undergoing testing at Phoenix's Sky Harbor International Airport since February 2007,¹¹² and additional pilot programs are now underway in Los Angeles, Baltimore, Denver, Albuquerque, New York's Kennedy Airport, and Reagan National in Washington, D.C.¹¹³

The pilot programs are operated on a voluntary basis; passengers subject to secondary searches have the choice between a pat-down and body-scan.¹¹⁴ While comprehensive tests results are yet unavailable, the TSA estimates that more than ninety percent of Phoenix air passengers have chosen body-scans over pat-down searches.¹¹⁵ Currently, the TSA intends to continue further testing to allow the TSA "to determine the role the[] technolog[y] will play in the future."¹¹⁶

2. Millimeter Wave Technology

Millimeter wave technology utilizes electromagnetic waves to render a three-dimensional image of the body.¹¹⁷ The energy emitted by millimeter wave technology is 10,000-

boarding the airplane with explosives in his shoes, walked through metal detectors several times before boarding the plane. *Id.* TSA officials say he would not have successfully bypassed screening checkpoints had backscatter devices been in use. *Id.*

112. Transportation Security Administration, *Our Approach: Whole Body Imaging*, *supra* note 108. The technology has been used for years in all sorts of security situations, from prisons and U.S. Customs checkpoints, to South African diamond mines. Thomas Frank, *Phoenix Test Site for TSA X-Ray: ACLU Objects to 'Virtual Strip Search,'* USA TODAY, Aug. 22, 2008, at 1A, available at http://www.usatoday.com/news/washington/2006-11-30-tsa-xray_x.htm. See also Miller, *supra* note 1.

113. Thomas Frank, *10 Airports Install Body Scanners: Devices Can Peer Under Passengers' Clothes*, USA TODAY, June 6, 2008, at 3A, available at www.usatoday.com/printedition/news/20080606/a_bodyscan06.art.htm.

114. See Press Release, Transportation Security Administration, *TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport*, *supra* note 110; see also Transportation Security Administration, *Our Approach: Whole Body Imaging*, *supra* note 108.

115. Transportation Security Administration, *Our Approach: Whole Body Imaging*, *supra* note 108. Cf. Access Intelligence, LLC, *TSA Tests Millimeter Wave Screening at Phoenix Sky Harbor*, AIR SAFETY WEEK, Oct. 15, 2007, <http://www.aviationtoday.com/asw/categories/commercial/16516.htm> (as of October 2007, seventy-nine percent of the public had opted to try backscatter over the pat-down).

116. See Hawley Testimony, *supra* note 23, at 7-8.

117. Press Release, Transportation Security Administration, *TSA Announces Bi-coastal Launch of Millimeter Wave Imaging Technology*, (Apr. 17, 2008), available at <http://www.tsa.gov/press/releases/2008/0417.shtm>.

times less than a cell phone.¹¹⁸ Like backscatter, the millimeter wave machine is able to display metallic and nonmetallic items hidden below clothing, including plastic and liquid weapons and explosives,¹¹⁹ albeit with a slightly lower resolution.¹²⁰

Millimeter machines are being tested alongside backscatter scanners on the same voluntary basis and in the same airports.¹²¹ The TSA recently announced it will purchase and deploy thirty additional machines by the end of 2008.¹²²

3. *Privacy Concerns*¹²³

While praised for their detection capabilities,¹²⁴ body-scans present alarming privacy concerns for air travelers.¹²⁵

118. *Id.*

119. See Transportation Security Administration, Our Approach: Whole Body Imaging, Millimeter Wave, <http://www.tsa.gov/approach/tech/mwave.shtm> (last visited Sept. 11, 2008).

120. Access Intelligence, LLC, *supra* note 115.

121. See Transportation Security Administration, Our Approach: Whole Body Imaging, *supra* note 108; see also Press Release, Transportation Security Administration, TSA to Conduct First Real-World Test of Cutting-Edge Backscatter Technology (Oct. 21, 2004), available at http://www.tsa.gov/press/releases/2004/press_release_0527.shtm. 122.

122. Press Release, Transportation Security Administration, TSA Pilots Millimeter Wave Technology at Miami International Airport; Advanced Technology X-Ray also Deployed, (July 21, 2008), <http://www.tsa.gov/press/releases/2008/0721.shtm>.

123. Other concerns presented by the use of new technology and not addressed in this comment include those of speed, cost, and size. Price estimates of backscatter machines are between \$100,000 and \$200,000 per machine. Miller, *supra* note 1. Although size estimates vary depending on the manufacturer, the largest machine is four feet by seven feet by ten feet, which is "awfully big for an airport lobby." *Id.* (quoting Randal Null, Chief Technology Officer, American Science and Engineering, Inc.). Time estimates are less than ten seconds per scan, and less than one minute for the entire process. Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110. The impact of these concerns impliedly depends on how the machines are ultimately used. For example, speed and cost would be of utmost concern if the machines are used as a mandatory check for each passenger, as many more machines, and more searches, would be necessary. For purposes of this comment, which recommends that the machines be used as a secondary search mechanism, these concerns would appear to be less burdensome.

124. See Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110.

125. Miller, *supra* note 1. Susan Hollowell, director of the TSA security laboratory, after hiding weapons on her person and entering the backscatter

In its unprocessed form, the technology produces images described as “so sharp that the shape of a person’s navel is visible, along with the shapes of other, more private parts.”¹²⁶

The American Civil Liberties Union (the “ACLU”) likens the technology to a “virtual strip search” that is highly invasive and not narrowly tailored, absent probable cause, to meet the needs of airport security.¹²⁷ In response to the TSA pilot program in Phoenix, the ACLU’s Timothy D. Sparapani appeared before the Senate Committee on Commerce, Science, and Transportation to condemn the TSA’s authorization and funding of body-scan machines.¹²⁸ His concerns included that use of the machines will lead to unnecessary secondary searches,¹²⁹ that passengers would be required to display personal details of their bodies,¹³⁰ and the possibility that the images could be reproduced or appear on the Internet.¹³¹ Concerns also exist over the potential for selective or improper use of the technology based on cultural

machine, stated that the technology “basically makes you look fat and naked—but you see all this stuff.” *Id.*

126. *Airport Body Search May Reveal More Than Passengers Know*, CABLE NEWS NETWORK, Aug. 21, 2000, <http://archives.cnn.com/2000/TRAVEL/NEWS/08/21/bodysearch.ap/index.html>. For a vivid example of an image produced by the technology *without* the use of built-in privacy software, visit <http://www.privacyinternational.org/issues/cctv/bodysearch.gif>.

127. Saletan, *supra* note 67.

128. *Aviation Security: Hearing before the Senate Comm. on Commerce, Science, and Transportation*, 109th Cong. (2006) [hereinafter *Sparapani Testimony*] (statement of Timothy D. Sparapani, Legislative Counsel, American Civil Liberties Union), <http://www.aclu.org/privacy/gen/24856leg20060404.html> (last visited Sept. 17, 2008). The ACLU has outlined what they believe to be the principles of airline security, which include (1) that new security technology must be genuinely effective; (2) the level of privacy intrusion should reflect the level of risk; (3) those technologies that reduce the gravest threats must be implemented first; (4) technologies must focus on accomplishing the critical objective that authorizes their application; (4) minimally intrusive screening technologies should be implemented in lieu of ineffective passenger pre-screening proposals, such as Secure Flight and Registered Traveler; and (5) Security measures should be implemented in a non-discriminatory manner. *Id.*

129. *Id.* “Even the presence of a seemingly innocuously shaped item, such as a prosthetic device or implant, will require subsequent (and potentially humiliating) verification.” *Id.*

130. *Id.* (explaining that passengers expect to keep personal details, “such as evidence of mastectomies, colostomy appliances, penile implants, catheter tubes, and the size of their breasts or genitals” private).

131. Elisabeth Salemme, *Backlash on Backscatter*, TIME, Jan. 4, 2007, available at <http://www.time.com/time/magazine/article/0,9171,1574165,00.html> (quoting ACLU “privacy expert” Jay Stanley).

or racial factors.¹³²

The TSA has taken steps to remedy some of these concerns. First, manufacturers now integrate software systems into the machines that distort the images they produce.¹³³ The result is an image of the human form that blurs many intimate details of the body, including the face, but that retains some ability to display concealed items.¹³⁴ Described as a “chalk outline of a person,” the image generated by the masking software sacrifices a degree of detection capability, as the blurred images “start to lose the ability to [detect] . . . C4” explosives.¹³⁵

Second, the TSA has guaranteed that the officer viewing station will be remotely located.¹³⁶ The officer attending the passenger will not view the images and the remotely located officer will not be able to associate the image with the person being screened.¹³⁷ The remote screening officer will also be the same sex as the passenger.¹³⁸ Third, the manufacturer contends that it is not possible for the screening officer to save, transmit, print, or otherwise store the images.¹³⁹ All images are immediately and automatically deleted from the system after viewing.¹⁴⁰

The TSA has stood confidently behind these measures as adequate remedies to the privacy concerns posed by body-scanning devices.¹⁴¹ In fact, the TSA stated that the

132. *Sparapani Testimony*, *supra* note 128. It is unclear, however, whether body-scans would illicit additional concerns in this regard beyond those presented in the context of magnetometer and pat-down searches.

133. Frank, *supra* note 113.

134. *Id.* A similar system is in development using electromagnetic waves. *Id.*

135. Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110.

136. *Id.*

137. *Id.*

138. Barbara Yost, *Nudity Has Become an Option*, GLOBE AND MAIL (Toronto), Apr. 25, 2007, at R6, available at <http://www.theglobeandmail.com/servlet/story/RTGAM.20070425.wphoenix25/BNStory/PersonalTech/home>.

139. American Science & Engineering, Inc., TSA Z Backscatter Pilot: TSA Initiates Pilot Testing of Privacy Enhanced SmartCheck Personnel Screening System, http://www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp (last visited Sept. 11, 2008).

140. *See id.*

141. Frank, *supra* note 113. TSA Assistant Administrator Randy Null stated in an interview with *USA Today* that the TSA is now “very comfortable” with the privacy protections offered by the modern systems. Frank, *supra* note 112.

machines could replace walk-through magnetometers and become a primary search mechanism in the near future.¹⁴² However, privacy groups remain skeptical and continue to warn of the possibility of “widespread use—and abuse” of the technology.¹⁴³

II. AIRPORT SEARCHES AND THE FOURTH AMENDMENT

The Fourth Amendment secures “[t]he right of the people to be secure in their persons . . . against unreasonable searches and seizures.”¹⁴⁴ The reasonableness of a search is determined “by assessing, on the one hand, the degree to which [the search] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of a legitimate government interest.”¹⁴⁵

A balance between these competing interests is most commonly met where the government produces a warrant establishing probable cause.¹⁴⁶ In the context of airport searches, however, probable cause, or even a minimal level of individualized suspicion, does not set the constitutional floor for protection.¹⁴⁷

Warrantless airport searches, including mandatory magnetometer searches, are frequently justified based on their use as part of a general regulatory scheme “aimed at a group or class of people rather than a particular person.”¹⁴⁸ The Supreme Court has repeatedly upheld the constitutionality of these so-called “administrative searches” “where the risk of public safety is substantial and real.”¹⁴⁹

142. *Id.*

143. *Id.* (quoting Barry Steinhardt, head of the ACLU’s technology and liberty program).

144. U.S. CONST. amend. IV.

145. *United States v. Knights*, 534 U.S. 112, 118–19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

146. See Antoine McNamara, Note, *The “Special Needs” of Prison, Probation, and Parole*, 82 N.Y.U. L. REV. 209, 212 n.11 (2007) (citing *Horton v. California*, 496 U.S. 128, 133 (1990)) (holding that the general Fourth Amendment standard requires a warrant outlining (1) the scope of the search, and (2) that the search is supported by probable cause that it will uncover evidence of a crime); see also *Ornelas v. United States*, 517 U.S. 690, 696 (1996) (citations omitted) (holding that probable cause “exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found”).

147. See *United States v. Aukai*, 497 F.3d 955, 962 (9th Cir. 2007).

148. *People v. Dukes*, 580 N.Y.S.2d 850, 851–52 (N.Y. 1992).

149. *Id.* at 852. The Court has not yet explicitly held that airport searches

Although mandatory airport searches are routinely upheld in this manner, the predicate justifications vary between “general reasonableness,” “consent,” and the “stop and frisk” rationale of *Terry v. Ohio*.¹⁵⁰

A. “*Terry*” Stops

The Supreme Court in *Terry v. Ohio* held that a warrantless search by a law enforcement official is constitutional, provided that it is “strictly circumscribed by the exigencies which justify its initiation.”¹⁵¹ Therefore, a search for weapons by an officer who is fearful of immediate harm must be “limited to that which is necessary for the discovery of weapons . . . and may realistically be characterized as something less than a ‘full’ search.”¹⁵²

The Fourth Circuit applied the *Terry* search rationale to justify airport magnetometer searches in *United States v. Epperson*.¹⁵³ The court concluded that the *Terry* exception, meant to protect “others . . . in danger,”¹⁵⁴ extends to protection of the general public in the context of airport searches. Accordingly, the court applied the *Terry* balancing approach, holding that an airport search must be “justified at its inception,” and “reasonably related in scope to the circumstances which justified the interference in the first place.”¹⁵⁵ Noting that magnetometer searches are minimally invasive, the court held that a slight invasion of privacy is warranted in light of the strong governmental interest in public safety.¹⁵⁶

are permissible administrative searches, but has “[o]n three occasions . . . suggested that airport screening searches are constitutionally reasonable administrative searches.” *Aukai*, 497 F.3d at 959 n.2 (citing *Chandler v. Miller*, 520 U.S. 305, 323 (1997); *City of Indianapolis v. Edmond*, 531 U.S. 32, 47–48 (2000); *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 675 (1989)).

150. *Gibson v. State*, 921 S.W.2d 747, 757–58 (Tex. App. 1996). For an argument in favor of a new justification for preflight passenger searches under the Fourth Amendment, see Steven R. Minert, *Square Pegs, Round Hole: The Fourth Amendment and Preflight Searches of Airline Passengers in a Post-9/11 World*, 2006 B.Y.U. L. REV. 1631, 1660–67 (2006).

151. *Terry v. Ohio*, 392 U.S. 1, 26 (1968).

152. *Id.*

153. *United States v. Epperson*, 454 F.2d 769, 770 (4th Cir. 1972).

154. *Id.* at 772 (quoting *Terry*, 392 U.S. at 30).

155. *Id.* at 771 (quoting *Terry*, 392 U.S. at 20).

156. *See id.*

B. Implied Consent

Some courts justify administrative searches where consent to the search is “voluntary, unequivocal, specific and freely and intelligently given rather than resulting from duress or coercion.”¹⁵⁷ Some courts, including the Fifth and Eleventh Circuits, have applied the justification to the context of airport searches, where consent to the screening process is considered implied and irrevocable.¹⁵⁸

Under the consent doctrine, all individuals who present themselves for entry on an airplane, regardless of suspicion, are subject to a reasonable search.¹⁵⁹ Therefore, consent alone, while considered as an element in favor of justifying a given search, does not satisfy the Fourth Amendment reasonableness requirement. Instead, consent-based searches require a balancing of public necessity, effectiveness, and degree of intrusion.¹⁶⁰

There is a general consensus that present-day primary search procedures, namely magnetometer searches, satisfy the consent-based balancing inquiry.¹⁶¹ First, airport searches invoke significant public safety concerns; courts often describe the threat of airline terrorism as “unquestionably grave and urgent.”¹⁶² Second, magnetometers, at least prior to the emergence of body-scans, “have every indicia of being the most efficacious that could be used.”¹⁶³ Finally, courts applying the consent doctrine hold that magnetometer searches are justifiably invasive, given both the minimally invasive nature of the technology and the reduced expectation of privacy inherent in the so-called “voluntary” search.¹⁶⁴

157. *Gibson v. State*, 921 S.W.2d 747, 757 n.3 (Tex. App. 1996) (citing *Schneekloth v. Bustamonte*, 412 U.S. 218, 228 (1973)).

158. *United States v. Herzbrun*, 723 F.2d 773, 776 (11th Cir. 1984); see also *United States v. Skipwith*, 482 F.2d 1272, 1277–76 (5th Cir. 1973).

159. See *Skipwith*, 482 F.2d at 1276.

160. *Id.* at 1275. The Eleventh Circuit also adopted the *Skipwith* test. *Herzbrun*, 723 F.2d at 775.

161. See *United States v. Hartwell*, 296 F. Supp. 2d 596, 602 (E.D. Pa. 2003), *aff'd*, 436 F.3d 174 (3d Cir. 2006).

162. *Id.* (quoting *United States v. Davis*, 482 F.2d 893, 901 (9th Cir. 1973)).

163. *Id.* (quoting *Skipwith*, 482 F.2d at 1275).

164. *Skipwith*, 482 F.2d 1272.

C. General Reasonableness

Some courts justify airport searches under a general reasonableness standard “since as a practical matter, an airport search could not be subjected to the warrant requirement” typically mandated by the Fourth Amendment.¹⁶⁵ Courts rejecting the implied consent justification cite the inherent governmental coercion involved in an election between submitting to a search and exercising one’s constitutional right to travel.¹⁶⁶

The Ninth Circuit in *United States v. Aukai* applied the general reasonableness justification, expressly rejecting implied consent as a justification for airline administrative searches.¹⁶⁷ In *Aukai*, the court upheld the secondary search of a passenger who failed to present a valid identification to security officers.¹⁶⁸ Sitting en banc, the Ninth Circuit justified the use of a magnetometer and subsequent pat-down search of Daniel Aukai because it was “no more extensive nor intensive than necessary, in light of current technology, to detect the presence of weapons or explosives,” and it was “confined in good faith to that purpose.”¹⁶⁹ Similar to the consent doctrine and the *Terry* exception, *Aukai* requires that the search be “well-tailored to protect personal privacy, escalating in invasiveness only after a lower level of screening disclosed a reason to conduct a more probing search.”¹⁷⁰

The United States District Court for the Eastern District of Pennsylvania articulated a similar multi-step search test in *United States v. Hartwell*.¹⁷¹ The *Hartwell* court upheld the actions of an officer who frisked the pocket of a traveler who repeatedly failed walk-through and hand-held

165. *Hartwell*, 296 F. Supp. 2d at 602 (quoting *United States v. Albarado*, 495 F.2d 799, 804 (2d Cir. 1974)).

166. *Gibson v. State*, 921 S.W.2d 747, 757 n.3 (Tex. App. 1996) (citing *Albarado*, 495 F.2d at 807); see also *United States v. Kroll*, 481 F.2d 884, 886 (8th Cir. 1973)).

167. *United States v. Aukai*, 497 F.3d 955, 960 (9th Cir. 2007). According to the court, administrative searches rely on statutory authority rather than on a theory of implied consent. *Id.* at 960–61 (citing *United States v. Biswell*, 406 U.S. 311, 315 (1972)).

168. *Aukai*, 497 F.3d at 963.

169. *Id.* at 962 (quoting *United States v. Davis*, 482 F.2d 893, 913 (9th Cir. 1973)).

170. *Id.* (quoting *United States v. Hartwell*, 436 F.3d 174, 180 (3d Cir. 2006)).

171. *Hartwell*, 296 F. Supp. 2d 596.

magnetometer searches.¹⁷² The court concluded that the officers “had exhausted all purely voluntary means of resolving the alarm” by resorting first to handheld metal detection prior to conducting the pat-down.¹⁷³ Therefore, the least restrictive search available to the officers at that point was either to request that Hartwell produce the item, or in the alternative (upon his non-compliance), to conduct a pat-down search to produce it themselves.¹⁷⁴ Accordingly, the “general reasonableness” doctrine requires that the search be tailored to the particular harm presented at each security “layer.”

D. A Common Theme: Proportionality

Despite their varied formulae, the tests based on *Terry*, “consent,” or “general reasonableness” each articulate a substantially similar balancing approach that requires proportionality at each security “layer.”¹⁷⁵ Accordingly, the administrative airport search justifications are reconcilable in that they all set forth a similar base-line reasonableness test, albeit with slightly different considerations.

First, the prevailing distinction between the three doctrines, the element of implied consent, is largely irrelevant for purposes of our discussion.¹⁷⁶ Implied consent, where applicable, merely serves as a justification for invoking a primary search, which, as is pointed out in *Epperson*, is a separate inquiry into whether the *scope* of the search is reasonable.¹⁷⁷ Therefore, once the primary airport search is invoked, consent does not factor into what kind of search is conducted. Since our inquiry focuses on the nature of the primary search, rather than whether a primary search is itself warranted, the distinction presented by the consent doctrine is largely irrelevant.

Second, even if relevant, the consent doctrine is largely inconsistent with more recent administrative search

172. *See id.* at 603–04.

173. *Id.* at 604.

174. *Id.*

175. *See, e.g.*, *United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007); *United States v. Skipwith*, 482 F.2d 1272 (5th Cir. 1973); *United States v. Hartwell*, 296 F. Supp. 2d 596 (E.D. Pa., 2003), *aff'd*, 436 F.3d 174 (3d Cir. 2006).

176. *See Aukai*, 497 F.3d at 959–60.

177. *United States v. Epperson*, 454 F.2d 769, 772 (4th Cir. 1972).

jurisprudence. “Consent” is given, as a matter of law, only where the individual submits to the search freely and without coercion.¹⁷⁸ Therefore, “consent,” as recognized in more recent case law, is not invoked where an individual must elect between submitting to a government-operated search and abstaining from air travel.¹⁷⁹ Rather, such a decision invokes coercion, rendering any consideration of the element of consent inappropriate.¹⁸⁰

Absent the element of “consent,” the three justifications are substantially similar: *Terry* requires a search “reasonably related in scope to the circumstances which justified the interference,”¹⁸¹ “consent” requires a balancing of public safety and effectiveness against intrusion,¹⁸² and general reasonableness requires that the search is “no more extensive nor intensive than necessary.”¹⁸³ So described, each doctrine necessitates a properly tailored search that equally considers the competing values of privacy and safety.

Therefore, despite a lack of consensus as to the particular justification for administrative searches, reasonableness remains the constitutional minimum.¹⁸⁴ Accordingly, in determining the appropriate layer for body-scan searches, the TSA must successfully and carefully balance the potential security benefits of body-scan technology with basic Fourth Amendment privacy protections.

III. BODY-SCAN SEARCHES AND THE FOURTH AMENDMENT: RECONCILING SAFETY AND PRIVACY

As demonstrated by the events of 9/11, the safety of air travelers and the general public alike depends on reliable airport screening procedures.¹⁸⁵ However, the proportionality requirement of the Fourth Amendment requires that airport security measures employ a degree of risk management that appropriately considers the protection of personal privacy. In

178. *Gibson v. Texas*, 921 S.W.2d 747, 757 n.3 (Tex. App. 1996) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 228 (1973)).

179. *See, e.g., United States v. Albarado*, 495 F.2d 799, 804 n.15 (2d Cir. 1974); *United States v. Kroll*, 481 F.2d 884, 886 (8th Cir. 1973).

180. *See, e.g., Albarado*, 495 F.2d at 806–07; *Kroll*, 481 F.2d at 886.

181. *Epperson*, 454 F.2d at 771 (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968)).

182. *United States v. Skipwith*, 482 F.2d 1272, 1275 (5th Cir. 1973).

183. *United States v. Aukai*, 497 F.3d 955, 962 (9th Cir. 2007).

184. *See* U.S. CONST. amend. IV.

185. *See Aukai*, 497 F.3d at 956.

fact, the TSA, conceding this point, seeks to employ a "layered" security approach such that any single search tool need not be overly invasive.¹⁸⁶

Given the invasive nature of body-scan devices,¹⁸⁷ the question remains as to how to appropriately tailor the use of this technology in a manner that equally considers these conflicting interests. Although current search methods and technologies, such as walk-through magnetometers and pat-down searches, fit neatly into present-day primary and secondary search jurisprudence, uncertainty exists as to how the TSA can implement the technology without impermissibly infringing on Fourth Amendment rights.

A. *Routine Body-Scan Searches Are Unconstitutional*¹⁸⁸

The TSA recently indicated that body-scan technology may soon become the centerpiece of the "checkpoint of the future," replacing magnetometers as the primary, routine search mechanism deployed at all airport checkpoints.¹⁸⁹ Deploying body-scans in this manner, however, is an unconstitutional use of the technology. As the following discussion will show, requiring every domestic airline passenger to display an outlined form of his body, absent cause, does not strike the appropriate constitutional balance between safety and privacy.

1. *Body-scans Are More Intrusive Than Walk-Through Magnetometers*

Airport security systems have evolved over time.¹⁹⁰ Today, walk-through magnetometers are seen as commonplace and routine, particularly in the setting of airport screening.¹⁹¹ Accordingly, magnetometer searches are widely upheld as a minimal invasion of privacy that "does not annoy, frighten or humiliate those who pass through it."¹⁹²

186. *Hawley Testimony*, *supra* note 23.

187. *See* discussion *supra* Part I.D.; *see also* discussion *infra* Part III.B.

188. While this comment focuses on the use of backscatter and millimeter wave technology for scanning individual travelers, the same technology does have tremendous potential to screen carry-on and checked luggage as well. *See Sparapani Testimony*, *supra* note 128.

189. *Kutz Testimony*, *supra* note 2, at 9.

190. *See* *Gibson v. State*, 921 S.W.2d 747, 759 n.5 (Tex. App. 1996).

191. *Id.* at 759.

192. *Id.* at 758 (quoting *United States v. Albarado*, 495 F.2d 799, 805-06 (2d

Body-scan searches, however, are not constitutionally comparable.

The privacy intrusions of backscatter and millimeter wave devices are significant.¹⁹³ Absent the use of privacy-filtering software, the technology produces extremely detailed images that expose intimate parts of the body and invade basic privacy expectations.¹⁹⁴ Not only do body-scans subject travelers to this “virtual strip search,”¹⁹⁵ but the search is conducted in front of a captive audience of fellow travelers, all apparently aware of the fact that this person’s naked body is being remotely viewed.¹⁹⁶ Therefore, as compared to minimally invasive magnetometer searches, body-scans present a much higher potential for humiliation.

Though the modern form of the technology, which attempts to recapture some elements of privacy, is less intrusive,¹⁹⁷ the “chalk outline” image continues to present significantly more privacy concerns than magnetometer searches. First, the potential for humiliation continues to be a concern. Many individuals desire to conceal highly personal details of their bodies, such as evidence of surgeries, implants, and medical devices.¹⁹⁸ Though many of these items would likewise alert a magnetometer, body-scans would detect additional non-metal items. Additionally, body-scans do more than merely detect the presence of these objects; the fact that the device produces an image is itself a source of potential humiliation beyond that presented by magnetometers.¹⁹⁹

Second, body-scans present an opportunity for abuse that does not exist in magnetometer searches.²⁰⁰ Although the TSA assures that the images cannot be saved, some privacy experts continue to be wary that the images will be reproduced or otherwise exploited by screening personnel,²⁰¹ a

Cir. 1974)).

193. See discussion *supra* Part I.D.

194. See Miller, *supra* note 1.

195. See Yost, *supra* note 138.

196. Frank, *supra* note 113.

197. See discussion *supra* Part I.D.

198. *Sparapani Testimony*, *supra* note 128. The TSA has stated that body-scans can detect implants larger than small pins, such as shoulder and knee replacements. Yost, *supra* note 138.

199. See Saletan, *supra* note 67.

200. *Sparapani Testimony*, *supra* note 128.

201. Salemme, *supra* note 131.

concern that simply does not exist with magnetometers.

Third, body-scan searches introduce a subjective element into the primary screening process that does not exist with magnetometer searches. While magnetometers automatically detect metallic items, body-scans require the intervention of a human element whereby a screening officer must subjectively differentiate between threatening and non-threatening items displayed on a screen.²⁰²

This subjective feature implicates two potentially intrusive scenarios not seen with magnetometer searches. First, there is a fear that the screening officers may consider race, sex, weight, or other impermissible factors when determining whether the passenger poses a threat that requires further inquiry.²⁰³ While the officers are remotely located, the images are detailed in such a manner that a screening officer could potentially be made aware of these physical characteristics.²⁰⁴ Again, magnetometers do not present similar concerns.

Second, even absent the potential for prejudice, the subjective element will likely result in a greater number of unnecessary secondary searches than magnetometer searches.²⁰⁵ Regardless of their level of training, officers will be faced with the difficult task of differentiating between harmless devices, such as medical implants, and concealed weapons and explosives. While the accuracy of the machines is somewhat unknown, it stands to reason that devices of similar shape and density to a threatening object would similarly alert the attention of a screening officer, regardless of whether the device is in fact threatening.²⁰⁶ In fact, the privacy software in the modern form of the technology, while minimizing the initial intrusion, could inevitably amplify privacy concerns by diminishing the accuracy of the search.²⁰⁷ Accordingly, primary body-scan searches would potentially lead to many unnecessary secondary searches that would not otherwise result from a purely objective primary search.

202. *Sparapani Testimony*, *supra* note 128.

203. *Id.*

204. *Id.*

205. *Id.*

206. *Id.*

207. See Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110.

Finally, and along similar lines, the fact that body-scans are more effective at detecting a wider range of dangerous items alone increases the likelihood that use of the technology will result in a larger number of false positive tests.²⁰⁸ While this fact makes body-scans more effective, it also makes them more intrusive, in that more harmless passengers will be subject to invasive secondary searches.²⁰⁹

Given these many privacy concerns, body-scans do not present a level of intrusion comparable to that of “minimally invasive” magnetometer searches. To the contrary, in their unprocessed form body-scans are more accurately comparable to the “full” search condemned by the administrative search doctrine,²¹⁰ while modified body-scans are more like a “carefully limited search of the clothing,” or a “physical frisk.”²¹¹ This fact, while alone not rendering mandatory body-scans unconstitutional, raises serious questions as to whether the Fourth Amendment would prevent the TSA from instituting the technology as a routine search mechanism.

2. *Routine Body-Scan Searches Are Not Appropriately Tailored to Satisfy the Fourth Amendment*

In addition to being far more intrusive than magnetometer searches, routine body-scan searches are not appropriately tailored to satisfy the Fourth Amendment. As discussed above, the judicial framework of airport screening searches requires that the scope of a given search is appropriately tailored in a manner that equally considers privacy and safety.²¹² Accordingly, whether routine body-scan searches are unconstitutionally oppressive necessarily requires an inquiry into whether less-invasive alternatives exist.²¹³

a. *The TSA Has Access to Minimally Invasive “Primary” Search Alternatives*

The 9/11 Commission stated plainly that “[n]o single

208. *Sparapani Testimony*, *supra* note 128.

209. *Id.*

210. *See, e.g.*, *Terry v. Ohio*, 392 U.S. 1, 26 (1968).

211. *United States v. Epperson*, 454 F.2d 769, 772 (4th Cir. 1972).

212. *See supra* Part II.

213. *See United States v. Aukai*, 497 F.3d 955, 962 (9th Cir. 2007); *see also* discussion *supra* Part III.A.

security measure is foolproof.”²¹⁴ Accordingly, the TSA is currently developing minimally invasive alternative technologies and procedures that have the potential to improve the effectiveness of primary screening searches.²¹⁵ These include the SPOT behavioral recognition program, Secure Flight watch lists, and the use of less intrusive emerging technologies such as EntryScan and handheld explosive detection devices.²¹⁶ Each of these, combined with magnetometers, can be collectively used to create a minimally intrusive, yet more proficient primary security layer.

Behavioral recognition programs such as SPOT operate in a layer of security that employs human capital to complement the use of technology in other primary searches.²¹⁷ If more widely deployed,²¹⁸ SPOT programs have the potential to effectively detect threats presented by nonmetallic weapons and explosives.²¹⁹ Despite concerns, this program is carefully designed to prevent racial bias by allowing officers to consider only “culturally independent,” objective behavioral cues.²²⁰ Furthermore, SPOT searches are unseen by a vast majority of passengers, and those who initially raise suspicion are subjected only to minimal questioning.²²¹ Of these individuals, less than twenty percent must undergo a secondary search.²²² Therefore, though the search method remains in testing,²²³ SPOT has the potential to become an additional minimally invasive tool in the

214. *Hawley Testimony*, *supra* note 23, at 4 (quoting THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON THE TERRORIST ATTACKS UPON THE UNITED STATES 392 (2005)).

215. *Kutz Testimony*, *supra* note 2, at 4. The current layered approach includes “intelligence gathering and analysis, checking passenger manifests against watch lists, and assigning undercover air marshals to certain flights.” *Id.*

216. See discussion *supra* Part I.B.

217. Karp & Meckler, *supra* note 42. “It may be the only thing I know of that favors the human solution instead of technology.” *Id.* (quoting Kip Hawley, Administrator of the Transportation Security Administration).

218. *Id.* (“Securities specialists say [SPOT] can enhance, but not replace, existing detection machines and procedures.”).

219. *Id.*

220. Press Release, Nat’l Sci. Found., New Technologies Could Make Airport Screening More Effective and Less Cumbersome, *supra* note 43.

221. Karp & Meckler, *supra* note 42.

222. *Id.*

223. Press Release, Nat’l Sci. Found., New Technologies Could Make Airport Screening More Effective and Less Cumbersome, *supra* note 43.

primary search layer.

A second screening mechanism that is currently underutilized is passenger watch-list screening, which uses a minimal level of personally identifying information to screen potentially dangerous individuals.²²⁴ The comprehensive “Secure Flight” computer watch list program, currently in development, presents an opportunity to further improve the primary search system without having to implement mandatory body-scan searches.²²⁵

Although privacy concerns exist surrounding the use of this and similar database programs,²²⁶ the TSA has been active in protecting passenger information from potential leaks,²²⁷ and continues to redesign the system with privacy and accuracy as top priorities.²²⁸ If the TSA is successful in implementing a program with accurate data that successfully secures personal information, Secure Flight has the potential to be a minimally intrusive primary search mechanism in that it merely cross-checks basic information, such as name and address, that already exist in government databases.²²⁹

The TSA is also actively developing and employing many explosive-detection technologies that are potentially less invasive than body-scans.²³⁰ These technologies, including EntryScan “puffers” and handheld detection devices, have the ability to detect explosive materials invisible to magnetometers.²³¹ Given this capability, the technologies can be more widely used as either primary, secondary, or random searches to improve general explosive detection capabilities without requiring an invasive “virtual strip search.”²³²

Finally, in addition to technological shortcomings, the TSA audits uncovered numerous *procedural* deficiencies,

224. Secure Flight Program, *supra* note 39.

225. *Id.*; see also discussion *supra* Part I.B.2.

226. Secure Flight Program, *supra* note 39.

227. *Id.* (“TSA will not collect or use commercial data to conduct Secure Flight watch list matching.”).

228. *Id.* (“TSA requested comments on the data elements through the rulemaking process to determine whether date of birth and gender should be mandatory data elements, and will consider all comments received.”).

229. *Id.*

230. See discussion *supra* Part I.B.4.

231. See discussion *supra* Parts I.B.4, I.D.

232. Yost, *supra* note 138. Alessandra Soler Meetze, executive director of the ACLU’s Arizona chapter, prefers the Entry Scan “puffers” as a less intrusive alternative to body-scans. *Id.*

including inattentive management and a general lack of effective TSO training.²³³ Therefore, technology should not be considered the single and exclusive remedial measure; the TSA must take appropriate action to ensure the vigilance of screening officers prior to resorting to invasive technologies such as body-scanners.

b. Routine Body-Scan Searches Are Not Sufficiently Effective to Justify the Additional Invasion of Privacy

The constitutional limits of primary checkpoint searches are evaluated by careful consideration of efficacy and privacy.²³⁴ Having established that potentially effective, less invasive searches exist, the question remains as to whether the additional safeguards offered by body-scan searches beyond those available from these alternatives justify the additional invasion of privacy. This comment argues that although body-scans likely offer detection capabilities beyond the available alternatives, such incremental improvements fall out of proportion with the alarming invasive qualities of the body-scan technology when it is used as a primary search.

First, body-scan machines should not be considered a “cure-all” solution in such a manner that could potentially justify their invasive qualities. The detection capabilities of body-scan machines are still largely unknown—while the TSA is pleased with the initial test results, it still remains to be seen whether body-scan searches are truly effective at detecting weapons and explosives.²³⁵ Further, in addition to contributing to the invasiveness of body-scans, the subjective characteristics of the technology, discussed previously,²³⁶ also mitigates the effectiveness of the searches themselves.²³⁷

Moreover, while the government has made steps to mitigate the invasive qualities of the technology, those very same efforts degrade the technology’s detection capability to the point where it loses the ability to detect certain

233. OIG AUDIT, *supra* note 3, at 5.

234. See discussion *supra* Part II.D.

235. See *Hawley* Testimony, *supra* note 23, at 6; Frank, *supra* note 113.

236. See discussion *supra* Part III.A.1.

237. See *id.* Further questions remain regarding the efficiency, speed, and size of the machines. See *supra* note 123 and accompanying text.

threatening objects.²³⁸ While the modified, “masking” form of the technology would likely still enhance detection capabilities over current technologies,²³⁹ potential terrorists would have a dangerous advantage: knowledge of what kinds of modern weapons can still evade detection.²⁴⁰

Therefore, in order for the technology to *significantly* enhance detection capability, the images would have to be graphic. However, the graphic, unmodified form of the technology, which exposes genitalia and fat folds among other private parts of the body,²⁴¹ is more analogous to a “full” search than it is to a “minimally invasive” magnetometer search. Therefore, despite the potential for substantial improvements in detection capability, the unmodified technology “peers beneath clothing” in a manner that per se violates the tailoring requirement of the administrative search doctrine.²⁴² Meanwhile, the *modified* images, given their sacrificed detection capability, do not offer the kind of substantial improvement in detection capability to justify the still highly invasive nature of the technology.²⁴³

Accordingly, while difficult to quantify, the detection capability of modified body-scan searches is less than perfect, if not substantially deficient. Therefore, the *undoubtedly* substantial escalation in privacy invasion over that resulting from magnetometers and alternative emerging technologies is, most likely, out of proportion with the incremental gain in detection capability. While modern travelers are accustomed to “commonplace,” minimally invasive magnetometer searches, the *modified* body-scan technology invades a basic expectation of privacy beneath one’s clothing that is not justified by anything less than a substantially significant improvement in detection capability. Consequently, because the *unmodified* version of the technology is overly invasive to

238. See Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110.

239. See Frank, *supra* note 113.

240. See *id.* (stating that the modified images lose the ability to detect C4 explosives).

241. *Airport Body Search May Reveal More Than Passengers Know*, *supra* note 126.

242. See discussion *supra* Part II.D. It seems as if the TSA would concede this point by the simple fact that they have made steps to implement the masking technology rather than proceeding with the more invasive search.

243. See discussion *supra* Part I.D.3.

the point where no improvement in detection capability would justify its use, routine body-scan searches are, in either form, unconstitutionally “more intensive than necessary;”²⁴⁴ neither the modified or unmodified versions of the technology strike the appropriate constitutional balance.

This conclusion, however, does not address whether the technology may nevertheless have a constitutionally appropriate place in a successive security layer, where the circumstances present an elevated risk of harm.

B. Modified Body-Scans Are Less Intrusive and More Effective Than Pat-Down Searches

The privacy protections built into modern body-scan technology have mitigated the Fourth Amendment concerns surrounding their use.²⁴⁵ Although more invasive than walk-through magnetometers,²⁴⁶ present day body-scans offer a less invasive and more effective security tool than pat-down searches.²⁴⁷

1. Body-Scan Searches Are Less Intrusive Than Pat-Downs

While comparing the invasive qualities of two dissimilar searches may prove problematic, modified body-scan searches appear to be less intrusive than current TSA pat-down procedures. Unlike body-scans, which produce a remote image, pat-down searches involve significant physical intrusion.²⁴⁸ The searches subject travelers to contact with intimate parts of their bodies, a process that is potentially degrading and humiliating.²⁴⁹ Furthermore, pat-downs present a risk of inappropriate mishandling and sexual groping.²⁵⁰

Conversely, modified body-scan images involve a significantly lower invasion of privacy.²⁵¹ The “chalk

244. *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)).

245. See discussion *supra* Part I.D.3.

246. See discussion *supra* Part III.A.1.

247. See discussion *supra* Part I.B.3.

248. See *Goo*, *supra* note 63; see also discussion *supra* Part I.B.3.

249. See *id.*; see also *Lew*, *supra* note 65.

250. *Lew*, *supra* note 65.

251. See discussion *supra* Part I.B.3.

outline"²⁵² form rendered by the machine is effective in masking both the identity of the individual and many of the private details of the human form.²⁵³ Furthermore, because the body-scan officer and image are remotely located, the invasion of privacy is more subtle and not as readily apparent to the awaiting passengers as is a pat-down.²⁵⁴ This machine interface is not present in pat-downs, and thus further mitigates the potential for humiliation created by the awaiting passengers and the security officer.²⁵⁵

Finally, the fact that body-scans do not require human contact appears to significantly mitigate the public's concern regarding the invasiveness of the search. While operating the pilot program in Phoenix, the TSA reports that ninety percent of individuals subject to a secondary search opted in favor of a body-scan over a pat-down.²⁵⁶ Assuming that the passengers' consent is informed (in that they know what a body-scan entails), the overwhelming passenger preference for body-scans is an indication that physical pat-down searches are more invasive than remotely located imaging.

2. *Body-Scan Searches Are More Effective Than Pat-Downs*

Finally, body-scan searches, even in their modified form, are a more effective security tool than pat-downs.²⁵⁷ Though the TSA has been somewhat secretive surrounding body-scan test results, the technology is presumptively more accurate for two primary reasons.

First, while body-scans render an image of the entire body, the effectiveness of a pat-down search is limited to its permissible parameters.²⁵⁸ Although pat-downs are

252. Press Release, Transportation Security Administration, TSA Unveils Backscatter Technology Testing at Phoenix Sky Harbor Airport, *supra* note 110.

253. See Saletan, *supra* note 67.

254. See discussion *supra* Part I.B.3.

255. See Saletan, *supra* note 67 ("Putting a machine interface between you and the examining officer protects your visual as well as tactile privacy. . . . [T]he officer who sees you on the monitor never sees you in the flesh.")

256. Transportation Security Administration, Our Approach: Whole Body Imaging, *supra* note 108.

257. See, e.g., Frank, *supra* note 113. However, the TSA will not divulge precisely what does and does not show up in the images and will not say whether the machines have yet to successfully detect dangerous objects. Yost, *supra* note 138.

258. See discussion *supra* Part I.B.3.

invasive,²⁵⁹ searching officers are not permitted to search every part of the body,²⁶⁰ such as inside religious headwear,²⁶¹ or in or around sensitive parts of the body.²⁶² Furthermore, when searching more sensitive, yet permissible areas, the officers are required to use the back of their hand, further limiting their ability to detect hidden items.²⁶³ Therefore, not only does this limit the effectiveness of the search, but it gives those wishing to surpass the security system the knowledge of where to hide a dangerous item, i.e. in-between breasts, genitalia, or in a prosthetic.²⁶⁴ Body-scans, having the ability to detect items located in these areas, are not similarly limited.

Second, the potential for human error in pat-down searches is more prevalent. While a body-scan searching officer must recognize an object projected onto a screen, a pat-down officer must be able to detect a hidden item by touch alone. Therefore, the officer conducting the pat-down must be able to differentiate between threatening and harmless objects below one or more layers of clothing, and further, the officer must be trusted to execute a comprehensive search without passing over any areas of the body. While similar shortcomings exist in body-scan searches, they are not as prevalent; the officer is not given as much discretion as to the extent of the search, nor does it take any further effort on his or her behalf to reach its permissible scope. It stands to reason, therefore, that image-based detection technology, even in its modified form, is more effective than a restricted pat-down search.

Body-scans are, therefore, a more effective, yet less invasive search than a pat-down. That being the case, the most logical use of the technology resides *in place of* pat-down

259. See discussion *supra* Part I.B.3.

260. See, e.g., Goo, *supra* note 63 ("Airport security screeners . . . will be instructed not to touch women passengers between their breasts as part of new pat-down procedures, the Transportation Security Administration said.")

261. The Sikh Coalition, TSA Develops New Procedure for Screening Turbans at U.S. Airports, Oct. 17, 2007, <http://www.sikhcoalition.org/advisories/TSADevelopsNewProcedure.htm>.

262. See Goo, *supra* note 63.

263. Legalmatch.com, Inappropriate Pat-down Searches During an Airport Security Screening, <http://www.legalmatch.com/library/article/inappropriate-pat-down-searches-during-an-airport-security-screening.html> (last visited Sept. 23, 2008).

264. *Id.*

searches in the secondary security layer.

IV. PROPOSAL: IMPLEMENT BODY-SCANS AS A SECONDARY SEARCH MECHANISM

Although body-scan machines are a promising security tool,²⁶⁵ use of the technology in an overly invasive manner is not justified merely because it adds a degree of safety.²⁶⁶ Given the particularly intrusive nature of this technology,²⁶⁷ the constitutionally appropriate “checkpoint of the future” is one where the modified form of the technology is utilized not in place of magnetometers, but instead, as a secondary search in place of pat-downs. Use of body-scans after there is “reason to conduct” a secondary search strikes the appropriate balance between the imperative goals of securing our nation’s airports and acknowledging basic privacy interests.²⁶⁸

As previously set forth, this proposal relies on two theories: that body-scans are unreasonable when used as primary searches, and that body-scans offer a more effective yet *less* intrusive alternative to pat-down searches.²⁶⁹ Given this framework, body-scan searches are most appropriate when deployed in the secondary security layer.

A. *Primary Body-Scan Searches Are Unconstitutional*

As demonstrated, use of body-scans on a routine basis is unconstitutionally “more intensive than necessary.”²⁷⁰ While the searches would likely incrementally improve detection capability, the masking technology degrades the ability of the scans to see certain threatening objects to the point where that gain falls short of a substantial improvement.

Absent a substantial gain in detection capability, the invasive qualities of the modified technology are proportionately outweighed by the substantial additional invasion of privacy.²⁷¹ Furthermore, absent the masking

265. See discussion *supra* Part I.D.

266. See discussion *supra* Part III.A.

267. See discussion *supra* Part III.A.1.

268. See *United States v. Aukai*, 497 F.3d 955, 962 (9th Cir. 2007).

269. See discussion *supra* Part III.B.

270. *Aukai*, 497 F.3d at 960 (quoting *United States v. Davis*, 482 F.2d 893, 908 (9th Cir. 1973)).

271. See discussion *supra* Part III.A.

technology, the technology ceases to provide the necessary basic Fourth Amendment protections guaranteed by the administrative search doctrine. Use of body-scans in either its original or modified form as a primary search, therefore, does not satisfy the Fourth Amendment balancing test.²⁷²

B. Secondary Body-Scan Searches Are Constitutional

After a screening officer establishes a “reason to conduct” a secondary search,²⁷³ an enhanced privacy invasion is justified if it is appropriately tailored in scope to protection of the aircraft, its passengers, and the general public.²⁷⁴ As discussed previously, body-scans are advantageous over present-day secondary searches because they offer a less-intrusive alternative that is more effective at detecting dangerous weapons and explosives.²⁷⁵ Therefore, given that reasonable pat-down searches are held to be constitutional,²⁷⁶ and that body-scans are *more* appropriately tailored secondary searches,²⁷⁷ it is logical to conclude that secondary body-scans are constitutionally permissible.

C. The TSA Must Continue to Pursue Minimally Invasive Primary and Secondary Search Tools

This proposal presupposes that the TSA will continue to develop security procedures across all levels of human capital, procedures, and technologies.²⁷⁸ Currently, available security systems lack the ability to intercept modern explosive devices.²⁷⁹ Therefore, the TSA must continue to develop and implement minimally invasive search technologies in the primary search layer so that mandatory body-scans do not, at some unforeseen time, become a necessary evil.

272. See discussion *supra* Part III.A.

273. Again, this comment does not address whether the TSA guidelines for determining when an individual fails a primary search are constitutionally justified.

274. See *supra* Part II.

275. See discussion *supra* Part III.B.

276. See, e.g., *United States v. Lopez-Pages*, 767 F.2d 776 (11th cir. 1985).

277. See discussion *supra* Part III.B.

278. See *Kutz Testimony*, *supra* note 2 (recommending that the TSA improve those three areas); see also discussion *supra* Part I.B.

279. See *Kutz Testimony*, *supra* note 2 (report to Congress on the vulnerabilities of current security screening procedures as exposed through covert testing by the Government Accountability Office).

At the same time, the TSA must continue to make strides to guarantee the constitutional application of secondary body-scan searches. This means that routine, primary searches must judge objective criteria and be designed to detect true threats. Though primary searches will necessarily lead to some false positive tests, the TSA must continue efforts to minimize the potential for arbitrary and oppressive interference with personal privacy.²⁸⁰ This means not only utilizing the current “masking” technology, but also seeking further privacy protections that do not substantially mitigate detection capability. Otherwise, shielding the general traveling public from unnecessary body-scan searches by using them in the secondary layer is just an illusory protection.

CONCLUSION

Domestic airport security systems are ill-equipped to meet the challenge of modern security threats.²⁸¹ Given the particular elusiveness of modern weapons, it is imperative that technologies are developed and implemented to remedy an inadequate security system.²⁸² However, the emerging role of technology in airport screening procedures implicates a fundamental question—to what extent should privacy be subrogated for increased public safety?

This question is particularly relevant in the case of body-scanning technologies, which have the ability to produce invasive images of the human body.²⁸³ Though apparently effective at detecting various types of threatening objects,²⁸⁴ the unmodified form of the technology produces extremely invasive images comparable to the “full” search condemned by the administrative search doctrine.²⁸⁵ While the government claims that the masking software adequately addresses these concerns, the problem is that the modification degrades the images to the point where the technology no longer has the

280. *Gibson v. State*, 921 S.W.2d 747, 757 (Tex. App. 1996). For instance, the TSA has made an effort to evaluate only objective, race neutral criteria in its SPOT program. *Hawley Testimony*, *supra* note 23.

281. *See Kutz Testimony*, *supra* note 2.

282. *Id.*

283. *See discussion supra* Part I.D.

284. *See discussion supra* Part I.D.

285. *See, e.g., Terry v. Ohio*, 392 U.S. 1, 26 (1968).

ability to detect some threatening objects. Therefore, because the modified technology still requires a substantially more invasive search over existing alternatives, the technology's diminished detection capability fails to justify using it as a primary search mechanism.²⁸⁶

Though impermissible as a primary search, body-scans do have a constitutionally appropriate place in the airport security system.²⁸⁷ If implemented appropriately as a secondary search tool, modified body-scans have the potential both to improve detection capabilities *and* to provide more respect for the privacy interests of suspicious passengers.²⁸⁸ Therefore, despite the growing prevalence of intrusive technologies, there can be some comfort in the fact that improving detection capabilities and recognizing basic Fourth Amendment rights do not have to be mutually exclusive goals.

286. See discussion *supra* Part I.D.3.

287. See discussion *supra* Part IV.

288. See discussion *supra* Part III.
