Bombing Out: Using Full-Body Imaging To Conduct Airport Searches in the United States and Europe Amidst Privacy Concerns

Étienne Lombard*

* © 2010 Étienne Lombard. J.D. candidate 2011, Tulane University Law School; B.A. 2002, Boston University. Special thanks to Dean Jancy Hoeffel and Travis LeBlanc for helpful comments and suggestions. The author thanks his father, Rene Ga. Lombard, and his mother, Rhoda L. Lombard, for their undying support.

I. INTRODUCTION

Umar Farouk Abdulmutallab forever changed how people around the world travel through airports. While aboard a flight from Amsterdam bound for Detroit, Michigan, on December 25, 2009, Abdulmutallab, a twenty-three-year-old Al-Qaeda operative from Nigeria, attempted to detonate an incendiary device hidden in the seat of his underwear.[1] Dubbed the "underwear bomber," Abdulmutallab's failed effort incited adverse reactions from aviation security experts, politicians, and passengers as each contemplated how to make flying safer.[2]

Two direct and highly anticipated consequences of the failed Christmas day bomb are the heightened security measures in airports and the accompanying changes in security protocols.[3] In some nations, such as France and Germany, questions remain about the extent of the changes.[4] Some decision makers question whether any changes are necessary at all.[5] In other nations, such as the Netherlands and Nigeria, countries through which Abdulmutallab travelled, the changes were swift: they immediately responded to the failed attack by installing full-body scanners.[6] The United States and the United Kingdom likewise

1. *Dutch, Nigerians To Use Full Body Scans for Air Travelers*, CNN.COM, Dec. 30, 2009, http://www.cnn.com/2009/WORLD/Europe/12/30/airline.terror.schiphol/index.html?iref=allsearch.

2. *See, e.g.*, Alan M. Dershowitz, *Stopping the Next "Underwear Bomber,"* FRONTPAGEMAG.COM, Jan. 6, 2010, http://frontpagemag.com/2010/01/06/stopping-the-next-"underwear-bomber"-by-alan-m-dershowitz/.

3. Press Release, The White House, Remarks by the President on Strengthening Intelligence and Aviation Security (Jan. 7, 2010), http://www.whitehouse.gov/the-press-office/remarks-president-strengthening-intelligence-and-aviation-security.

4. Robert Marquand, *Europe Warms to Full Body Scanners at Airports After Northwest Bomb Scare*, CHRISTIAN SCI. MONITOR, Dec. 30, 2009, http://www.csmonitor.com/World/Europe/2009/1230/Europe-warms-to-full-body-scanners-at-airports-after-Northwest-bomb-scare.

5. *See id.*

6. *Dutch, Nigerians To Use Full Body Scans for Air Travelers*, *supra* note 1.

implemented a search regime premised on using full-body scanners.[7] Other nations are contemplating whether to follow suit.

This latest foray, full-body or Advanced Imaging Technology (AIT) scanners, utilizes advances in digital imaging technology to scan a detailed impression of an individual's body. Specifically, AIT uses imaging technology to detect contraband hidden within clothing or on the body of individual passengers.[8] The imagers use either low frequency radio waves or weak X-rays to discover objects hidden beneath clothes.[9] Accordingly, scanners using either of these technologies depict images of passengers naked. Since these technologies capture and display images of the naked body, many commentators have described the process as a virtual strip search.[10] For these reasons, the newness of AIT, coupled with anticipation of widespread use, elicits questions about whether such devices infringe upon privacy interests, the extent to which government may invade one's privacy, and the ease with which scans enter the public realm.

This Comment examines the use of full-body scanners at airports in the United States and Europe and whether usage comports with the established privacy laws. Part II discusses the events leading to the push for employing AIT at airports in the United States and the European Union (EU). Part III discusses AIT, presents the technologies used to effect body scans, and discusses the standard operating procedures levied for using AIT. Part IV analyzes the legality of airport searches under the applicable laws. Part V identifies the vulnerabilities, challenges, and future implications of employing AIT at airports. Part VI concludes by assessing the scope of the breach of privacy and presents key recommendations that further advance the stated government objective of protecting public safety while concomitantly protecting privacy rights.

---

7. Press Release, The White House, *supra* note 3; Marquand, *supra* note 4.

8. TRANSP. SEC. ADMIN., U.S. DEP'T OF HOMELAND SEC., PROCUREMENT SPECIFICATION FOR WHOLE BODY IMAGER DEVICES FOR CHECKPOINT OPERATIONS 1 (2008), http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf.

9. Leila Atassi & James Ewinger, *Manufacturer Says Full Body Scanners at Airports Are a Valuable Tool in Fighting Terror*, CLEVELAND.COM, Dec. 28, 2009, http://blog.cleveland.com/metro/2009/12/manufacturer_says_full_body_sc.html.

10. Kit Eaton, *Full-Body Scanners at Airports: The Good, the Bad, and the Ugly*, FASTCOMPANY.COM, Dec. 30, 2009, http://www.fastcompany.com/blog/kit-eaton/technomix/full-body-scanners-airports-good-bad-and-ugly.

II. BACKGROUND: THE ROAD TO EMPLOYING ADVANCED IMAGING TECHNOLOGY

The most significant changes to airport security occurred after the September 11, 2001 (9/11) attacks on the United States. Prior to the attacks, many airports around the world relied on magnetometers, commonly called metal detectors, as the primary means of searching individuals for weapons that could facilitate "sky-jacking." However, the advent of terrorists using box-cutters,[11] chemicals,[12] or other nonmetallic weapons to overtake airplanes for the express purpose of wreaking destruction manifested the growing inefficacy of using magnetometers alone.[13] Magnetometers possess inherent limitations in the scope of their search ability because they are only able to detect metals. However, they frequently fail to accomplish even this purpose.[14] Before the attacks, weapons passed undetected in sixty-eight to ninety-five percent of all government-conducted tests.[15] As one passenger with surgically replaced metal knees observed in 2001, unlike magnetometers in a local Florida courthouse with less traffic and security personnel, those in several airports failed to alert security agents when he walked through them.[16] Likewise, a retired Federal Aviation Administration Security Inspector reported that he smuggled weapons past airport security with regularity, achieving a ninety-five percent success rate in 2003.[17] More recently, in 2008, one passenger carried a loaded gun through a security checkpoint; the weapon was not detected by TSA screeners.[18]

Principally, magnetometer-based search regimes rely upon outdated technology to discover threats levied by terrorists who have adapted their

---

11. James Barron, *Thousands Feared Dead as World Trade Center Is Toppled*, N.Y. TIMES, Sept. 11, 2001, http://www.nytimes.com/2001/09/11/national/11WIRE-PLAN.html.

12. *See, e.g.*, A.G. Sulzberger & William K. Rashbaum, *Guilty Plea Made in Plot To Bomb New York Subway*, N.Y. TIMES, Feb. 23, 2010, at A1. While on a December 2001 flight from Paris to Miami, Richard Reid attempted to detonate a triacetone triperoxide (TATP)-based bomb hidden in his shoe. TAPT is a powerful, combustible, and highly unstable compound comprised of drain cleaner, bleach, and acetone. Philippe Naughton, *TATP Is Suicide Bombers' Weapon of Choice*, TIMES ONLINE, July 15, 2005, http://www.timesonline.co.uk/tol/news/uk/article544334.ece.

13. *See* Naughton, *supra* note 12.

14. Blake Morrison, *Airport Security Failures Persist*, USA TODAY, July 1, 2002, at A1; *see also* Airline Pilots Sec. Alliance, *Airport Weapons Screening Reliability: < 5%*, SECURE-SKIES.ORG, http://www.secure-skies.org/weaponsscreening.php (last visited Aug. 16, 2010).

15. Airline Pilots Sec. Alliance, *supra* note 14.

16. *Metal Detectors at TIA Fail To Ensure Safety*, ST. PETERSBURG TIMES, Sept. 18, 2001, http://www.sptimes.com/News/091801/Pasco/Use_lottery_to_aid_vi.shtml.

17. Airline Pilots Sec. Alliance, *supra* note 14.

18. *Loaded Gun Slips Through Airport Security*, CNN.COM, Jan. 23, 2008, http://www.cnn.com/2008/US/01/23/airport.gun/index.html.

techniques to minimize detection. As the Underwear Bomber illustrates, terrorists use powders and other nonmetals to promote their destructive agenda. Recognizing these strategic changes and the vulnerabilities of a system that fails to account for them, the United States and the United Kingdom both contemplated AIT by 2007;[19] the United States first began an AIT pilot program that same year.[20] Thus while Abdulmutallab created a heightened impetus for implementing new scanning methodologies, the United States and Members of the EU previously considered implementing a more sophisticated, comprehensive means of searching than magnetometers and pat downs.

A. United States

In the wake of 9/11, Congress responded to the potential threat of attack by passing the Aviation and Transportation Security Act (ATSA), which federalized airport security and authorized the creation of the Transportation Security Administration (TSA).[21] ATSA furnishes the TSA with authority "to conduct research, development, testing and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction."[22] To fulfill this responsibility the TSA explored new methods of detection. "Since fiscal year 2002, the Transportation Security Administration . . . invested over $795 million" on testing passenger-screening technologies.[23] The TSA first explored AIT in 2007, introducing forty millimeter wave (MMW) scanners to airports around the country.[24] A second pilot program, which commenced during August of 2009, featured scanners applying backscatter

---

19. Press Release, TSA, TSA Test Second Passenger Imaging Technology at Phoenix Sky Harbor Airport (Oct. 11, 2007), http://www.tsa.gov/press/release/2007/press_release_10112007.shtm.

20. Calvin Biesecker, *TSA Awards Whole Body Imaging Contract to Rapiscan*, ALL BUSINESS, Oct. 1, 2009, http://www.allbusiness.com/government/government-bodies-offices-government/13377309-1.html.

21. *See* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG NO. 04-37, AUDIT OF PASSENGER AND BAGGAGE SCREENING PROCEDURES AT DOMESTIC AIRPORTS (2004), http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_04_37_0904.pdf.

22. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR TSA WHOLE BODY IMAGING 3 (2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf (internal quotation marks omitted).

23. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-128, AVIATION SECURITY: DHS AND TSA HAVE RESEARCHED, DEVELOPED, AND BEGUN DEPLOYING PASSENGER CHECKPOINT SCREENING TECHNOLOGIES, BUT CONTINUE TO FACE CHALLENGES (2009), http://www.gao.gov/new.items/d10128.pdf.

24. Biesecker, *supra* note 20.

technology; two months later the TSA agreed to purchase 150 such imagers.[25]

ATSA also authorizes the TSA to hire agents, institute a series of primary and secondary screening mechanisms, and deploy air marshals charged with preserving in-flight security.[26] Pursuant to this charge, the TSA instituted a series of mandatory passenger screening procedures comprised of, inter alia, pat downs, magnetometer tests, and a requirement that travelers remove both outer clothing and shoes.[27] These procedures have prompted frequent complaints from passengers upset about the hassle of removing clothes, standing in long queues, and undergoing pat downs. The heightened interpersonal interaction also causes consternation because this process can generate false positives.[28] Recent observations, like the passenger who successfully carried a loaded gun through a checkpoint at Ronald Reagan Washington National Airport before self-reporting, echo passenger concerns and demonstrate continued procedural inefficacy.[29] During congressionally mandated tests of the screening system,[30] federal inspectors routinely smuggled improvised explosive devices (IEDs) or IED components through checkpoints at various airports.[31] Understandably, concerns abound over passengers smuggling contraband, weapons, or explosives onto airplanes.

As discussed *infra*, AIT eliminates many of these problems because scanning is quick, comprehensive, and obviates the need for security personnel to invade passengers' personal space. Despite these advantages, the scans reveal pornographic-like images of passengers.[32] Mindful of the potentiality for abuse by the TSA or its agents, privacy advocates have sought to implement restrictions on AIT scans through legislative and judicial forums.[33] To curb potential privacy intrusions, Congressman Jason Chaffetz introduced the Whole Body Imaging

---

25. *Id.*

26. 49 U.S.C. § 44901(a)-(e) (2006); *see also id.* §§ 44903(a)-(e), 44917(a).

27. *See id.* § 44903(a)-(e).

28. *RPT—UPDATE 6 – 'Explosive' at California Airport Found to be Honey*, REUTERS, Jan. 5, 2010, http://www.reuters.com/assets/print?aid=USN057258620100106.

29. *See* Loaded Gun Slips Through Security, *supra* note 18.

30. 49 U.S.C. § 44904(a)-(b).

31. 60 Minutes, *Screening the TSA*, CBS NEWS.COM, Dec. 21, 2008, http://www.cbsnews.com/video/watch/?id=5205160n&tag=related;photovideo; *GAO: Investigators Pass Security at 19 Airports with Bomb Parts*, CNN.COM, Nov. 14, 2007, http://www.cnn.com/2007/US/11/14/gao.airport.security/index.html.

32. Although pornographic-like may be hard to define, as the late Supreme Court Justice Potter Stewart remarked, "I know it when I see it." Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

33. *See* H.R. 2027, 111th Cong. (2009), *available at* http://www.govtrack.US/congress/billtext.xpd?bill=h111-2027.

Limitations Act of 2009, which requires that AIT scans be used solely as a secondary means of passenger screening.[34] Under its terms, passengers would only be required to undergo an AIT scan upon failing a primary test, such as magnetometer screening.[35] The legislation also creates an affirmative right for passengers to request and receive a pat-down search and imposes criminal penalties upon any government employee who knowingly stores, transfers, shares, or copies images produced by AIT scanners.[36]

Attacking AIT through the judiciary, a privacy group, the Electronic Privacy Information Center (EPIC), filed a lawsuit against the Department of Homeland Security, seeking to compel the Department to provide internal documents that manifest a failure to establish any meaningful privacy safeguards for passengers undergoing an AIT scan.[37] In short, EPIC sought to expose an alleged contradiction in the Department's publicly stated position that a privacy algorithm guards against scanners depicting naked images of each passenger. The lawsuit followed a previous failed attempt to deter AIT use.[38] As part of the Privacy Coalition, a group comprised of at least twenty-four privacy organizations, EPIC sent a letter to Homeland Security Secretary Janet Napolitano stating, "'Your agency will be capturing the naked photographs of millions of American air travelers suspected of no wrongdoing.'"[39]

Despite these privacy concerns, TSA officials adamantly advocated using AIT because it can uncover threats, such as ceramic knives or IED components, which are inherently beyond the limited scope of metal detectors.[40] Thus, the foremost advantage of using AIT scans is that they

---

34. *Id.* The legislation was approved by more than 300 of the 435 Members of the House of Representatives and is currently awaiting Senate approval. Jason Chaffetz, *Don't Let Security Scanners Erase Our Privacy*, CNN.COM, Dec. 31, 2009, http://www.cnn.com/2009/OPINION/12/31/chaffetz.whole.body.images.privacy.security/index.html.

35. H.R. 2027.

36. *Id.*

37. Complaint for Injunctive Relief, Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., No. 09-02084 (D.D.C. 2009), *available at* http://epic.org/privacy/airtravel/tso_foia_suit.pdf. The complaint arose because the Department refused to comply with the request filed pursuant to the Freedom of Information Act. *Id.*

38. *Id.*

39. John Schwartz, *Debate over Full-Body Scans vs. Invasion of Privacy Flares Anew After Incident*, N.Y. TIMES, Dec. 30, 2009, at A14 (quoting the Coalition's letter).

40. *See* Michael Chertoff, *Plugging a Security Gap*, WASH. POST, Jan. 1, 2005, at A15. Since leaving office, former head of Homeland Security, Michael Chertoff, has been criticized by some pundits for leaving his former governmental position to advocate for body scanners because his security consulting agency clientele includes an AIT manufacturer. Kimberly Kindy, *Chertoff Accused of Abusing Public Trust by Touting Body Scanners*, WASH. POST, Jan. 1, 2010, at A07;

allow security administrators to discover nonmetallic items previously deemed untraceable. The introduction of AIT in airports is not the only use of AIT by governments in the United States. Currently, a federal courthouse in Virginia, along with at least one state courthouse in Colorado, California, and Illinois, employ AIT scanners.[41] The Pennsylvania Department of Corrections also uses AIT.[42] These developments suggest that the use of AIT will expand to courts, prisons, and other government facilities throughout the country.[43] Thus it seems likely that AIT, the cutting edge of detection and prevention methodology, is the future of security.

B. European Union

The EU establishes a set of common practices for all Member States to follow. Pursuant to article 4(2) of the European Community Regulation No. 300/2008, the European Commission (EC) possesses the authority to adopt aviation security methods for all twenty-seven Member States.[44] In accordance with this regulation, the EU strongly considered the use of AIT scans in 2008[45] as a means of overcoming challenges inherent in using magnetometers and pat downs: an inability to detect nonmetallic weapons, variations in the quality of pat downs, passenger complaints about the invasiveness of pat downs, the time required to conduct pat downs, and the expense incurred to employ the overall system.[46] To ascertain the impact of AIT scanners on human rights, privacy, personal dignity, and data protection, the European Parliament authorized the EC to conduct an assessment, or consultation,

---

see also Cam Simpson & Daniel Michaels, *TSA Pressed on Full-Body Scans Despite Concerns*, WALL ST. J., Jan. 9-10, 2010, at A2.

41. *Safety & Privacy Concerns Regarding the Millimeter Wave Whole Body Imager*, THE TSA BLOG (Apr. 24, 2008, 3:10 PM), http://www.tsa.gov/blog/2008/04/safety-privacy-concerns-regarding.html.

42. *Id.*

43. *See id.*

44. Commission Regulation 300/2008, of the European Parliament and the Council of 11 March 2008 on Common Rules in the Field of Civil Aviation Security and Repealing Regulation (EC) No. 2320/2002, 2008 O.J. (L 97) 72, 75-76 (EC) [hereinafter Commission Regulation 300/2008], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF.

45. Press Release, European Comm'n, Aviation Security: Workshop on Body Scanners (Nov. 7, 2008), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/684&format=HTML&aged=0&language=EN&guiLanguage=en.

46. European Comm'n, Consultation, *The Impact of the Use of Body Scanners in the Field of Aviation Security on Human Rights, Privacy, Personal Dignity, Health and Data Protection*, at 2, http://ec.europa.eu/transport/air/consultations/doc/2009_02_19_body_scanners_questionnaire.pdf (last visited July 30, 2010).

comprised of a questionnaire distributed to privacy groups, airport operators, and aviation security experts.[47] The consultation also established a Body Scanner Task Force charged with compiling the resultant data, which would ultimately contribute to shaping AIT implementation legislation.[48] However, the EC's attempt to create rules on the use of full-body scanners met stark resistance from Member States fraught with privacy concerns[49] and negative publicity that summarily considered the scanners a violation of dignity and human rights.[50] Subsequently, the EU abandoned a coordinated enterprise in 2008.[51] Before doing so, the EC agreed that passengers must have the option of declining a body scan and that Member States must not be compelled to use AIT.[52] Accordingly, aside from these determinations, no EU-wide regulations on AIT exist. Despite the lack of a coordinated effort, Member States remain free to implement AIT as long as implementation and use comports with EU laws or national regulations.[53] Within this framework, the United Kingdom and Italy have joined the Netherlands in implementing either a pilot or permanent AIT regime, with emphasis on flights destined for the United States.[54]

---

47. *Id.*

48. *Id.* The questionnaire and Body Scanner Task Force were part of a public-private dialogue to address the previously mentioned concerns and ultimately to make a recommendation on whether AIT should be adopted. *Id.*

49. Simpson & Michaels, *supra* note 40. At least one member of the European Parliament executed a petition to fellow Members, exhorting them to prevent the use of AIT at airports because the "advantages of such scanners [fail to] outweigh the serious violation of people's personal privacy." Notice to Members of the European Parliament, Petition 1556/2008 by Johannes Koll (German) on Body Scanners in Airports (July 7, 2009), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-427.110+01+DOC+PDF+V0//EN&language=EN.

50. Marquand, *supra* note 4.

51. *EU Members Divided over Airport Body Scans*, BBC NEWS, Jan. 7, 2010, http://news.bbc.co.uk/2/hi/europe/8446604.stm. "European Members of Parliament voted 361 against and 16 in favor (with 181 abstentions)" on the subject of body scans. Marquand, *supra* note 4.

52. ERIK GRUNEWALD ET AL., GERMAN AEROSPACE CTR., ANNUAL ANALYSES OF THE EUROPEAN AIR TRANSPORT MARKET: ANNUAL REPORT 2008, at 234 (2008), http://ec.europa.eu/transport/air/observatory_market/doc/annual_2008.pdf.

53. *EU Members Divided over Airport Body Scans*, *supra* note 51.

54. *Id.* EU Justice Commissioner Viviane Reding articulated the intent to address privacy concerns associated with AIT by updating EU privacy laws because she is "convinced that body scanners have a considerable privacy-invasive potential. Their usefulness is still to be proven. . . . Therefore I cannot imagine this privacy-intrusive technique being imposed on us without full consideration of its impact." Viviane Reding, Info. Comm'r, European Union, Keynote Speech at the European Parliament Data Protection Day: Privacy: The Challenges Ahead for the European Union (Jan. 28, 2010), http://europa.eu/rapid/pressReleaseAction.do?reference=SPEECH/10/16. Likewise, Transport Secretary of Belgium, Etienne Schouppe, decries use of AIT as being "excessive" and considers current security measures sufficient. *EU Members Divided over*

Reactions to using AIT have been mixed. In the United Kingdom, after scans revealed both genitalia and breast implants, advocates raised concerns that use of the imagers could violate the Protection of Children Act (1978), which makes illegal any process that creates "an indecent image or a 'pseudo-image' of a child."[55] Pursuant to this antichild pornography statute, the program commenced only after persons under eighteen received a scanning exemption.[56] Subsequently, Parliament revoked the exemption and parties under eighteen must now be scanned.[57]

Like the advocates concerned with whether the scans of children constitute child pornography, the general public also voiced privacy concerns. In a poll conducted by the Guardian Online (U.K.), approximately seventy-three percent of participants expressed that the introduction of body scanners represented an unnecessary intrusion of privacy.[58] Despite these sentiments, the approval rate, measured by the percentage of passengers preferring body scans, increased from seventy-two percent in the three weeks prior to the underwear bomb to ninety-two percent during the second week of 2010.[59] Reduced stress and the expeditious pace of scanning likely explain the twenty percent increase. Correspondingly, many who once characterized AIT as a violation of privacy and human dignity before Abdulmutallab's failed underwear bomb have since reversed their positions.[60] Reflecting the underlying rationale for this change of heart, one German commentator remarked, "'Privacy finds its limits when the life of others is at risk, and that is the case in this matter. People who are worried and put their privacy above the lives of others should not underestimate the extent to which Germans would like to stay alive.'"[61]

Airport Body Scans, *supra* note 51. In contrast, Italy announced plans for a pilot program at airports in Rome, Milan, and Venice while the United Kingdom announced plans to adopt a permanent AIT screening strategy. *Id.*

55. Alan Travis, *New Scanners Break Child Porn Laws*, GUARDIAN, Jan. 4, 2010, http://www.co.uk/politics/2010/Jan/04/new-scanners-child-porn-laws.

56. *Id.*

57. *Air Passengers Who Refuse a Full Body Scan To Be Barred from Their Flights*, MAILONLINE, Feb. 2, 2010, http://www.dailymail.co.uk/news/article-1247715/Passengers-refuse-body-scan-Heathrow-Manchester-airports-barred-flights.html.

58. *Scan or Scam?*, GUARDIAN, Jan. 4, 2010, http://www.guardian.co.uk/commentisfree/libertycentral/poll/2010/jan/04/terrorism-body-scanner-airport.

59. Helen Carter, *More Passengers Agree to Full-Body Scan in UK Airport Trial*, GUARDIAN, Jan. 7, 2010, http://www.guardian.co.uk/uk/2010/jan/07/full-body-scan-uk-airport.

60. *See* Marquand, *supra* note 4.

61. *Id.* (quoting a front-page editorial in the German daily *Die Welt*).

III. AIT: HOW IT WORKS AND HOW IT IS BEING APPLIED

A. Function: The Technologies Used

Two forms of body scanning technology currently dominate the AIT market: millimeter wave and backscatter. An alternate form of scanning, thermal sensory imaging (TSI), is available but has not yet been adopted by the TSA or comparable agencies abroad. While the clear images produced by the scans provide for a more comprehensive search of the prospective passenger, the duration of time required to conduct body scans, approximately fifteen to thirty seconds,[62] also makes AIT scans appealing to aviation security agents and passengers. This is in sharp contrast to pat-down searches, which can consume two to four minutes.[63] Also, the standard imagers arrive equipped with both a transfer and a memory function, enabling each operator to transfer, retain, and preserve scans for future use or storage in a database.[64]

1. Backscatter Technology

Rapiscan Systems,[65] American Science and Engineering,[66] and Tek84[67] have each developed contraband detection systems using backscatter technology. This material dependent scattering technology captures data from x-ray photons scattered about the thing being scanned and plots the resultant pattern.[68] As used with whole body imaging, each scan exposes the prospective passenger to a high-speed yet thin, low intensity x-ray beam.[69] The beam then reflects off the individual's body and any objects placed or carried thereon. Subsequently, the impression created by the scan is converted into a digital image and displayed on a remote monitor.[70]

---

62. Jessica Ravitz, *Airport Security Bares All, or Does It?*, CNN.COM, May 18, 2009, http://www.cnn.com/2009/TRAVEL/05/18/airport.security.body.scans/.

63. *Id.*

64. TRANSP. SEC. ADMIN., *supra* note 8, at 4-5. Although the scanners, as manufactured, possess the ability to transfer and retain such images, the TSA purports that these functions are deactivated prior to shipping pursuant to its request. *Id.*

65. *Backscatter for People Screening*, RAPISCAN SYS., http://www.rapiscansystems.com/sec1000.html (last visited Mar. 3, 2010).

66. *Z Backscatter*, AM. SCI. & ENG'G, INC., http://www.as-e.com/products_solutions/z_backscatter.asp (last visited Mar. 3, 2010).

67. *Partial Body Scanner for Checkpoint Screening*, TEK84 ENG'G GROUP, http://tek84.com/castscope.html (last visited Mar. 3, 2010).

68. *Z Backscatter*, *supra* note 66.

69. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 22.

70. Sample images abound on the Internet. *Imaging Technology*, TRANSP. SEC. ADMIN., http://www.tsa.gov/approach/tech/ait/index.shtm (last visited Mar. 3, 2010). Unlike the current interaction of backscatter images, early versions depicted either a chalk-like outline of a detailed,

2. Millimeter Wave Technology

Smiths Detection,[71] and L-3 Communications[72] supply high-resolution contraband detection systems premised upon MMW. MMW applies nonionizing radio frequency energy in the millimeter wave spectrum to create an image based on the energy reflected from the individual's body.[73] Afterwards, a three-dimensional image resembling a negative is displayed on a remote monitor for analysis.[74]

3. Thermal Sensory Imaging

Florida based Thermal Matrix developed TSI to provide a concealed object detection mechanism that compromises neither passenger modesty nor privacy.[75] TSI uses sensory technology designed for the United States military and proprietary analytical software to evaluate and identify potential threats.[76] The output generated from scans displays an outline of the individual along with any image that blocks heat emanating from the human body.[77] This is in direct contrast to either millimeter wave or backscatter technologies, which depict virtual nude images. Also distinct from millimeter wave or backscatter technologies, TSI allows image readers to detect powders, liquids, and gels. It also permits security personnel to scrutinize large crowds.[78]

---

yet ghostly image of the person scanned. Julia Layton, *Do "Backscatter" X-ray Systems Pose a Risk to Frequent Fliers?*, HOWSTUFFWORKS, Feb. 27, 2007, http://science.howstuffworks.com/backscatter.htm.

71. *Eqo: Revolutionising People Screening*, SMITHS DETECTION, http://www.smithsdetection.com/eqo.php (last visited Sept. 12, 2010).

72. *Advanced Imaging Technology*, L3 COMMC'NS SEC. & DETECTION SYS., http://www.dsxray.com/products/advancedimagingtech.htm (last visited Mar. 3, 2010).

73. U.S. DEP'T OF HOMELAND SEC., *supra* note 22; *see also Imaging Technology*, *supra* note 70.

74. Julia Layton, *supra* note 70.

75. *Airline Security: Airport Security Screening Without Privacy Violations*, THERMAL MATRIX, http://www.thermalmatrixusa.net/airline-security.html (last visited Aug. 6, 2010).

76. *Id.*; *see also Products: ACT*, THERMAL MATRIX, http://www.thermalmatrixusa.net/act.html (last visited Aug. 7, 2010).

77. Cam Simpson & Daniel Michaels, *Effective Screenings with No Privacy Concerns*, WALL ST. J. ONLINE, http://online.wsj.com/video/effective-screenings-with-no-privacy-concerns/DAF82A59-6F84-4619-8CCD-D3BBF819E8C4.html (last visited Mar. 3, 2010); *see also Thermal Matrix White Paper on Airport Security and the Privacy of Full Body Scanners*, THERMAL MATRIX 4 (2009), http://www.thermalmatrixusa.net/pdf/AirportWhitePaper2.docx.

78. *Id.*

B. Application: Policies

1. Standard Operating Procedures for AIT in the United States

Pursuant to TSA policy, AIT scans are not mandatory.[79] Instead, passengers possess the option of undergoing a body scan. Accordingly, individuals may choose instead to receive a pat down from a designated TSA agent.[80] Also, to concomitantly placate privacy concerns discussed *supra* and to comply with the Fair Information Practice Principals (FIPPs) developed by the Department of Homeland Security Privacy Office, the TSA instituted policies aimed at protecting passenger privacy.[81] Although the full range of procedures governing the scanning process, including regulations on the behavior of AIT remote operators, remains unpublished in light of their sensitive nature,[82] the procedure provides:

- operators will be absolutely prohibited from bringing any device with photographic ability into the viewing area.
- the viewing operator will be located remotely, rendering the viewer unable to see who is being scanned.
- the constraints of the machine permit that one scan must be cleared before the next image becomes viewable.[83]
- upon an "anomaly," the TSA agents on the scene will be alerted by radio and the individual will undergo a physical pat down in the area of the body where the anomaly was identified.[84]

To further mollify privacy concerns, the TSA announced a special arrangement with the manufacturers to modify the scanners.[85] Pursuant to these agreements, manufacturers began installing a blurring feature

---

79. *Imaging Technology*, *supra* note 70.

80. *Id.*

81. U.S. DEP'T OF HOMELAND SEC., *supra* note 22, at 6. The principles effectively serve as best practices, guiding all department procedures that impact citizens' privacy. The principles are (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, (8) Accountability and Auditing. *Id.* at 6-9.

82. *Id.* at 5. An allegedly outdated TSA manual surfaced on the Internet during late 2009. The manual details the processes and procedures that airport screeners must follow, including a mandate to screen anyone with a passport from Cuba, North Korea, Yemen, and Somalia, along with other confidential information. Bob Orr, *Unredacted TSA Manual Leaked Online*, CBS NEWS, Dec. 8, 2009, http://www.cbsnews.com/stories/2009/12/08/eveningnews/main5942088.shtml; *see also* TRANSP. SEC. ADMIN., U.S. DEP'T OF HOMELAND SEC., AVIATION SECURITY, SCREENING MANAGEMENT STANDARD OPERATING PROCEDURES (2008), *available at* http://cryptome.org/tsa-screening.zip.

83. *Imaging Technology*, *supra* note 70.

84. U.S. DEP'T OF HOMELAND SEC., *supra* note 22.

85. *Imaging Technology*, *supra* note 70.

wherein the machines blur faces.[86] Still, a casual inspection of a scanned image reveals that genitalia remain discernable.[87] Supplemental modifications purportedly obviate the scanners' ability to collect, store, and transmit scanned images; the manufacturer will disable these functions after the devices arrive at airports.

2. Standard Operating Procedures for AIT in the European Union

Because the EU abandoned a coordinated program, there exist no EU-wide standard operating procedures. However, "aviation-security specialists from the European Union, airlines and airports" left open the possibility for developing such standards when they unanimously agreed upon "the need for a coordinated EU approach [in combating terrorism targeted at transportation outlets], which could include" the use of full-body scanners.[88] Thus, it follows that while no EU-wide standardized security protocols exist, they are imminent. Yet the absence of a coordinated approach towards updating airport security methods does not absolutely preclude Member States from establishing their own strict policies and procedures, such as implementing AIT.[89] The United Kingdom, after electing to use AIT, began instituting guidelines for operating the scanners, protecting passenger modesty, and preserving passenger privacy.[90] As of February 1, 2010, key principles of the Interim Code of Practice for AIT specify:

- the person being scanned may request that the screen reader is of the same sex
- collected images must be immediately destroyed after a scanning analysis
- screen readers must be limited to viewing one image at a time
- there must be no method of reproducing or transferring the images
- airport operators must give passengers an opportunity to provide evidence of their age, gender, race, ethnic origin and religion or beliefs
- passengers must be given the following notice: "'For the benefit of all passengers' security, passengers may be required to be screened

86. *Id.*
87. Carter, *supra* note 59.
88. Simpson & Michaels, *supra* note 40.
89. *Id.*
90. DEP'T FOR TRANSP., INTERIM CODE OF PRACTICE FOR THE ACCEPTABLE USE OF ADVANCED IMAGING TECHNOLOGY (BODY SCANNERS) IN AN AVIATION SECURITY ENVIRONMENT 3-4 (2010), *available at* http://www.dft.gov.uk/pgr/security/aviation/airport/bodyscanners/codeofpractice/pdf/cop.pdf.

> using body scanning equipment. Screening will be conducted by security officers acting on behalf of the airport operator. Images of passengers will not be saved.'"[91]

In a written statement to the House of Commons, Lord Andrew Adonis, Secretary of State for Transport added that although a small number of passengers will be selected for scanning during the initial deployment, a permanent policy mandates that anyone who declines a scan will not be permitted to fly.[92] Further, "[p]assengers must not be selected on the basis of personal characteristics (i.e. on a basis that may constitute discrimination such as gender, age, race or ethnic origin)."[93] Succinctly summarizing proponents' argument for using AIT at airports throughout the world, Lord Adonis also remarked, "These scanners are designed to give airport security staff a much better chance of detecting

---

91. *Id.* The full text of the guidelines germane to this discussion reads as follows:

> An effective privacy policy must be put in place by the airport operator to protect passengers when being screened by body scanners. The policy must include a requirement that the equipment is sited in such a way to ensure that the Security Officer(s) conducting analysis of the image (the screener) must not be able to see the person whose image they are viewing and the Security Officer(s) resolving any issues identified by the body scanner should not be able to see the image of the person being searched. A person selected for scanning may request that the screen reader is of the same sex as the person. If further resolution is required (i.e. a targeted hand search), an appropriate method of communication must be employed between the screen reader and the body searcher that does not include the use of the image to ensure that this privacy is protected.
>
> In order to classify a passenger's security status when using a body scanner, it is necessary to capture an image for analysis. The analysis is currently conducted by a Security Officer and in the future it may be possible to be analysed automatically by the machine.
>
> Immediately after the scanning analysis is completed and the passenger moves away from the body scanner, all images of the passenger must be destroyed and irretrievable. Whilst an image is being analysed, it must only be possible for the screener to view that image. In exceptional circumstances where a screener believes there is a viable threat to the safety of passengers or staff, an additional appropriate Security Officer may be required to view the image. There must be no method of copying or transferring images.
>
> Communications will be available at the security screening area to inform passengers that "For the benefit of all passengers' security, passengers may be required to be screened using body scanning equipment. Screening will be conducted by security officers acting on behalf of the airport operator. Images of passengers will not be saved." Airport operators must provide to persons selected for screening the opportunity to provide details of their age, gender, race, ethnic origin and religion or beliefs.

Id.

92. Written Statement by Lord Andrew Adonis, Sec'y of State for Transp. (Feb. 1, 2010), http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/press/speechesstatements/statements/adonis20100201.

93. *Id.* (internal quotation marks omitted).

explosives or other potentially harmful items hidden on a passenger's body."[94]

IV. THE LEGALITY OF AIRPORT SEARCHES: SEARCHING THE PERSON

A. United States

The Fourth Amendment prescribes limitations on the scope of a permissible search by government actors. It provides:

> The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[95]

Reasonableness, the hallmark of any Fourth Amendment inquiry, is measured by balancing the degree to which a challenged government action intrudes upon an individual's privacy against the degree to which the intrusion promotes a legitimate government interest.[96] Consequently, the scope of the search must reasonably fit the need justifying it.[97]

Within this construct, the Supreme Court of the United States has reasoned that the Fourth Amendment allows for limited circumstances during which law enforcement officials may conduct a search absent individualized suspicion, a precursor to the requirement of probable cause.[98] Consistent with this definition, airport searches generally fall within this limited class.[99] The intrusions, termed "administrative" searches, operate within the scope of the Fourth Amendment as long as they are part of a greater regulatory scheme targeted at a specific group of people instead of a single specific person.[100]

---

94. *Id.*
95. U.S. CONST. amend. IV.
96. Terry v. Ohio, 392 U.S. 1, 20-21 (1968).
97. *Id.*
98. *Id.* at 27.
99. United States v. Hartwell, 436 F.3d 174, 178 (3d Cir. 2006). While acknowledging the necessity of airport administrative searches, the United States Supreme Court has not yet specifically addressed them. *Id.* at 178 n.5. In *City of Indianapolis v. Edmond*, the Court commented in dicta, "Our holding . . . does not affect the validity of . . . searches at places like airports . . . , where the need for such measures to ensure public safety can be particularly acute." 531 U.S. 32, 47-48 (2000). Likewise, in *Chandler v. Miller*, the Court observed that "blanket suspicionless searches . . . may rank as 'reasonable'—for example, searches . . . routine at airports." 520 U.S. 305, 323 (1997).
100. *See* Camara v. Municipal Court, 387 U.S. 523, 530 (1967); *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1999) (holding that a checkpoint aimed at identifying drunk drivers is constitutional).

The seminal case in this area is *City of Indianapolis v. Edmond*.[101] In *Edmond*, the Court found that administrative searches conducted at roadway checkpoints violated the Fourth Amendment. The City of Indianapolis installed six checkpoints with the aim of constricting the flow of illegal narcotics.[102] During stops of a predetermined quantity of vehicles, police followed written procedures when approaching the vehicle; requesting a license and registration; and advising the driver that police are searching for drugs.[103] An officer would stand outside the vehicle, scanning the driver for signs of intoxication and engaging in a plain-view examination of the vehicle's contents while another officer and drug sniffing dog walk about the vehicle.[104] The Court determined that the stop, seizure, and search violated the Fourth Amendment because the primary purpose of the checkpoint was to discover proof of ordinary criminal malfeasance.[105] The Court reasoned that although it has allowed suspicionless searches when affected to achieve a "special need[] beyond the normal need for law enforcement," such as regulating border access, the purpose of the search conducted by police in *Edmond* was to root out ordinary criminal activity.[106] In short, the Court found that the City of Indianapolis using suspicionless to reduce the flow of narcotics through the city limits, violated the Fourth Amendment because narcotics interdiction does not rise to the level of a "special need."[107] In reaching its conclusion, the Court reasoned that the absence of some individualized suspicion or threat to public safety, such as an imminent terrorist attack, renders unjustifiable an effort to broadly control criminal activity.[108]

Hence, despite the Fourth Amendment's requirement of probable cause, the government may intrude upon individual privacy to conduct an airport search despite a lack of reasonable suspicion. Accordingly, courts consistently uphold the constitutionality of warrantless airport searches on the basis of administrative necessity: the government must conduct such searches to guard public safety and to protect the public in instances where the risk of harm is both real and substantial.[109]

---

101. *Edmond*, 531 U.S. 32.
102. *Id.* at 34.
103. *Id.* at 35.
104. *Id.*
105. *Id.* at 41-42.
106. *Id.* at 37-39 (internal quotation marks omitted).
107. *Id.* at 42-44.
108. *Id.* at 47-48.
109. Chandler v. Miller, 520 U.S. 305, 323 (1997). Public safety is defined as instances where the risk is both substantial and real. *Id.*

Airport searches operate within the ambit of the Fourth Amendment when a court finds a favorable balance between "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[110] In *United States v. Hartwell*, the United States Court of Appeals for the Third Circuit upheld the validity of an airport search after Mr. Hartwell tripped a magnetometer at a security checkpoint and subsequently underwent a secondary search with a wand-style magnetometer.[111] The court reasoned that airport checkpoint searches passed the balancing test because (1) the government interest in "preventing terrorist attacks on airplanes is of paramount importance," (2) searches provide the only effective means of detecting potential hijackers, and (3) the search methods used were only minimally intrusive—they were tailored to protect personal privacy.[112]

The reasoning expressed by the *Hartwell* court, which focused on public safety, deterrence, and degree of invasiveness, permeates jurisprudence upholding the validity of airport administrative searches. The notion of implied consent presents another rationale upon which courts frequently rely.[113] Because of the self-evident nature of the public safety and deterrence rationales, this Comment will not examine them further. Instead, this Comment will closely assess the import of implied consent and degree of invasiveness.

1. Implied Consent

Passengers seeking to board a plane in the United States have grown accustomed to the heighted level of security pervading domestic airports. Accordingly, courts have reasoned that purchasing a ticket and attempting to board a plane demonstrates implied consent to undergo the screening process.[114] The necessary corollary to the notion of implied consent is that a passenger may choose to not travel by airplane. However, this option is limited at best. Unlike the era of travel prior to the early 1970s, where air travel represented an accoutrement of the wealthy few, air travel is now commonplace.[115] By 1970 the annual total

110. Illinois v. Lidster, 540 U.S. 419, 427 (2004) (internal quotation marks omitted).

111. United States v. Hartwell, 436 F.3d 174, 175 (3d Cir. 2006).

112. *Id.* at 179-81.

113. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 630 (3d ed. 1996).

114. *See, e.g.*, United States v. Aukai, 440 F.3d 1168, 1172-73 (9th Cir. 2006).

115. *See* Adam Thierer, *20th Anniversary of Airline Deregulation: Cause for Celebration, Not Re-Regulation*, HERITAGE FOUND., Apr. 22, 1998, http://www.heritage.org/research/regulation/bg1173.cfm.

volume of passengers approached nearly 200 million people.[116] Comparatively, for an eleven-month period in 2009, the total volume of passengers traveling domestically approached 569 million people.[117] Viewed in this light, commercial airliners serve as the equivalent of public buses carrying people to and from their respective destinations. Passengers must pay the requisite fare, including submitting to a search, in order to travel to a desired destination. Further highlighting the importance of air travel to modern society, travelers with time constraints lack a viable option because air travel generally presents the most expeditious means of transportation available. Within this context, the common air travelers' "willing" or voluntary submission to undergo a search fails to denote more than forced acceptance. In order to travel by air from or within the United States, a passenger must undergo a search. Thus the imposition or forced acceptance of searches necessarily should not mandate a lower expectation of privacy. Instead, the reduced expectation of privacy forced upon air travelers must be governed by the reasonableness manifested by the degree of invasiveness test.

2. Degree of Invasiveness

As stated *supra*, the core of the balancing test hinges on weighing the government need against the invasiveness of the government act. Regarding airport searches of a person, preserving public safety against terrorist acts clearly warrants government actors taking action to minimize the potentiality for harm. Such searches typically take place in two forms: magnetometer and pat down. Where the search process entails merely walking through a magnetometer, undergoing a hand-held magnetometer scan or pat down, courts generally find the search minimally invasive.[118] Indeed, use of magnetometers, both walk-through and hand-held, requires little or no physical interaction between government agents and prospective passengers. However, because pat downs require the invasion of passengers' personal space and face-to-face touching of each passengers' body by a stranger, they can thus lead to discomfort. Unlike pat downs, AIT scanners require no physical contact between passengers and security agents. Instead, employing AIT

116. *Id.*

117. RESEARCH & INNOVATIVE TECH. ADMIN., BUREAU OF TRANSP. STATISTICS, PASSENGERS: ALL CARRIERS—ALL AIRPORTS, http://www.transtats.bts.gov/Data_Elements.aspx?Data=1 (last visited Aug. 6, 2010).

118. *See* United States v. Marquez, 410 F.3d 612, 616-17 (9th Cir. 2005). *But see* United States v. Albarado, 495 F.2d 799, 802-09 (2d Cir. 1974) (finding that frisking a passenger after he activated a magnetometer without first asking him to remove metal objects violated the Fourth Amendment because it was not minimally invasive).

allows a stranger to view the intimate, naked details of the passenger's body. Thus, with AIT, travelers trade an invasion of personal space for a right to view their naked body.

Data gathered during AIT pilot programs at select airports indicates passenger acquiescence. According to the TSA, "Many passengers prefer advanced imaging technology. . . . [O]ver 98 percent of passengers who encounter[ed AIT] prefer it over other screening options [such as pat downs]."[119] "Additionally, [the pilot program indicated that] passengers with joint replacements or other medical devices that would regularly alarm a metal detector often prefer this technology because it is quicker and less-invasive than a pat down."[120] Furthermore, of 1756 total passengers scanned at John F. Kennedy International Airport and Los Angeles International Airport, only fifty-one elected to not undergo an AIT scan.[121] This data readily indicates, inter alia, that passengers prefer to not have their personal space infiltrated by TSA agents and would rather undergo a less physically invasive procedure that captures discernible images of their body while concomitantly saving time by eliminating the need to remove articles of clothing or stand in a queue.

B. European Union

Each Member State possesses express authority to conduct airport searches in order to ensure aviation security.[122] The designated method must comport with the Charter of Fundamental Rights of the European Union (Charter), which guarantees a right to human dignity (article 1), a right to the integrity of the person (article 3), and a right to protection of personal data (article 8).[123] While the traditional search methods,

---

119. *Imaging Technology*, *supra* note 70.

120. *Id.*

121. *Safety & Privacy Concerns Regarding the Millimeter Wave Whole Body Imagers*, *supra* note 41.

122. Commission Regulation 300/2008, *supra* note 44, at 72-74.

123. Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1, 9-10, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf [hereinafter Charter of Fundamental Rights]. The Charter became effective on December 1, 2009. *Id.*; Treaty of Lisbon, Dec. 13, 2007, 2007 O.J. (C 306) 1 (amending the Treaty on European Union and the Treaty Establishing the European Community, the Treaty of Lisbon incorporates the Charter of Fundamental Rights of the European Union as primary law). Article 1, on human dignity, provides, "Human dignity is inviolable. It must be respected and protected." Charter of Fundamental Rights, *supra*, art. 1. Article 3, on the right to the integrity of the person, provides:

> 1. Everyone has the right to respect for his or her physical and mental integrity.
> 2. In the fields of medicine and biology, the following must be respected in particular:
> - the free and informed consent of the person concerned, according to the procedures laid down by law,

magnetometer searches and pat downs of the person, remain the primary means of identifying passengers toting contraband, any new methodology adopted must not infringe upon fundamental rights.[124] New search methodologies must also comport with additional safeguards such as the 1995 Directive on Data Protection.[125] The Directive is the primary source of EU privacy regulations not articulated in the Charter.[126] It provides directives on the flow of private data used by government and corporate institutions.[127] However, article 13 of the Directive stipulates exemptions from adhering to the directives when necessary to protect national security, public security, or regulatory functions.[128] Airport searches fit neatly within each of these exceptions. New search methods must also overcome scrutiny from the article 29 Data Protection Working Party, an independent advisory board that makes recommendations on privacy issues and provides advisory opinions on matters of data protection.[129]

- the prohibition of eugenic practices, in particular those aiming at the selection of persons,
- the prohibition on making the human body and its parts as such a source of financial gain,
- the prohibition of the reproductive cloning of human beings.

Id. art. 3. Article 8, on the protection of personal data, provides the foundry for European privacy law. It allows:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Id. art. 8.

124. *Id.* art. 54. While the rights guaranteed by the Charter may be limited, any limitation must still respect those rights and freedoms. Such limitations may only be made if they are necessary to protect the rights and freedoms of others or if a limitation is necessary and genuinely accomplishes an objective within a recognized general interest of the EU. *Id.* art. 52.

125. *See* Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Privacy Directive], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

126. *See* Bob Sullivan, *Privacy Lost: EU, U.S. Laws Differ Greatly*, MSNBC.COM, Oct. 19, 2006, http://www.msnbc.msn.com/id/15221111/.

127. *Id.*

128. Privacy Directive, *supra* note 125, art. 13.

129. *Id.* arts. 29-30; *see also* Justice & Home Affairs, *Tasks of the Article 29 Data Protection Working Party*, EUROPEAN COMM'N, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf (last visited Aug. 6, 2010).

In the EU, there exists unquestioned authority to conduct airport searches. However, the introduction of body scanners presents unresolved questions about the scope of permissible searches. Indeed, changes in technology, such as the emergence of social networking on the Internet, coupled with the drive to use AIT scans in airports prompted the new EU Fundamental Rights Commissioner, Viviane Reding, to urge modernizing privacy and data protection laws.[130] These regulations have not undergone substantive revisions since their introduction in 1995.[131] Accordingly, the legal ambiguity as to whether using body scanners to effect airport searches expressly violates the fundamental right of privacy in the context of preserving public safety and national security, despite the exceptions included in the Charter, will likely be clarified. Consequently, unless a case manifests that prompts the European Court of Justice to intervene, Member States will continue a piecemeal body scanner implementation strategy that is subject to public opinion.

V. IMPACT OF AIT SCANNERS: VULNERABILITIES, CHALLENGES, AND FUTURE IMPLICATIONS

A. Vulnerabilities

Despite their speed and ability to capture detailed images of a person's body, these scanners are subject to at least four vulnerabilities. First, AIT scanners lack the ability to detect items hidden in body cavities.[132] As one commentator observed,

> All males have a body cavity. Females have two body cavities. In prisons, these body cavities are habitually used to smuggle drugs and improvised weapons past body searches, including complete nudity strip searches.

---

130. Press Release, European Union, Europeans' Privacy Will Be Big Challenge in Next Decade, Says EU Commissioner (Jan. 28, 2010), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/63&type=HTML. Ms. Reding is adamantly opposed to intrusions upon fundamental rights, such as privacy, even on the basis of antiterrorism and preserving national security. When asked about her position on body scanners, she remarked that "our need for security cannot justify any violation of privacy." Hunton & Williams LLP, *New EU Fundamental Rights Commissioner Reveals Privacy and Data Protection Priorities in the European Union*, PRIVACY & INFO. SEC. L. BLOG (Jan. 14, 2010, 2:46 PM), http://www.huntonprivacyblog.com/2010/01/articles/european-union-1/new-eu-fundamental-rights-commissioner-reveals-privacy-and-data-protection-priorities-in-the-european-union/. Ms. Reding also indicated an intention not to allow anyone to impose "rules that go against fundamental rights on anti-terrorism grounds." *Id.*; *see also* Anna Jenkinson, *Reding Stresses Charter of Fundamental Rights for New Post*, EUROPOLITICS, Jan. 12, 2010, http://www.europolitics.info/sectorial-policies/reding-stresses-charter-of-fundamental-rights-for-new-post-art259763-16.html.

131. Press Release, Europa, *supra* note 130.

132. Schwartz, *supra* note 39.

> Given the power of widely available explosives, the amount that can be carried inside a body cavity—let alone two—is sufficient to destroy ordinary pressurized airliners at normal flight altitudes. That makes "pat downs," or indeed any form of physical inspection that is remotely feasible in any airport of any normal country, entirely futile. That alone rules out scanners as a solution unless they are both very-high definition and pat downs are not allowed as an alternative.[133]

Second, these machines are incapable of discovering contraband concealed in the folds of an obese person's flesh.[134] Third, the scanners lack the ability to uncover potentially explosive powders not carried in containers.[135] Fourth, the scanners fail to identify passengers who smuggle surgically implanted bombs within their abdomen or buttocks.[136] As this short list illustrates, the current generation of AIT yields de minimis protection to public safety. Consequently, airlines remain susceptible to terrorist attacks.

B. Challenges

Despite the policies and procedures in place to protect against image transmission, namely immediate image deletion, banning photographic equipment in the remote room, and blurring the passenger's face, some images will undoubtedly be captured for private use and possibly be circulated. The ubiquitous nature of cellular telephones and other devices with photographic capabilities provides for the near certainty of a security breach. Recent estimates indicate that seventy-five percent of mobile telephones worldwide are manufactured with a camera module.[137] Thus, avoiding such a breach requires an absolute ban on

---

133. Edward N. Luttwak, *The Body Scanner Scam*, WALL ST. J., Jan. 19, 2010, at A25.

134. Schwartz, *supra* note 39.

135. Matthew L. Wald, *Documents Send Mixed Signals on Airport Scanners*, N.Y. TIMES, Jan. 13, 2010, at A21.

136. Peter Walker, *Invasion of the Body Scanners*, GUARDIAN, Jan. 3, 2010, http://www.guardian.co.uk/uk/2010/jan/03/invasion-of-the-body-scanners. Tests conducted in 2009 indicate that smuggling bomb components within the body was both feasible and untraceable by either millimeter wave or backscatter scans. *Id.*; *see also*, Christopher Leake, *Terrorists 'Plan Attack on Britain with Bombs INSIDE Their Bodies' to Foil New Airport Scanners*, DAILY MAIL, Jan. 30, 2010, http://www.dailymail.co.uk/news/article-1247338/Terrorists-plan-attack-Britain-bombs-INSIDE-bodies-foil-new-airport-scanners.html. One Al-Qaeda operative hid a bomb inside his body and used a cell phone signal to initiate its detonation. Leonard Doyle, *New Al-Qaeda 'Body Bombs' that Can Beat Airport Security are Alarming Terror Experts*, TELEGRAPH, Oct. 3, 2009, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/6258137/New-al-Qaeda-body-bombs-that-can-beat-airport-security-are-alarming-terror-experts.html.

137. *See generally* MKT. INTELLIGENCE & CONSULTING INST., THE WORLDWIDE MOBILE PHONE CAMERA MODULE MARKET AND TAIWAN'S INDUSTRY, 2009 AND BEYOND (2009), http://www.marketresearch.com/map/prod/2403287.html.

operators having mobile telephones and similarly situated devices in the remote room. As illustrated by U.S. officials smuggling IEDs through various airport security checkpoints, discussed *supra*, security agents and the security procedures implemented thus far are far from infallible. As a result, people with unique body types bear the risk of having their image ogled over, mocked, laughed at, and circulated.[138]

Furthermore, images withheld from the public frequently manifest publicly. For example, in one highly publicized instance, pursuant to standard operating procedure, two members of the California Highway Patrol photographed the gruesome decapitation of a debutante; her body was in such a mangled state that the coroner did not allow her parents to identify the body.[139] In direct contravention of protocol, the troopers sent copies of the pictures to themselves, departmental coworkers and to external contacts. Consequently, the parents discovered the pictures online.[140] Like the patrolmen who abused their administrative authority for entertainment or shock value, there exists the ready possibility that images obtained by AIT readers could circulate the Internet. Thus, despite a written policy against image capturing and dissemination, the difficulty lies in policy enforcement and discouraging agents' abuse of discretion.

Although not a direct limitation on the scanners themselves, use of AIT presents a distinct challenge to some theological beliefs, including Judaism and Islam. Conservative and Orthodox Jewish communities have expressed concerns that the scanners violate *tzniut*, a modesty requirement that generally calls for men and women to cover their

---

138. Illustrative, a TSA screener was arrested after attacking a co-worker who taunted him over the size of his genitalia. *For Airport Security, Size Matters: New High-Tech Screener Triggered Fight Over Manhood Insult*, SMOKING GUN, May 6, 2010, http://www.thesmokinggun.com/documents/stupid/airport-security-size-matters. Subsequent to undergoing an AIT scan, the tauntee claimed that co-workers would daily call him names like "little angry man" or ask "what size are you?"; the taunting often occurred in front of passengers. He described the teasing as "psychological torture." *TSA Screener Cited "Torture" In Scanner Case: Arrestee's Genitalia Was Exposed By "Full Body" Device*, SMOKING GUN, Sept. 14, 2010, http://www.thesmokinggun.com/documents/bizarre/tsa-screener-cited-torture-scanner-case. Likewise, a male security worker in London's Heathrow Airport received a warning from police and professional discipline after making inappropriate comments to a female colleague who inadvertently entered an AIT scanner. Michael Holden, *UK Airport Worker Warned in Scanner Ogling Claim*, REUTERS, Mar. 24, 2010, http://www.reuters.com/article/idUSTRE62N1T020100324. The woman claimed she was "traumatized" by the incident, which, coincidentally, was made public on the same day that lawmakers dismissed concerns that AIT scanners are invasive. *Id.* Capturing the full scope of these concerns, the head of a watch-dog group remarked, "For every official caught ogling like this, there are plenty more eyeing up law-abiding travelers." *Id.*

139. Jessica Bennett, *A Tragedy That Won't Fade Away*, NEWSWEEK, Apr. 25, 2009, http://www.newsweek.com/2009/04/24/a-tragedy-that-won-t-fade-away-print.html.

140. *Id.*

bodies.[141] Likewise, AIT imposes upon Islamic modesty laws, *haya*.[142] Similar to the *tzniut*, *haya* provides that only family members can see the naked body unless there exists an extreme necessity such as medical treatment, investigating a crime, or imminent danger.[143] Accordingly, the Fiqh Council of North America (FCNA), a body of certified Islamic scholars living in the United States and Canada, issued a fatwa, a religious decree on matters of Islamic law, against the scanners and began urging all Muslims to opt for pat downs.[144] Recognizing the importance of air safety, the FCNA proposes using other technologies that preserve the modesty of the human form yet still detect contraband.[145] Although not currently employed by any airport security administrator, thermal sensory imaging provides one such alternative.

C. Future Implications

The prevailing scanning methods used in AIT signal a forced change in the conceptualization of privacy. While some may argue that passengers forsake their right to privacy because they have notice that the search will occur, thus impliedly consenting to the scans, as discussed *supra*, passengers lack a comparable alternative to flying in airplanes. In short, the lack of comparable available alternatives leaves the passenger no choice. Consequently, governments, by imposing AIT upon passengers, effectively communicate that people no longer possess a reasonable expectation of privacy in the sanctity of their bodies.

Declassified TSA documents support the argument that the government seeks to alter passenger expectations of privacy. TSA bid specifications expressly sought the ability to inspect the area underneath passengers' clothes for contraband.[146] Despite potential privacy concerns, exploring alternatives to viewing a naked image of each passenger does

---

141. Josh Nathan-Kazis, *How Modern Airport Security May Run Afoul of Jewish Law*, JEWISH DAILY FORWARD, Jan. 22, 2010, http://www.forward.com/articles/123364/.

142. *Muslim-American Body Issues Fatwa Against Airport Body Scanners*, TIMES OF INDIA, Feb. 12, 2010, http://timesofindia.indiatimes.com/world/us/Muslim-American-body-issues-fatwa-against-airport-body-scanners/articleshow/5564134.cms. Specifically, the Qur'an encourages men and women to "guard their private parts" and implores women not to display their bodies except to family members or slaves. *Holy Qur'an* 24:30-31.

143. *Muslim-American Body Issue Fatwa Against Airport Body Scanners*, *supra* note 142; *see also Statement of the FCNA on the Use of Full Body Scanners for Security at the Airports and Other Places*, FIGH COUNCIL OF N. AM., Feb. 9, 2010, http://www.fiqhcouncil.org/ [hereinafter *Figh Council Statement*] .

144. *Figh Council Statement*, *supra* note 143.

145. *Id.*

146. TRANSP. SEC. ADMIN., *supra* note 8, at 1.

not appear to have been a priority.[147] Conjunctively considering these ministerial decisions with the intimate details revealed by AIT scans, the use of AIT establishes the foundation for the application of more invasive techniques or technologies in the future—barring a successful legal challenge. These facts are substantially similar to the United States' experience with DNA.

Initially, in 1990, the FBI collected DNA for the express limited purpose of cataloguing sex offenders' genetic material.[148] In less than ten years after DNA collection began, a national DNA database emerged with over four million DNA samples belonging to unidentified persons, missing persons, and arrested offenders.[149] While the practical uses of a national DNA database[150] far outnumber the uses of naked images derived from AIT scans, there remains a distinct possibility, however remote, that images can be retained and stored in a national database. A recent discovery that the U.S. Marshall Service intentionally stored over 35,000 AIT scans of people who entered a federal courthouse in Orlando, Florida underscores the viability of this course of action.[151] Absent laws to the contrary, a future administration could determine, for example, that preserving security and public safety warrants it tracking changes in passenger scans between destinations. Alternately, a national flyer registry could develop where AIT scans are pinned to each individual passenger via an identification number. While predicting the future is impossible, government needs can and will change over time.

---

147. Jeremy Pelofsky, *U.S. Air Travelers Complain About Body Scans*, REUTERS, Mar. 16, 2010, http://www.reuters.com/article/idUSTRE62F4W020100317.

148. Kathryn Vercillo, *History and Purpose of the National DNA Database*, HUBPAGES, http://hubpages.com/hub/History-and-Purpose-of-the-National-DNA-Database (last visited Mar. 3, 2010).

149. *Id.*

150. *See CODIS Combined DNA Index System*, FED. BUREAU OF INVESTIGATION (FBI), http://www.fbi.gov/hq/lab/html/codisbrochure_text.htm (last visited Aug. 6, 2010).

> CODIS generates investigative leads in cases where biological evidence is recovered from the crime scene. Matches made among profiles in the Forensic Index can link crime scenes together; possibly identifying serial offenders. Based upon a match, police from multiple jurisdictions can coordinate their respective investigations and share the leads they developed independently. Matches made between the Forensic and Offender Indexes provide investigators with the identity of a suspect perpetrator(s). Since names and other personally identifiable information are not stored at NDIS, qualified DNA analysts in the laboratories sharing matching profiles contact each other to confirm the candidate match.

Id.

151. Mike M. Ahlers, *Agency Stored Body Images From Florida Courthouse*, CNN.COM, Aug. 4, 2010, http://articles.cnn.com/2010-08-04/US/marshalls.body.images_1_images-orlando-Courthouse-privacy-rights-group?_s=PM:US.

Accordingly, some rules must be enacted to prevent future devaluation of privacy rights.

VI. CONCLUSION

As AIT illustrates, technological advancements impinge upon conventional definitions of privacy. Consequently, the scope of the legal use of such instruments requires interpretation. In the EU, where the Charter grants express rights of privacy, modesty, and human decency, the outer limits of legality are clearly drawn by a reluctance to impose AIT upon the people and by mandating optional means of searching. Instead, the EU manifested a willingness to honor these rights by first considering alternatives to backscatter and MMW technology, allowing for further examination of AIT and by not infringing upon the decisions of Member States to use the available technology. Distinct from the EU, the United States possesses no express constitutional right to privacy. Unlike the EU, where the potential infringement upon guaranteed rights prompted the termination of a proposed system of uniform AIT scanning, no such restraint has been exhibited in the United States due to the ever-present fear of terrorist attack.[152] In order to properly guard privacy interests, the United States, EU, and its corresponding Member States should adopt the following considerations: (1) supplement the balancing test to consider whether an alternate means would accomplish the precise need articulated by the government interest, (2) establish a bright line rule concerning the extent to which privacy interests can be compromised by government activities, (3) strictly monitor the activities of remote room readers, and (4) jointly develop a comprehensive scanning technology that more effectively minimizes security vulnerabilities.

A. Supplement the Balancing Test To Consider Whether an Alternate Means Would Accomplish the Precise Need Articulated by the Government Interest

Traditionally strong arguments for the constitutionality of airport administrative searches are that searches using magnetometers or frisks of outside clothing are minimally invasive, passengers have notice of the impending search, and that passengers offer implied consent to undergo

152. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-401T, BETTER USE OF TERRORIST WATCHLIST INFORMATION AND IMPROVEMENTS IN DEPLOYMENT OF PASSENGER SCREENING CHECKPOINT TECHNOLOGIES COULD FURTHER STRENGTHEN SECURITY 17 (2010), *available at* http://www.gao.gov/new.items/d10401t.pdf.

searches. For these reasons, U.S. courts deem the balancing test satisfied and the degree of invasion minimal. However, technological advancement necessitates supplementing the balancing test to also evaluate whether alternate means are available to accomplish the need articulated by the government interest.

Applying this modified test to prevailing AIT passenger-scanning technology, usage of such devices is unreasonable because they violate privacy and the modesty protected by privacy interests. While the intelligence obtained from backscatter and MMW scanners may divulge evidence that suggests a pending attack, thermal imaging provides equivalent protection without the invasion of modesty or privacy. Accordingly, a reasonable alternative to backscatter and millimeter wave technology exists. Further, an evaluation of the reasonableness of AIT searches must consider passengers' forced acceptance of security procedures and the reduced expectation of privacy that inures. Passengers' deference to government authority and fear for their lives must not be held against them. A Government Accountability Office (GAO) report augments the finding that AIT is unreasonable. In the report, the GAO announced finding ambiguity as to whether AIT would have detected Abdulmutallab's underwear bomb.[153] The GAO based its assessment on the failure of TSA to evaluate the technology's vulnerabilities,[154] the intent to install 878 scanners by 2014,[155] the approximate cost of the scanners is between $130,000 and $170,000,[156] and the TSA's history of not evaluating security technologies before deploying them into live operation.[157]

---

153. *Id.* at 20.

154. *Id.* at 18-21.

155. *Id.* at 17.

156. *Id.* This cost does not include installation fees or the $50,000 per unit required to train TSA agents on using the machines. *Id.*

157. *Id.* at 19-20. The GAO specifically referred to the failed "Puffer" devices, or Electronic Trace Portals (ETP), which were supposed to dislodge particles from the person's body using gusts of air and then test the particles for indications of explosives. *Id.* at 19. Purchased for nearly $30 million, these machines frequently broke down due to dust, dirt, and grease accumulations and necessitated over $6 million in repairs. Thomas Frank, *Last Gasp for Anti-Bomb 'Puffers'; $36 Million Airport Program Scrapped*, USA TODAY, May 21, 2009, at 1A. Removing them will cost an additional $1 million. *Id.* When referring to the failed TSA effort, the GAO remarked:

> Deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. . . . [The] TSA's experience with the ETPs . . . demonstrates the importance of testing and evaluation in an operational environment. . . . TSA procured 207 ETPs and in 2006 deployed 101 ETPs to 36 airports, the first deployment of a checkpoint technology initiated by the agency. TSA deployed the ETPs even though agency officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not

B. Establish a Bright Line Rule Concerning the Extent to Which Privacy Interests Can Be Compromised by Government Activities

The effort to use AIT raises an important question: when public safety is a risk, how far will the courts allow the government to go in order to prevent terrorism? As one commentator observed:

> Yes, the machines show the shape of your body under your clothes. Big deal. That strikes me as way less intrusive than pat-downs, wands, bomb-sniffing dogs, hand inspections, and no-fly lists. If we put up with that stuff, why on earth would we suddenly draw the line at a full body scanner?[158]

Where do we draw the line? In answering this question, a necessary consideration must be that terrorists consistently demonstrate an acute adaptive ability to frustrate security procedures by exploiting existing vulnerabilities.[159] The use of AIT will likely prompt attackers to use bombs that can be inserted into body cavities, at which point aviation security personnel will respond by seeking to employ comprehensive technology that scours the individual from the outside in, seeking contraband. One such technology, the chair-like Bodily Orifice Security Scanner (BOSS), already exists and is currently used by prisons in the

---

> demonstrate reliable performance. Furthermore, the ETP models that were subsequently deployed were not first tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA procured and deployed ETPs without assurance that they would perform as intended in an operational environment. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. In June 2006, TSA halted further deployment of the ETP because of performance, maintenance, and installation issues. According to a senior TSA official, as of December 31, 2009, all but 9 ETPs have been withdrawn from airports and 18 ETPs remain in inventory. . . . In the future, using validated technologies would enhance TSA's efforts to improve *Last Gasp for Anti-Bomb 'puffers'; $36 Million Airport Program Scrapped* point security. Furthermore, retaining existing screening procedures until the effectiveness of future technologies has been validated could provide assurances that use of checkpoint technologies improves aviation security.

U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 152, at 19-20 (internal citations omitted).

158. Kevin Drum, *Full Body Scanning*, MOTHERJONES, Dec. 30, 2009, http://motherjones.com/kevin-drum/2009/12/full-body-scanning.

159. *See* Sheila MacVicar, *Al Qaeda Bombers Learn from Drug Smugglers*, CBS NEWS, Sept. 28, 2009, http://www.cbsnews.com/stories/2009/09/28/eveningnews/main5347847.shtml. An Al Qaeda operative smuggled a bomb past Saudi Arabian airport security and guards by hiding it in his rectum. *Id.*

United Kingdom to prevent smuggling and distribution of cellular telephones into their facilities.[160]

C. Strictly Monitor Remote Room Readers

To prevent remote room readers from preserving AIT scans and abusing their authority, measures must be installed to ensure that agents abide by the prescribed policies. One possible tactic includes subjecting remote readers to AIT scans. While this option seems like the quickest and most efficient means of enforcing cooperation, in light of the vulnerabilities identified *supra*, this test must be augmented by a security pat down or some other sweep to verify compliance.

D. Jointly Develop a Comprehensive Scanning Technology that More Effectively Minimizes Security Vulnerabilities and Preserves Privacy

The short list of vulnerabilities identified *supra* militates against investing $150,000 to purchase only one scanner. Accordingly, the United States and EU should pool their resources together to develop a comprehensive technology that considers each of the identified vulnerabilities and guards against them while concomitantly preserving privacy. As aviation security expert Bruce Schneier observed, aviation security methods typically lack foresight because they guard against only one type of threat.[161] To better protect their citizens, security administrators from the EU and the United States must collaborate. By sharing ideas and financial resources these hegemons are better equipped to develop the technology required to detect multiple potential forms of attack, such as bombs hidden in body cavities, without impinging upon passenger health. Until then, a piecemeal approach will continue to leave airports and passengers exposed to the risk of injury or death.

The Fourth Amendment of the United States Constitution protects the right to be secure in the person. Likewise, the EU Charter expressly guarantees rights to privacy and modesty. Arguably, AIT infringes upon these rights. Although reasonable minds may differ, one can easily understand why someone would find it unreasonable to use backscatter or MMW technology that depicts naked images of men, women, and

---

160. Dominic Casciani, *Care To Sit on the Boss Chair?*, BBC NEWS, Dec. 20, 2007, http://news.bbc.co.uk/2/hi/uk_news/magazine/7152744.stm. The Boss Chair functions as a metal detector scanning the rectum for ferrous metals. *Id.*

161. *See* Ravitz, *supra* note 62; *see also* Marnie Hunter, *Body Scanners Not 'Magic Technology' Against Terror*, CNN.COM, Dec. 30, 2009, http://www.cnn.com/2009/TRAVEL/12/30/airport.security.screening/index.html.

children. This understanding becomes readily apparent when considering that other forms of available technology accomplish the same precise objective. Perhaps this conclusion would be different if passengers voluntarily decided to walk through the airports completely naked. However, the fact that passengers are clothed suggests that they retain a reasonable expectation in the privacy of their naked bodies. Accordingly, the use of AIT violates expressly guaranteed rights in the EU and protected rights in the United States. Thus, the imposition of AIT absent some restraint upon government decision makers denotes that, truly, as one commentator remarked, "we are moving toward a world of significantly less information privacy."[162]

162. Edward Harrison, *Terrorism, Full-Body Scans and Privacy in the Digital Age*, CREDIT WRITEDOWNS, Jan. 11, 2010, http://www.creditwritedowns.com/2010/01/terrorism-full-body-scans-and-privacy-in-the-digital-age.html.