The handle http://hdl.handle.net/1887/20288 holds various files of this Leiden University dissertation.

Author: Klitou, Demetrius
Title: Privacy-invading technologies: safeguarding privacy, liberty & security in the 21st century
Date: 2012-12-14
5 | BODY SCANNERS: A strip search by other means*

5.1 CHAPTER INTRODUCTION

Since the tragic events of 9/11, the Transportation Security Administration (TSA) has critically served to enhance the ability of airport security screening to detect and/or discover potential threats to aviation security. The deployment of new technology has been central to this enhancement. Body scanners have only recently been deployed at airports across the US as an alternative to patdowns. There are also now calls for their use to eventually replace walk-through metal detectors. Body scanners, however, are highly intrusive upon the privacy of one’s body and may violate the Fourth Amendment of the US Constitution, if not proportionally and appropriately used.

Section 5.2 explains the privacy intrusiveness of (backscatter) body scanners, a type of body scanner, comparing them to a strip search. Section 5.3 explains how backscatter body scanners work. Section 5.4 points out their security benefits and drawbacks. Section 5.5 discusses the plausibility of the threat posed by plastic guns, ceramic knives, and liquid/chemical and plastic explosives, which backscatter body scanners are promoted for aiding in their detection or discovery. Section 5.6 describes the possible alternatives to backscatter body scanners in airport security screening.\(^\text{161}\) Section 5.7 describes the scope of deployment of body scanners in the US. Section 5.8 outlines the statutory law and case law of special relevance in the US. Section 5.9 evaluates and highlights the deficiencies and dilemmas of the US legal framework in terms of protecting privacy, fulfilling the principles of privacy and upholding the integrity of the Fourth Amendment with regards to the use of body scanners. Section 5.10 outlines some proposals on how to enhance the US legal framework. Section 5.11 briefly explains whether the focus should be on regulating the use or regulating the manufacture

* Chapter 5, despite subsequent additions and modifications, served as the basis for the article I published previously, titled: Backscatter body scanner - A strip search by other means (Computer Law & Security Report, Volume 24, Issue 4, Elsevier, July 2008), pp. 316-325.

\(^{161}\) This chapter will only discuss the security screening of passengers themselves and not their luggage or carry-on bags.
of body scanners. Section 5.12 outlines the international deployment of body scanners. Section 5.13 ends the chapter with some ending remarks.

5.2 A STRIP SEARCH BY OTHER MEANS?

Backscatter body scanners, manufactured by American Science and Engineering, Inc. (AS&E) and Rapiscan (a unit of OSI Systems, Inc.), enable the operator of the device to see just beneath the clothing of an individual, clearly revealing that individual’s naked body, including the shape and size of genitals, buttocks and female breasts. As Bill Scannell, a privacy advocate/technology consultant, asserts, “It shows nipples. It shows the clear outline of genitals”. Backscatter body scanners can also potentially reveal sensitive medical details about a person, such as mastectomies and colostomy appliances. The graphic anatomical detail of the images produced by backscatter body scanners has led Barry Steinhardt of the American Civil Liberties Union (ACLU) to persistently call their use a “virtual strip search”.

As virtual money is used to make payments by other means - electronic means, a virtual strip search is used to inspect one’s body by electronic means. But, could a virtual strip search be considered the same as a conventional strip search? Well, society and law enforcement bodies consider virtual money to be just another form of money. Interpol defines virtual money as “an encrypted code representing money, in the same way that paper money is only paper bearing certain characteristics such as graphics and serial numbers”. The only main difference is that virtual money is seen on a computer screen. Perhaps, just like virtual/electronic money is increasingly being used in place of conventional paper money and could one day become the dominant medium of exchange, unit of account or store of value in the digital age, virtual strip searches can also substitute conventional strip searches. As William Saletan asserts, “they [backscatter body scanners] don’t extend the practice of strip-searching. They abolish it”.

Essentially, the only significant difference between the use of backscatter body scanners, without the employment of a privacy algorithm, and the conduct of a conventional strip search is that an individual’s naked body is seen not in person, but via a computer screen and without the need to remove a single item of clothing. “Stripping is just a means. Virtual inspections [backscatter body scanners] achieve the same end by other means” (emphasis added).

Nonetheless, backscatter body scanners are at present being used as an alternative to patdowns, without the guarantee of the employment of a privacy algorithm. Advocates of backscatter body scanners assert that their use, as an alternative to patdowns, actually enhances the privacy of passengers, since patdowns require physical contact. But, the use of a backscatter body scanner, without the employment of a privacy algorithm, is comparable to conducting a strip search, and thus is considerably more intrusive than an appropriately conducted patdown. Although, according to the TSA, during the trial phase at Sky Harbor International Airport, 70% of passengers opted to be subjected to a backscatter body scanner instead of a patdown, it is unclear whether or not they were fully aware of the intrusive capability of backscatter body scanners or, for instance, if they were shown a true sample of the images generated. Moreover, it was not revealed what percentage of the passengers who opted to be scanned was male or female and it is also unknown how the passengers were surveyed.

In recognition of the intrusive capability of backscatter body scanners and to demonstrate their disapproval of the proposal to deploy them at US airports, Privacy International awarded the Federal Aviation Administration (FAA) the ‘Orwell Award’ for

\[167\] Ibid.


\[169\] On the other hand, this result was recently confirmed by a more appropriately conducted poll by Gallup. In the midst of the so-called Christmas day attack, 78% of US air travelers surveyed approved of the use of body scanners at US airports. see “In U.S., Air Travelers Take Body Scans in Stride”, 11 January 2010, available at: http://www.gallup.com/poll/125018/air-travelers-body-scans-stride.aspx

And even more recently, a survey study conducted by the IT firm Unisys in April 2010, as part of the Unisys Security Index, found that nearly 65% of Americans are willing to undergo full body scans for greater aviation security. see Unisys Press Release available at: http://www.unisys.com/unisys/news/detail.jsp?id=112000970001910179

But, these results still leave an average of 30% of Americans unwilling to undergo full body scans, which should not be discounted. Moreover, the willingness of US travelers will likely continue to drop as time elapses further away from the so-called Christmas day attack.
the “Most Invasive Proposal”. The Electronic Privacy Information Center (EPIC) has equally recognized that body scanners pose a serious threat to privacy and has called for the suspension of the use of body scanners at airports until appropriate laws and regulations are put into place.

5.3 HOW BACKSCATTER BODY SCANNERS WORK

Objects with a high atomic number (high Z materials), such as metallic weapons, absorb X-rays, while explosives, containing, for example, nitrogen and carbon, which have a low atomic number (low Z materials), scatter X-rays. The intensity of X-ray backscatter decreases as the atomic number (Z) increases. Human tissue is predominately composed of oxygen, which has a relatively low atomic number. The technology of backscatter body scanners works by projecting low-radiation X-rays onto an individual while standing in a portal. The X-rays that reflect off the individual or backscatter are detected by the scanner, identified where they came from and converted into a photographic-quality image displayed on a monitor, revealing any concealed objects of low Z material. Backscatter body scanners also recognize the lack of scattering and therefore can reveal any concealed object of high Z material. Concealed objects, both metallic and non-metallic, are distinguishable in backscatter images due to their significant differences in atomic number from human tissue. The image edges of concealed objects of low Z material are ideally enhanced to facilitate their detection.

---


171 Further information is available at: http://epic.org/privacy/airtravel/backscatter/


5.4 SECURITY BENEFITS AND DRAWBACKS OF BACKSCATTER BODY SCANNERS

Evidently, there are systemic vulnerabilities in the security screening process at airports. This is true not just in the US, but internationally. The covert security audits, conducted by the TSA and the GAO, have especially revealed the vulnerabilities at US airports. GAO investigators managed to get through airport security checkpoints undetected with either improvised explosive devices (IEDs) or improvised incendiary devices (IIDs) hidden both in their carry-on luggage and on their persons.\textsuperscript{174} In 2007, it was publicly disclosed that TSA screeners on numerous occasions failed to detect simulated explosives and bomb parts hidden under the clothes of TSA covert security auditors.\textsuperscript{175} A few months later, it was reported that a loaded firearm slipped through airport security\textsuperscript{176} and a TSA screener, during a covert security audit, failed to detect a fake bomb even after conducting a patdown.\textsuperscript{177}

While the vulnerabilities are partly due to “human factors”,\textsuperscript{178} the main problem, in the first place, is the incapability of walk-through metal detectors (WTMDs) to detect plastic guns, ceramic knives, and liquid/chemical and plastic explosives. The other significant problem is with patdowns. The quality of patdowns may vary significantly, due to human factors, and patdowns cannot reveal relatively small amounts of chemical or plastic explosives hidden very close to a person’s genitals, such as within their underwear.


\textsuperscript{178} “Human factors” refers to the demands a job places on the capabilities of, and the constraints it imposes on, the people doing it. For screeners, the human factors issues cited in past studies include the repetitive tasks screeners perform, the close and constant monitoring required to spot the rare appearances of dangerous objects, and the stress involved in dealing with the public, who may dislike being screened or demand faster action to avoid missing their flights”. U.S. General Accounting Office, Aviation Security: Long-Standing Problems Impair Airport Screeners’ Performance, GAO/RCED-00-75 (Washington, D.C.: 28 June 2000), p. 26.
Body scanners: A strip search by other means

since patdowns conducted at airports in the US and in Europe do not normally involve the touching of these sensitive areas. While the deficiencies of WTMDs and patdowns were always clear to security experts, these deficiencies have been especially highlighted by the so-called “underwear bomb” containing PETN (pentaerythritol tetranitrate) that made it through Amsterdam’s Schiphol Airport undetected on December 25, 2009.

Indeed, backscatter body scanners can (potentially) significantly enhance the security screening process at airports and reduce the adverse effects of human factors by facilitating security screeners to detect or discover any object hidden on a person that metal detectors and sometimes a patdown cannot or do not.¹⁷⁹

Nevertheless, like any single security apparatus, device or system, (backscatter) body scanners are certainly not foolproof. Since the low-radiation X-rays emitted from backscatter body scanners only penetrate about 0.1 inches (0.254 centimeters) of the skin, they are unable, for instance, to reveal threats hidden deeper in body cavities. Terrorists determined to get pass security screening with a bomb, for example, can hide explosives and a detonator in their rectum, which was indeed the new strategy reportedly used by al Qaeda to target Saudi Prince Mohammed Bin Nayef inside a palace in August 2009.¹⁸⁰

There is also a risk from high-explosives surgically implanted within skin tissue, where they may potentially not be revealed by body scanners, for example under breast tissue.¹⁸¹

In addition, body scanners apparently may also have potential difficulties in detecting

¹⁷⁹ During the second meeting of the Task Force on Security Scanners in 2010, first set up by the European Commission, representatives present from Schiphol Airport, Manchester Airport and the UK Department of Transport, for instance, explained that after their trial phases of body scanners, they are convinced that the evidence proves that body scanners offer immense security benefits and enhancements (i.e. improved detection of both metallic and non-metallic threats on a person). The European Commission has equally recognized and acknowledged the security benefits of body scanners, which must be seriously taken into consideration. see the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports (COM(2010) 311 final), 15.6.2010.


¹⁸¹ Reportedly, terrorists are known to have implanted PETN in the breasts of women. see “Terrorists Could Use Explosives in Breast Implants to Crash Planes, Experts Warn” (The Sun, 24 March 2010), available at: http://www.foxnews.com/world/2010/03/24/terrorists-use-explosives-breast-implants-crash-planes-experts-warn/?test=latestnews
explosives hidden in shoes or items stitched into clothing.\textsuperscript{182} The security vulnerabilities of body scanners were additionally highlighted by the GAO in a 2009 report\textsuperscript{183} and again most recently in a report released in 2010.\textsuperscript{184} Hence, the reason why a “holistic approach” is required for ensuring aviation security, as the European Commission argues, which embodies a combination of a variety of devices and methods.\textsuperscript{185}

On a different note, the non-security related drawbacks of backscatter body scanners include the requirement of up to 45 seconds to completely scan a passenger, and therefore backscatter body scanners may hinder the flow of passengers.\textsuperscript{186}

5.5 THE PLAUSIBILITY OF THE THREAT POSED BY PLASTIC GUNS, CERAMIC KNIVES, AND LIQUID/CHEMICAL AND PLASTIC EXPLOSIVES

Since the privacy intrusion should match the threat for which it aims to prevent or address, in accordance with the principle of proportionality, those threats themselves should be evaluated and explained.

First of all, there is no evidence that guns completely made of plastic, including ammunition, exist. Even if they do exist, it is highly doubtful terrorists could get their hands on one. A Glock is probably the closest known weapon to a plastic gun, made of

\textsuperscript{182} Jonathan Corbett, an engineer and blogger, has published a video showing how he managed to go through a backscatter body scanner without the system detecting a small metal case that was stitched into a special side pocket of the shirt he was wearing. YouTube is understandably restricting access to the videos. As the UK Daily Mail reports, he suggests that this is because the body scanners “blend metallic areas into the dark background – so if an object is not directly placed on the body, it will not show up on the scan”. see Moran, Lee. “How to get ANYTHING through TSA nude body scanners: Blogger exposes loophole in $1billion fleet” (7 March 2012), available at: http://www.dailymail.co.uk/news/article-2111417/TSA-nude-body-scanners-Jonathan-Corbett-video-exposes-loophole.html\#ixzz1oRILtdLo


\textsuperscript{186} Wilber, Del Quentin. “Airport Security Technology Stuck In the Pipeline” (Washington Post, 8 February 2008), available at: http://www.washingtonpost.com/wp-dyn/content/story/2008/02/07/ST2008020704150.html
83% steel by weight, but it is clearly detectable by metal detectors. Besides, the manufacture of plastic guns or any other undetectable firearm, which has less than 3.7 ounces of metal, has been banned in the US since 1988. However, the law explicitly does not ban the manufacture of such weapons exclusively for US military or intelligence agencies, and nor does it prevent their possible manufacture in other countries.

The threat posed by ceramic knives, which have blades made from zirconia and handles made from nylon, has been exaggerated, to some extent, and is certainly not serious enough to merit the widespread use of backscatter body scanners, regardless if ceramic knives are even harder and can remain sharper than steel knives. Although terrorists managed to hijack airplanes using only box cutters and then tragically crash the airplanes into buildings on 9/11, today reinforced cockpit doors are securely locked throughout flights, as required by law. In addition, the Aviation and Transportation Security Act of 2001 (ATSA) sanctioned the expansion of the federal air marshal service and authorized pilots to carry firearms. However, a recent CNN nationwide investigation revealed that only an estimated 1% of commercial airline flights on a daily basis are in fact protected by armed federal air marshals and field offices are increasingly shorthanded.

There are threats posed by liquid/chemical explosives carried on a person onboard an airplane. But, these threats vary in degree, depending on the type of liquid/chemical explosive. On August 10, 2006, an apparent terrorist plot to blow up airplanes, reportedly using triacetone triperoxide (TATP) made onboard, was thwarted in the UK. This led to restrictions on bringing any type of liquid onboard airplanes. TATP is a liquid explosive composed of hydrogen peroxide, sulfuric acid and acetone, each essentially innocuous to aviation security on their own, but explosive when mixed together. Although

187 An Act to reauthorize the ban on undetectable firearms (Public Law 108-174), which reauthorized for a further ten years the Undetectable Firearms Act of 1988 (Public Law 100-649).
188 Ibid.
189 Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 104.
190 Ibid., SEC. 105.
191 Ibid., SEC. 128.
TATP is indeed explosive, with power close to that of TNT, the implausibility lies in the immense difficulty of mixing the chemical ingredients onboard an airplane, without the proper apparatus and the necessary low temperature conditions, while managing not to alert other passengers in the process. In addition, before TATP can be detonated it must first crystallize out of solution, which can take hours, and a considerable amount is required to bring down an airplane. Instead of making TATP onboard an airplane, the explosive could be carried onboard, undetected by conventional methods of screening, given that it contains no nitro groups or metallic elements. However, TATP is one of the most unstable explosives known and thus it is likely to detonate prematurely when carried on a person, i.e. before boarding an airplane.

There are numerous other explosives in liquid form, such as nitroglycerin, nitromethane and Astrolite G, a mixture of ammonium nitrate and hydrazine. But, these compounds also present difficulties for terrorists. Nitromethane gives off a very pungent smell, which would likely alert airport screeners, nitroglycerin is highly unstable and a noticeable amount would be required to bring down an airplane, and hydrazine is extremely toxic and corrosive. But, these challenges and hazards might not be enough to deter terrorists, and additional methods, beyond those discussed here, for developing liquid or chemical explosives are certainly possible.

Other explosives that pose a considerable more serious threat to commercial aviation security include plastic explosives, such as C-4, PE4, Semtex, PETN and polymer-bonded explosives (PBX). These explosives are ready for detonation, undetectable to metal-detectors, generally odorless and only a relatively small amount is required to bring down an airplane. PETN was the explosive used by Umar Farouk Abdulmutallab, which he hid in his underwear and managed to get through security at Amsterdam’s Schiphol Airport undetected, in order to attempt to destroy a Northwest Airlines aircraft on December 25, 2009 (known as the “Christmas Day attack”). It was also reportedly

---


196 see Ibid.


198 Ibid.
the same type of explosive molded into the soles of the shoes of Richard Reid in an attempt to destroy an American Airlines aircraft around eight years earlier.

5.6 ALTERNATIVES TO BACKSCATTER BODY SCANNERS

The security checkpoint at airports is essentially the last layer of security or defense in commercial aviation, besides the strategic placement of Federal Air Marshals onboard airplanes, the mighty capabilities of the US Air Force and NORAD, and technical countermeasures against shoulder-fired missiles. Before passengers reach security checkpoints, there are a number of additional security measures taken. Passengers are required to submit accurate and thorough personal data when reserving an airline ticket and are profiled or pre-screened against a terrorist watch list maintained by the TSA. Passengers are also required to present a passport or ID card before boarding and these identity documents are checked for authenticity. Passports and ID cards from around the world are increasingly becoming more sophisticated and difficult to forge, albeit certainly not impossible. Bomb-sniffing dogs are also important and are used at airports across the US. Other methods of passenger screening include Screening of Passengers By Observation Techniques (SPOT), whereby TSA officers, known as Behavior Detection Officers (BDOs), are specially trained to look for subtle suspicious indicators, such as particular facial gestures, in what is known as micro-expression training. Finally, domestic and foreign (human) intelligence is certainly also a critical factor, if not the most critical, in discovering a terrorist plot and preventing its execution.

Although technology is just one element of ensuring aviation security and for screening passengers at airport security checkpoints, it is considered key to the development of the so-called “checkpoint of the future”. The development, testing and deployment of technological equipment, which detects explosives in all forms, chemical/biological weapons and non-metallic weapons, is mandated as a “high priority” for the DHS. Technology has consistently been considered critical for ensuring aviation security. For instance, from 2003-2004, the TSA and the DHS funded over 200 R&D projects with the aim of developing technologies for enhancing the security of transportation, particularly in aviation. In 2004, the TSA spent 79.5% of its $159 million

---

199 see Title 49 U.S.C, Subtitle VII, Part A, Subpart III, Chapter 449, Subchapter I, Section 44925(a).

transportation security R&D budget on researching and developing aviation security technologies and the DHS spent 71.9% of its $88 million R&D budget for the same purposes. And, this is just a fraction of the total amount of money the US Government has spent on procuring aviation security technologies.

The technological alternatives to backscatter body scanners, discussed below, are other devices that can also facilitate the detection of threats hidden on a person during the passenger screening process. With the exception of active millimeter wave portals, several of these alternatives are considerably more privacy-friendly, yet still capable of helping to ensure aviation security. However, arguably none of these alternative devices or technologies are foolproof either.

Active millimeter wave portals, prominently manufactured by L-3 Communications, are another type of body scanner. They are also being piloted or deployed at numerous airports and other locations across the US. Rather than low dose X-rays, extremely high radio frequency (RF) energy/waves is projected onto the body’s surface, rendering clothes lucent, and an image is created from the radio waves reflected. Therefore, similar to backscatter body scanners, active millimeter wave portals can practically see through clothes and can potentially reveal concealed metallic or non-metallic threats. Millimeter wave portals, however, may require less time to scan each passenger. But, the ability of millimeter wave portals to detect low-density objects or materials, such as chemical or liquid explosives, is not certain and has been called into question. Another drawback is that airport screeners may likely require additional specific training in order to correctly analyze the active millimeter wave images.

While the images produced by active millimeter wave portals are different from the images produced by backscatter body scanners and appear to be not as graphically detailed, active millimeter wave portals are still highly privacy-intrusive, essentially equal to that of backscatter body scanners, and certainly considerably more intrusive than ordinary patdowns. Active millimeter wave portals gained popularity over backscatter body scanners not because they are more privacy-friendly, but rather because they do not project X-rays, which is a publicized concern of passengers.

Millivision’s Automatic Threat Detection (ATD) System uses passive millimeter wave imaging technology, as opposed to active millimeter wave imaging technology. The system detects and distinguishes the millimeter wave energy that is naturally emitted from a person’s body from the wave energy emitted from objects hidden under a

---

201 *Ibid.,* p. 4 and p. 22. However, this funding is not only for checkpoint security or passenger/luggage screening, and includes the CAPPS II program and technical countermeasures for defending against shoulder-fired missiles.
person’s clothes and then generates an image, which can potentially help to discover any concealed object.\textsuperscript{202}

Combining digital video recorders with passive millimeter wave imaging technology, Brijot’s BIS-WDS\textsuperscript{®} GEN 2 is also capable of screening passengers for both concealed metallic and non-metallic weapons and explosives, but fully avoids the privacy concern of seeing through clothes by neither generating an anatomically detailed image nor absolutely requiring security officers to monitor the images. An on-board computer comprised of an “intelligent detection engine” can (potentially) pinpoint in real-time the location of potential threats on any person, whether still or moving, who enters the system’s “field of view” and automatically alert security officers.\textsuperscript{203} Brijot’s system can examine a person in as little as 0.5 seconds and therefore does not slow down at all the flow of passengers.\textsuperscript{204} Brijot’s BIS-WDS\textsuperscript{®} GEN 2 is much like Rapiscan’s WaveScan 200, which also uses passive millimeter wave technology. The intelligent detection engine, however, likely requires further development and validation in order to be assured of its effectiveness. Brijot’s SafeScreen is another privacy-friendly alternative, whereby metals, plastics, ceramics, composites, liquids, gels, explosives, etc. can be discovered on a person by detecting and showing objects that are colder or hotter than the surface temperature of the subject, also without generating an anatomically detailed image. Brijot is marketing these devices as means for primary security screening at airports and other locations.

ThruVision has also developed similar imaging technology. The T5000 passive terahertz imaging system is equally capable of revealing both metallic and non-metallic objects hidden under clothing on multiple still or moving persons some distance away. Terahertz rays or T-rays are a form of low-level radiation, between infrared light and microwaves on the electromagnetic spectrum, and are naturally emitted from all materials. The T5000 works by collecting the T-rays emitted off a person and processing them to form images that reveal any concealed objects, also without displaying physical details of the body.\textsuperscript{205} Picometrix also develops similar terahertz imaging technology.

\textsuperscript{202} Millivision, available at: http://www.millivision.com/technology.html
\textsuperscript{203} The technology, however, still requires further advancement in order to be a trustworthy replacement of well-trained screeners, as pointed out by Eckard Seebohm, Head of the Aviation Security Unit of the European Commission during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels.
\textsuperscript{204} Brijot, available at: http://www.brijot.com/products/BIS-WDS_Gen2
The SPO camera units, developed by QinetiQ also use passive millimeter wave technology to detect the waves naturally emitted by the human body and to determine if there are any “cold” objects, such as metals, plastics and ceramics concealed under a person’s clothing. Suspicious objects are meant to trigger a red light on the display monitor, prompting the operator to search the individual. SPOs do not rely on image screening and can rapidly scan people simultaneously as they are moving, thereby neither producing still nor revealing images. The TSA deployed SPO camera units at the Denver International Airport during the 2008 Democratic National Convention.206

While passive millimeter wave technology and the BIS-WDS® GEN 2, T5000 and SPO are viable and privacy-friendly alternatives to backscatter body scanners, they are also not yet as sophisticated and especially do not generate images that are clear or detailed enough to offer the same degree of security benefits of active millimeter wave portals or backscatter body scanners.207 Moreover, these alternatives still require further testing and operational trials. For now, the TSA is testing passive millimeter technology at Boston’s Logan International Airport, and the technology is also being tested in the UK.

Alternatives to advanced imaging technologies include the explosive trace detection (ETD) technology of General Electric’s EntryScan, which is a trace portal machine (also known as a “puffer machine”). EntryScan works on the premise that when a terrorist prepares an explosive device tiny amounts of the explosive materials get on their skin, clothes or hair. When a person steps into the gateway of an EntryScan, air is blasted onto that person and the tiny particles that are liberated are collected and instantly analyzed for explosive chemicals. This screening methodology probably does not raise any privacy concerns. However, an obvious drawback with puffer machines is that they are not reliable if a terrorist has worn a full protective suit when preparing the explosive device concerned and has tightly sealed it in plastic. Puffer machines have been deployed in airports across the US, but they are currently being phased out due to maintenance issues and problems caused by dust and dirt continuously breaking down the machines.208

Other non-invasive ETD technologies or methods include the use of portable or stationary ‘swabbing devices’ that are able to detect explosive chemicals on a per-


207 This representatives from Schiphol Airport pointed this out during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels. The meeting was chaired by Eckard Seebohm, Head of the Aviation Security Unit of the European Commission.

Body scanners: A strip search by other means

son’s hands or on his or her hand bags. Thousands of these devices have already been deployed at US airports and the TSA has begun to randomly select people for hand swabbing. The devices can be used not just at security checkpoints, but also throughout an airport including at boarding gates. There are, however, also drawbacks with these devices. Legal and non-threatening substances could potentially result in ‘false positives’ and ‘false negatives’ could result when a terrorist has successfully managed to completely avoid touching the hidden explosive.

Ahura Scientific’s FirstDefender is a hand-held device that uses a method of analysis called raman spectroscopy to detect explosives or other chemicals in sealed plastic or glass containers. The FirstDefender works by projecting a laser beam onto the unknown solid or liquid substance and analyzing the light that scatters back to the device. Every substance scatters light in a unique way and the FirstDefender can determine the scattering patterns of a vast array of explosives, toxic industrial chemicals, toxic industrial materials and chemical warfare agents. The most serious drawback is that the FirstDefender cannot analyze substances in non-translucent containers or those hidden underneath clothes and a considerable amount of the substance is required. Prospective advancements in raman spectroscopy, known as Surface Enhanced Raman Spectroscopy (SERS), can incredibly enhance the sensitivity of this explosive detection technique, but the technology is still in its early stages.

On the other hand, the Fido® PaxPoint™, a handheld device developed by ICx Technologies, is capable of detecting liquids used in making explosive devices in both clear and opaque containers by analyzing vapors emitted from the bottle’s opening. The TSA is piloting the device.

The GK1, developed by Nemesysco, uses Layered Voice Analysis (LVA) technology to determine in advance the real intentions of people and to conduct a threat assessment by using input from 3-5 questions. The GK1 is like a lie detector. LVA uses signal-processing algorithms that can differentiate between a “normal” voice and a “stressed” voice. If the GK1 detects stress, security personnel can take the concerned person aside.

---


for further questioning and a patdown. The system is based on the premise that all voices have a certain frequency and any deviation from that frequency can indicate an increase in stress, excitement or anticipation. The GK1 has been tested at Moscow Domodedovo International Airport.\footnote{Nemesysco, available at: http://security.nemesysco.com/gk1.html} The GK1 is part of the growing movement towards using biometric sensors at airports to measure the body temperature, respiration and heart rate of passengers, which can be potentially used to determine their intentions or state of mind. However, voice analysis or other biometric sensors might not work on hardened terrorists that are neither physically nor emotionally affected by their mission. Moreover, the GK1 could unnecessarily subject people who are just naturally stressed and nervous to thorough questioning or a patdown by security personnel. The technology, however, is also not yet sophisticated enough.

A potential technological alternative to deploying new explosive detection devices or advanced imaging technologies is perhaps the comprehensive improvement of the PNR system and the requirement of additional personal data from passengers, including the more effective use of that data. In this case, more data protection rights may be sacrificed for greater corporeal privacy.

5.7 SCOPE OF DEPLOYMENT IN THE US

Backscatter technology has been around for decades, however, only recently has the US Government officially authorized the expansion of backscatter technology onto passenger screening and appropriated extensive funding to do so.\footnote{see Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), SEC. 4013.} Even before that, the US Government provided the necessary R&D funding for advanced X-ray screening systems for individuals.\footnote{see HR 1271, “FAA Research, Engineering, and Development Authorization Act of 1997” (Public Law No: 105-155)}

Backscatter body scanners have reportedly been either piloted or fully deployed at dozens of major international airports across the US, including: O’Hare in Chicago; JFK in New York; LAX in Los Angeles; Miami International Airport; Hartsfield-Jackson in Atlanta; George Bush International Airport in Houston; Dulles International
Airport; and Sky Harbor International Airport in Phoenix, Arizona. Backscatter body scanners are also being used in several prisons in the US and reportedly other domestic locations.

In the US, as of November 2009, according to the TSA and what has been reported, 46 backscatter body scanners were piloted at 23 airports, and 40 millimeter wave portals have been deployed at 19 airports. Six airports are using the advanced imaging technology for primary screening, rather than as an alternative to a patdown for secondary screening.

The TSA earlier on announced plans to deploy an additional 150 backscatter body scanners beginning 2010, already purchased from Rapiscan in 2009, at airport security checkpoints across the US and use them to replace WTMDs. And, as a consequence of Umar Farouk Abdulmutallab’s attempt to destroy a Northwest Airlines aircraft on December 25, 2009, using PETN hidden in his underwear and undiscovered by a patdown, the deployment of body scanners will only increase. Already the US Secretary for Homeland Security, Janet Napolitano, has announced that an additional 300 body


Other airports in the US where body scanners have been deployed include: Albuquerque International Sunport Airport; Baltimore/Washington International Thurgood Marshall Airport; Bob Hope Airport; Cleveland Hopkins International Airport; Denver International Airport; Detroit Metro Airport; Indianapolis International Airport; Jacksonville International Airport; McCarran International Airport; Raleigh-Durham International Airport; Richmond International Airport; Rochester International Airport; Ronald Reagan Washington National Airport; San Francisco International Airport; Salt Lake City International Airport; Tampa International Airport; Tulsa International Airport. see http://www.tsa.gov/approach/tech/imaging_technology.shtml, last visited 12/11/09.


218 see http://www.tsa.gov/approach/tech/imaging_technology.shtml


220 In acknowledging that the deployment of body scanners will likely increase, the stock market shares for the manufacturers of body scanners surged during the aftermath of the Christmas Day attack (particularly more so for backscatter body scanners). By January 11 2010, the shares of OSI Systems, Inc. (NASDAQ:OSIS) (parent company of Rapiscan), for example, jumped nearly 50%, from around $22 to around $32 a share.
scanners will be deployed in 2010.\textsuperscript{221} That makes a total of 450 additional body scanners planned for deployment in 2010.\textsuperscript{222} Furthermore, the Obama Administration revealed their proposed budget for 2011 (fiscal year October 2010-September 2011), subject to congressional approval, which allocates a whopping $734 million for Advanced Imaging Technology (AIT) and the procurement of 1,000 additional body scanners. However, at around $150,000 each, this funding would be sufficient to procure over 4,000 body scanners, which is more than enough to deploy body scanners at practically every airport security checkpoint in the US, with extra for airports outside the US.

On the other hand, none of the 150 backscatter body scanners purchased by the US Government in 2009 and delivered by Rapiscan have yet to be deployed and are currently (as of February 2010) reportedly still sitting in storage,\textsuperscript{223} but reportedly will be swiftly deployed.

\section*{5.8 LAWS, CODES AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE US}

In the US, as a common law country, case law and judicial interpretations of the Fourth Amendment of the US Constitution play a particularly important role. The Fourth Amendment provides:

\begin{quote}
The right of the people to be secure in their persons, houses, papers, and effects, 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.
\end{quote}


The Fourth Amendment gives individuals freedom from any unreasonable search and seizure conducted by the US Government and has significantly served as the basis of the right to privacy in the US, but is not explicitly a constitutional right to privacy per se.

As the US Supreme Court affirms “[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State”. At first, this was limited to physical intrusions upon a person’s property. However, adapting to technological advancements, the US Supreme Court in Katz v. United States later extended the interpretation of the Fourth Amendment to include not just properties or physical places, but also people, as long as the person concerned exhibits first “an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable”. This condition formulated by Justice Harlan is commonly known as the Katz test or the Harlan standard. The Fourth Amendment furthermore requires that the US Government “accept as axiomatic the principle that people harbor a reasonable expectation of privacy in their ‘private parts’.

In Kyllo v. United States, the US Supreme Court held that the use of a thermal imaging device to search for evidence in the interior of a home through its walls, which would otherwise not be possible without physically entering the home, constituted a search for the purposes of the Fourth Amendment and was unreasonable and thus unconstitutional without a warrant. In addition, the US Supreme Court based its judgment on the potential of thermal imaging to reveal intimate details. If the same legal reasoning is applied, the use of fully-intrusive backscatter body scanners to peer through an individual’s clothes, revealing intimate details, which would otherwise not be possible without physically removing that individual’s clothes, may also constitute a search for the purposes of the Fourth Amendment (Minert, 2006).

The US Supreme Court in Terry v. Ohio held that a warrantless search for weapons by a law enforcement officer is constitutional if it is “strictly circumscribed by the exigencies

225 see Olmstead v. United States, 277 U.S. 438 (1928).
227 Ibid., at 361. Concurring opinion of Justice Harlan.
230 Ibid.
which justify its initiation” and “limited to that which is necessary for the discovery of weapons which might be used to harm the officer or others nearby, and may realistically be characterized as something less than a “full” search, even though it remains a serious intrusion”. The 4th Circuit, just several years later, extended the reasoning of the US Supreme Court in *Terry v. Ohio* to justify airport searches using magnetometers to search for weapons in order to prevent the hijacking of airplanes and the subsequent physical “frisk”, depending on the information provided by the magnetometer.

Although the Fourth Amendment prohibits “unreasonable searches”, it nonetheless does not necessarily signify a warrant is required for all searches. Indeed, what the Fourth Amendment explicitly requires is that searches are “reasonable”. If the search is reasonable, then it is constitutional and, therefore, lawful.

While all passengers must be searched before boarding an airplane, it is widely recognized that the conduct of any border search must therefore still be reasonable and in accordance with the Fourth Amendment. Privacy does not just vanish at borders and US Customs agents or airport screeners are not given a blanket license to intrude upon the privacy of individuals. For instance, the limited right to privacy at airports does not entail that passengers can be strip searched without grounds of reasonable suspicion, regardless of the legitimate public interests. As the 9th Circuit Court affirmed, “exercise of the constitutional right to travel may not be conditioned upon the relinquishment of another constitutional right [i.e. the Fourth Amendment] […].”

The US Supreme Court has provided the preliminary grounds to determine if a search is reasonable. To determine its “reasonableness,” “the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted” must be considered. As the 5th Circuit Court in *United States v. Skipwith* affirmed, to determine the reasonableness of a border search the fol-

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


The following three factors must be considered: “public necessity, efficacy of the search, and degree of intrusion […].” The US Supreme Court, in another case several decades later, held that the reasonableness of a search can be determined “by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of a legitimate governmental interests.” Aviation security is undoubtedly considered a legitimate public (or governmental interests) and searches at airport security checkpoints undoubtedly play a critical role in ensuring aviation security.

US Customs agents or other authorized government officials are legally permitted to conduct searches of individuals at borders without a warrant. This is commonly known as the “border search exception”. Warrantless border searches are also deemed reasonable and acceptable under the Fourth Amendment since they occur at a border and have long been considered necessary in order for a state to protect itself and ensure legitimate governmental interests. US courts have firmly established that “the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior”. Airports located anywhere within the US act as the “functional equivalent of the border”. Moreover, it would obviously be impractical or unrealistic for the TSA to require a warrant to carry out airport security screening.

Border searches are divided into routine and non-routine. Routine border searches do not require reasonable suspicion to be carried out since they are minimally intrusive.

---


239 see Title 19 U.S.C. Chapter 4, Subtitle III, Part V, Section 1582 of the Tariff Act of 1930; Title 19 U.S.C. Chapter 3, Subtitle IV, Part 5, Section 482.


Based on the "border search exception", "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant". Non-routine border searches, on the other hand, require reasonable suspicion to be carried out, since they are considerably more intrusive.

A strip search is by law a non-routine (border) search and, thus, requires reasonable suspicion. As the 11th Circuit Court affirms, "[r]easonable suspicion to justify a strip search [at a border] can only be met by a showing of articulable facts which are particularized as to the person and as to the place to be searched". "A strip search under federal law includes the exposure of a person’s naked body for the purpose of a visual or physical examination". Alternatively, there are uniform statutory definitions from state legislatures of what constitutes a strip search. As the US Court of Appeals for the 4th Circuit affirmed:

Virginia’s statutory law, which is similar to that of most states, provides that, “[s]trip search shall mean having an arrested person remove or arrange some or all of his clothing so as to permit a visual inspection of the genitals, buttocks, anus, female breasts, or undergarments of such person". (emphasis added).

An X-ray search of an individual’s body is also by law a non-routine border search. As the US Court of Appeals for the 11th Circuit affirms:

In United States v. Pino, 729 F.2d 1357, 1359 (11th Cir.1984), we recognized that the “the amount of [reasonable] suspicion needed for an x-ray [is] ... the same amount needed for a strip search.” (citing Vega-Barvo, 729 F.2d at 1345).
A patdown is by law a routine border search and thus does not require reasonable suspicion.\textsuperscript{250} A patdown, also known as a frisk, is defined as:

to run the hand rapidly over the outer clothing of (a suspect) for the purpose of finding concealed weapons.\textsuperscript{251}

The TSA is a component of the DHS and was established with the enactment of the ATSA, which federalized airport screening. Absorbing the security responsibilities of the FAA, the TSA is now primarily responsible for the security of all forms of public transportation, which includes civil/commercial aviation, and for the development and implementation of security procedures thereof. Under this authority, the TSA is self-regulating the use of body scanners, whereby self-regulations and internal self-reporting, rather than legally binding ‘hard’ rules and independent, external inspection, are relied upon.

The self-regulations declare that the TSA does not store, print, transmit or export the images produced by the body scanners and the TSA has consistently proclaimed that the machines do not have these capabilities. The TSA also proclaims that it is their policy to use software cloaking or a privacy algorithm, also known as a “modesty filter”, which converts backscatter images into what the TSA describes as a “drawing”. In addition, a security officer views the images in a remote operator console. However, the rules governing the operating procedures of TSOs using the body scanners have not been revealed, which are supposed to be documented in standard operating procedures (SOPs). The TSA has refused to reveal the rules “due to the sensitivity of the technical and operational details”.\textsuperscript{252} For the same reason of not wanting to reveal sensitive information of a national security nature, the DHS initially refused to comply with a request under the Freedom of Information Act (FOIA) filed by EPIC for documents, contracts and procedures pertaining to the capabilities and technical specifications of body scanners in use. In response, EPIC filed a FOIA lawsuit against the DHS and, as a consequence, the DHS complied with some of EPIC’s demands by disclosing documents that reveal the technical specifications and the procurement contracts for body scanners with Rapiscan and L3.

Contrary to the previous declarations of the TSA that the body scanners are not capable of storing or transmitting the images generated, the documents obtained by

\textsuperscript{250} see United States v. Beras, 183 F.3d 22 (1st Circuit, 1999).

\textsuperscript{251} Merriam-Webster’s Dictionary of Law (1996).

\textsuperscript{252} Privacy Impact Assessment for TSA Whole Body Imaging, DHS, 17 October 2008, p. 4.
EPIC on TSA operational requirements and procurement specifications instead reveal that the TSA has indeed required that the machines have storage and export capabilities (albeit when in test mode, as opposed to screening mode), and an Ethernet interface connection that supports Transmission Control Protocol/Internet Protocol (TCP/IP). The official documents also confirm that the privacy algorithms can be disabled.

With regards to the admissibility of digital evidence, US courts may apply the Federal Rules of Legal Evidence. Rule 1001 (3) states:

An “original” of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original.”

Therefore, an image produced by a body scanner, used to justify the subsequent removal of a passenger’s clothes to attain the suspected concealed weapon or contraband, is admissible as evidence in a court of law.

Nevertheless, wrongfully obtained evidence, in violation of the Fourth Amendment, may be excluded from criminal proceedings in a court of law. This is commonly known as the “exclusionary rule.” As Rule 402 of the Federal Rules of Legal Evidence states:

All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

In accordance with the E-Government Act of 2002, a Privacy Impact Assessment (PIA) may need to be conducted for body scanners, if indeed the images generated are

---


254 Digital evidence may include, but is not limited to: the content of computer hard drives, computer printouts, GPS data, e-mails and digital video.

considered personally identifiable information.\textsuperscript{256} A PIA evaluates how personal information in identifiable form is collected, maintained and disseminated by government agencies. PIAs must be conducted before or during the development, procurement or modification of information technology systems, and not after, in order to “ensure sufficient protections for the privacy of personal information”.\textsuperscript{257} As a result, some argue that PIAs are grounded on the “precautionary principle”\textsuperscript{258} and serve as an example of the needed extension of this legal principle to the protection of privacy (Friedewald, M., et al. (eds.): SWAMI Deliverable D3, 2006).\textsuperscript{259}

5.9 DEFICIENCIES AND DILEMMAS OF THE US LEGAL FRAMEWORK

After assessing the effectiveness of the US legal framework in protecting privacy, based on the principles of privacy and the criteria of adequacy, significant legal deficiencies and dilemmas in the US come to light, with regards to the use of body scanners. Even if backscatter body scanners are determined to be the most effective devices for detecting liquid/chemical and plastic explosives, and other threats, which arguably has yet to be decisively proven, numerous privacy concerns and legal questions need to be addressed before this technology is further used on passengers. Fear of an “endless debate” must not overshadow these concerns.\textsuperscript{260}

\textsuperscript{256} US Federal courts have held, for example, that a videotape is a “record” for the purposes of the Privacy Act 1974, if the videotape contains the means of identifying the individual concerned (see: Albright v. United States, 631 F.2d 915 (D.C. Cir. 1980)). Thus, if the images generated by body scanners are stored in a “system of records”, in which the concerned individual’s image is identifiable, it is also possible that these images may constitute a “record” for the purposes of the Privacy Act 1974 and are, therefore, in this sense, subject to the Act. However, as argued in the next section, body scanner images may not necessarily constitute information in personally identifiable form.

\textsuperscript{257} E-Government Act of 2002, Section 208.

\textsuperscript{258} The precautionary principle was originally developed in the context of environmental protection and refers to the need to anticipate the plausible or potential environmental harm of an act, policy or technology, and to take preventive measures against the potential harm, even if there is uncertain scientific evidence proving the harm is real. The principle is found in the 1992 Rio Declaration on Environment and Development (Principle 15) and is also a core element of the EU’s environmental policy.

\textsuperscript{259} SWAMI (Safeguards in a World of Ambient Intelligence) was an EU project aimed to provide an overview of the key social, legal and ethical implications of ambient intelligence and highlight the privacy threats.

First of all, the legal framework, as it stands, does not fulfill the *use limitation and purpose specification principles*, nor does it ensure *clarity* or *foreseeability*. In terms of regulating the use of backscatter body scanners, the law does not clarify whether the use of backscatter body scanners is a routine or non-routine search or stipulate what level of suspicion is required before their use is permitted and under what legal protections. There is essentially no case law that explicitly defines or clarifies when the use of backscatter body scanners is reasonable and unreasonable or in accordance with the Fourth Amendment.\(^{261}\)

Since the TSA is already equating the use of (fully-intrusive) body scanners to a routine border search, their use can easily develop into the standard technique or primary means of passenger screening at airports, replacing not only patdowns, but also WTMDs. This was already suggested by (former) TSA Chief Kip Hawley with regards to millimeter wave portals.\(^{262}\) As Vina points out, “[b]y substituting the Body Scan for a patdown, Customs has ingeniously laid a foundation for a more liberal application of the Body Scan for now and in the future” (2002, p. 436). Hence, the most recent change in TSA’s policy regarding the circumstances surrounding the use of active millimeter wave portals.

As a result, eventually no level of suspicion or consent will be required. Once that legal justification is made and their use is considered the norm, there is also nothing to prevent the expansion of the use of body scanners to other locations (and for reasons other than aviation security), particularly if the advancement of body scanner technology increases the speed in which persons can be scanned, decreases the size of the devices, increases their portability, further increases the distance in which people can be scanned from\(^{263}\) and allows for the incorporation of the backscatter technology within CCTV sur-

---


263 In the Netherlands, the *NRC Handelsblad* reported that it has learned that the Rotterdam police department seeks to develop within three years a portable device that can see through people’s clothing to check for concealed weapons. According to *NRC Handelsblad*, Rotterdam’s police have received from the government a 500,000-euro grant to develop the device and are now approaching companies, universities and research institutes to develop it. While there are already devices, such as ThruVision’s T5000, that can see through people’s clothes meters away in the outdoors, portability for the police is also important. see Heck, Wilmer. “Dutch police try to develop x-ray vision” (NRC Handelsblad, 8 January 2010), available at: http://www.nrc.nl/international/Features/article2454112.ece/Dutch_police_try_to_develop_x-ray_vision
Body scanners: A strip search by other means

The law’s ambiguity could be stretched to initiate the use of body scanners at both public and commercial locations, such as sports arenas, mass transportation areas, government buildings, manufacturing sites, schools or shopping malls. Nevertheless, a body scan is already currently not genuinely voluntary. Forcing a person to choose between the rights enshrined in the Fourth Amendment and the right to travel “constitutes coercion”. As the EU’s Article 29 Data Protection Working Party argues, “[m]any passengers will consent to being scanned because by doing so they will avoid potential problems or delays, while their first priority is to get on board of their flight on time. Such consent is not sufficiently free”. The Article 29 Working Party further adds that “[i]f the consequences of consenting undermine individuals’ freedom of choice, consent would not be free”.

In 2008, the US House of Representatives approved H.R. 2200 (Transportation Security Administration Authorization Act), which aims to limit the use of body scanners in airport screening. Contrary to the recent change in TSA’s policy on the use of body scanners, Sec. 215 of H.R. 2200 prohibits the use of the devices as the sole or primary method of screening passengers and delineates their use as an optional alternative to patdowns in secondary screening. The bill was referred to the US Senate and, as of January 2012, no further steps have been taken.

While approving specific legislation regulating body scanners is called for, this particular piece of legislation is erroneous. The bill makes no mention of the mandatory use of privacy algorithms and in fact defines a body scanner (termed ‘whole body imaging technology’) as a device “that creates a visual image of the individual’s full body, showing the surface of the skin”. The words “showing the surface of the skin” certainly implies that the form of body scanners the bill is referring to include those with their

---

264 ThruVision’s terahertz ray technology already integrates CCTV technology allowing for enhanced public or urban surveillance.

265 For example, the New York Police Department is already testing terahertz imaging scanners (to be placed on police vehicles) for detecting concealed weapons. see Wagstaff, Keith. “Police Developing Tech to Virtually Frisk People from 82 Feet Away” (Time Magazine, 20 January 2012), available at: http://techland.time.com/2012/01/20/police-developing-tech-to-virtually-frisk-people-from-82-feet-away/


268 Ibid., p. 12.

269 On the other hand, Senators Klobuchar (D-MN) and Bennett (R-UT) introduced a bill that mandates the deployment of body scanners at US airports and mandates their use for primary screening.
full intrusive capabilities intact, i.e. those that generate the graphic images we should be concerned about, rather than those that employ modesty filters or privacy algorithms. Moreover, the bill proposes a framework that equates the use of body scanners, in their full intrusive manner, with appropriately conducted patdowns and permits their use as an alternative to patdowns. Therefore, the proposed bill correctly prohibits the use of fully-intrusive body scanners for primary screening purposes, but incorrectly promotes their use for secondary screening.

To compensate for the fact that a patdown conducted appropriately, or in accordance with the TSA’s SOPs, or as described in the TSA’s official training manual, is certainly less intrusive than the images generated by body scanners, whether backscatter or millimeter wave, and therefore their use as an alternative to patdowns is not justifiable, the TSA has made patdowns more intrusive. Last year, the TSA announced a new patdown procedure known as the ‘enhanced patdown’, which included patting down sensitive areas of the body – the breast and groin areas of females and the groin area of males.\(^{270}\) The enhanced patdown considerably increased complaints from passengers, particularly from female passengers. Since then, the TSA has instructed airport screeners not to touch female passengers between the breasts.\(^{271}\) Nevertheless, there have been numerous reports that passengers, who refused to go through a body scan and instead opted for a patdown, are being subjected to very thorough patdowns.\(^{272}\) Moreover, in accordance with the Screening Management SOP, patdowns may still now include the patting of “sensitive areas” of the body if deemed necessary.\(^{273}\)

On top of that, the law is inconsistent. Since a X-ray search of an individual’s body is considered by law to be a non-routine border search\(^{274}\) and backscatter body scanners emit X-rays, the minimal or no level of suspicion required at present to use backscatter

\(^{270}\) The full body patdown could be similar to the enhanced patdown.


\(^{273}\) The Screening Management SOP (Implementation Date: June 30, 2008), which was leaked on the web and is Sensitive Security Information for only the “Need to Know”, distinguishes between the different types of patdowns: full body patdowns; bulk-item patdowns; limited patdowns of the stomach area, the back and both legs; and finally patdowns that may include the patting of sensitive areas. The Screening Management SOP is different from the Screening Checkpoint SOP.

\(^{274}\) see Brent v. Ashley, 247 F.3d 1294 (11th Circuit, 2001).
Body scanners: A strip search by other means

Body scanners is contrary to case law. Furthermore, given that the end result of backscatter body scanners, without software cloaking, is similar to that of strip searches and far more intrusive than patdowns, the same legal reasoning behind conducting a patdown is inconsistently and wrongfully being applied to the use of backscatter body scanners.

As a result of the legal framework failing to bring clarity and legal foreseeability to the use of body scanners, the principle of enforcement/redress is also not fulfilled. In terms of clarifying when their use by an airport security screener has violated the Fourth Amendment and when evidence has been wrongfully obtained from their use, there are no laws specific enough to be enforceable in a court of law. As the US Supreme Court affirms, “the right allegedly violated must be defined at the appropriate level of specificity before a court can determine if it was clearly established”.275 Similarly, governmental agents are generally “shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known”.276 Consequently, TSA airport screeners or Transportation Security Officers (TSOs) are, at present, arguably shielded from legal action for any inappropriate use of body scanners.

The law, as it stands now, is not up to date with the capability of the latest visualization technology, since it is not in line with the technological reality that strip searches can occur by electronic means and without the need for a person’s clothes to be removed. Furthermore, the law does not permit the flexibility to adapt to new technologies. Due to the constrained definition of a strip search, generally accepted in the US, the use of body scanners cannot be legally construed to constitute a strip search. Therefore, even if the use of backscatter body scanners poses a similar degree of privacy intrusion as a full body strip search, the law is essentially unable to obligate the same level of suspicion.

The legal framework is dependent on self-regulations. Although the PIA conducted by the DHS on the deployment and use of body scanners essentially approves of the current circumstances surrounding their use, including the self-regulations and operating protocols of the TSA,277 over relying on the TSA to self-regulate the scope and manner of use of body scanners is naïve at best. Self-regulations, without the corresponding binding ‘hard’ laws as a basis and without the external enforcement mechanisms in place, are far from reliable. Such an approach to regulation elevates valid


concerns of accountability and supervision. But, the TSA already has a history of not always respecting privacy. For instance, the Inspector General of the DHS found that the "TSA did not consistently apply privacy protections in the course of its involvement in airline passenger data transfers",\(^{278}\) nor reliably disclose to the public the scope of its use and dissemination of passenger data.\(^{279}\) Besides, the SOPs governing the use of body scanners by TSOs are not \textit{readily accessible}. Moreover, the PIA conducted on body scanners is fundamentally based, for the most part, on the voluntary use of body scanners for secondary screening and not on the changed policy of the TSA to use body scanners in place of WTMDs for primary screening.

The legal framework pertaining to body scanners is, for the most part, \textit{ambiguous, altering and not legally binding}. Since the self-regulations are not binding or fixed, they could simply change at the discretion of the TSA, regarding, for instance, the employment of a modesty filter or privacy algorithm and the retention of backscatter images. As former TSA Chief Kip Hawley admitted, in an interview with Bruce Schneier, "We [TSA] do not now store [backscatter] images for the test phase (function disabled), and although we haven’t officially resolved the issue, I fully understand the privacy argument and don’t assume that we will store them if and when they’re widely deployed"\(^{280}\) (emphasis added). The DHS has reportedly asked the manufacturers of backscatter body scanners to de-activate the storage and data export capabilities of body scanners, but the DHS/TSA could just as easily re-activate these capabilities, and no law prohibits the TSA or security screeners from doing so, nor mandates that the body scanner manufacturers must de-activate or completely remove these capabilities in the first place. Essentially, since there is no binding law regulating the manufacture and design of body scanners, there is neither a guarantee that the images will not be stored or transmitted nor a guarantee that a privacy algorithm will always be employed. There is simply no binding law that mandates that the TSA must employ a privacy algorithm. In addition, the self-regulations do not sufficiently restrict the use of backscatter body scanners on children and pregnant women, nor evidently guarantee that an Image Operator or TSO of the same gender of the individual being scanned sees the backscatter images.

The TSA has already drastically altered their policy regarding the circumstances surrounding the use of backscatter body scanners and active millimeter wave portals.


\(^{279}\) Ibid., pp. 42-48.

The TSA previously announced that it will begin to pilot active millimeter wave technology in primary screening or in place of WTMDs at six airports (Tulsa International Airport, followed by the International airports in San Francisco, Las Vegas, Miami, Albuquerque, and Salt Lake City). Passengers who refuse to receive millimeter wave screening will undergo both walk-through metal detector screening and a patdown.281 As of November 2009, ten airports are now using the imaging technology for primary screening,282 and once again the TSA announced plans to use an additional 150 backscatter body scanners in place of WTMDs beginning in 2010. There is thus no guarantee that the use of body scanners, whether the backscatter or millimeter type, will remain as a voluntary alternative to patdowns or WTMDs.

The PIA on body scanners only confirmed that the DHS/TSA indeed intends to entirely replace patdowns for secondary screening with the use of body scanners, and even down the road to replace WTMDs with body scanners for primary screening. As the PIA declares, “[a] subsequent phase will evaluate WBI [Whole Body Imaging] technology for individuals undergoing primary screening”.283 The DHS/TSA is following through with this declaration and is now planning for all passengers to “go through the whole-body imager instead of the walk-through metal detector”, as announced by Robin Kane, TSA’s Assistant Administrator for Security Technology.284

Besides, PIAs, as they stand now, are focused primarily on personal data, and may not be fitting for body scanners. While body scanners generate images of the naked body, the images may not necessarily constitute information in personally identifiable form per se or in the legal sense, and nor are personal identifiers or the identification of the individual appended to the images. As a result, since body scanner images may not necessarily constitute a means of identifying the individual concerned, it is unlikely that the Privacy Act 1974 is applicable to the images generated by body scanners. In any case, the Privacy Act 1974 is certainly not applicable when the body scanner images are not actually stored, even though the images produced by (fully-intrusive) body scanners are seriously privacy-invasive.

---


The legal framework pertaining to privacy was equally designed to control data as traditionally understood and not to regulate privacy intrusion in other domains, such as the human body (Wood, 2006, p 89). The Privacy Act 1974, for instance, regulates how government agencies may collection, use, disseminate and retain personally identifiable information, and therefore it is immediately questionable if the nearly 40-year-old piece of legislation can effectively regulate body scanners. Moreover, the set of Fair Information Practice Principles (FIPPs), developed by the DHS, and used by the TSA as a template in the PIA on body scanners, oddly omit the essential principles of enforcement/redress and proportionality.

In addition, the legal framework, as it stands, does not fulfill the principle of proportionality. The law does not do enough to prevent the prospective required use of body scanners in their full intrusive capability on all air travelers, which would force hundreds of millions of people to be subjected to a strip search by electronic means. This would undoubtedly cause the potential use of body scanners to be disproportionate and unreasonable, since certainly that many people do not pose a threat to aviation security nor exhibit a reasonable level of suspicion to justify being electronically or digitally strip-searched.

Already the current approach of using body scanners is not proportional to their purported aim of ensuring the security of commercial aviation. If a traveler, whether domestic or international, sets off a walk-through metal detector at an airport’s security checkpoint or ‘arouses’ a minimal level of suspicion or is randomly selected for additional or secondary screening, known as “sweep screening,” or is selected by the Computer Assisted Passenger Profiling System (CAPPS), he or she is normally subject to a patdown or other special screening requirements. Even passengers wearing loose-fitting clothes, for instance, could be selected for secondary screening for unduly suspicion that they could be hiding something. Since TSA airport screeners, as a matter of policy, are currently using body scanners, where deployed, as an alternative to patdowns, their use automatically in practice does not require the same level of suspicion, if any, as a strip search. According to the TSA, an estimated two million passengers per week or 15% of air travelers are selected for patdowns.285 As a result, millions of passengers, who do not pose a threat to the security of commercial aviation, may potentially be subjected to a strip search by electronic means in order to exercise their right to travel.

The “reasonable expectation” of privacy, which is the foundation from which privacy is defined in the US, is also problematic. As a number of legal scholars have argued, the Katz test is flawed in that unless an individual takes extraordinary steps or

affirmative measures to protect his or her privacy, he or she does not have a subjective or reasonable expectation of privacy (Kearns, 1998, p. 1005; Paton-Simpson, 2000, p. 306). In addition, as Minert points out, society’s expectation of privacy could easily become a mere echo of the government’s expectation of privacy (2006, pp. 1653-54). Similarly, as the Report on the Surveillance Society argues, the reasonable expectation of privacy will surely be depressed if people “get used to” increasingly more surveillance (Wood, 2006, p. 80). This argument is consistent with the US Supreme Court’s judgment in 

Kyllo v. United States

that the more widespread the deployment and adoption of a particular technology the less “reasonable expectation” of privacy the public enjoys with respect to its use.286 This is also somewhat true for body scanners, as their deployment becomes increasingly widespread and well-known publicly. Moreover, the never-ending advancement and escalating deployment/use of PITs gradually diminishes our “reasonable expectation” of privacy, as people view the outcome to be increasingly necessary for their security/safety.

Although there is some case law applicable to backscatter body scanners, as outlined above, there is nevertheless a vacuum of law, which courts are left to fill in. Essentially, US statutory laws are inadequate for regulating the use and manufacture of backscatter body scanners. As a result, the legal framework is primarily dependent on case law for direction.

In sum, the US legal framework is inadequate to safeguard privacy with regards to the deployment and use of body scanners. Under the current conditions, whereby the employment of a privacy algorithm or the deletion of the images is not mechanically or automatically guaranteed and other safeguards are not legally binding, the use of body scanners as a primary means or secondary means of passenger screening is disproportionate and constitutes an unjustified violation of privacy in a democratic society. With the growing use of body scanners at airports across the US, the law, as it stands now, is unable to adequately uphold the integrity of the Fourth Amendment or defend the right to bodily privacy.

5.10 RECOMMENDATIONS ON ENHANCING THE US LEGAL FRAMEWORK

If we adopt the “originalist” or “textualist” approach to understanding the US Constitution, then entirely new laws should be adopted, when deemed necessary, by elected legislators/representatives, instead of over relying on the interpretations of judges, which can sometimes vary or be inconsistent.

Even if the use body scanners are deemed proportional to the legitimate aim of diminishing the threat posed by plastic guns, ceramic knives, and liquid, chemical, plastic explosives, new and specific laws are necessary nonetheless. Any new and specific legislative act on body scanners must be based, in part, on the principles of privacy, since body scanners and their growing deployment and use at airports are a threat to the right to privacy and the constitutional protections of the Fourth Amendment. Specific laws for body scanners, enacted by the US Congress, would eliminate the excessive dependence on US courts to fill in the existing legal vacuum. After all, only the legislative branch is meant to create law in the US, as opposed to the judicial branch, which is principally meant to apply it.

Legislation can either primarily regulate the design and manufacture of backscatter body scanners (rules on technical specifications) or instead primarily regulate their use (rules on operating standards). In other words, the full intrusive capabilities of body scanners can be maintained, while their use is strictly regulated, or the intrusive capabilities can be permanently limited during design and manufacture, thereby not requiring such strict regulation on their use. Either way, legislation should apply, where applicable, the core principles of privacy.

Focus on manufacturer-level regulations/laws

Regulation at the manufacturer-level should permanently minimize the intrusion upon privacy from the get-go. The burden is placed considerably more on the manufacturers rather than on the airport screeners. Legislation should mandate the automatic, built-in employment of a privacy software algorithm, in order to greatly reduce the intrusiveness of (backscatter) body scanners, thereby minimizing the infliction of indignity and humiliation upon individuals. It is important to note that the meaning of “built-in” here refers to the permanent employment of the software solutions, rather than a software add-on approach. The software can blur out the face and genitals and/

---

287 This approach is, for example, prominently advocated by US Supreme Court Justice Antonin Scalia. see, e.g., Scalia, Antonin. A Matter of Interpretation: Federal Courts and the Law (Princeton University Press, 1997).
Body scanners: A strip search by other means

or obscure the details associated with the entire body, in what is known as a “virtual fig leaf” or “modesty filter”. These capabilities are already available and are increasingly being further developed. Rapiscan, for instance, developed software that converts body scanner images into “generic figures”, which resemble an avatar, as opposed to an image of an individual’s genitals. However, it is essential to ensure that the effectiveness of these privacy algorithms or software solutions are validated and cannot be circumvented. Moreover, in no circumstances, should the privacy algorithms or filters or software solutions be capable of being disabled at airports.

Nevertheless, the creation of a “drawing” or “chalk outline” of one’s body, as it is often described as or referred to, may still remain somewhat or slightly intrusive and therefore, based on the use limitation and purpose specification principles, built-in restrictions on the ability to print, retain or otherwise distribute/export the backscatter images must be ensured. However, in exceptional circumstances, when a weapon or contraband is revealed, the limited retention, export or printing may be necessary as evidence in a court of law to justify the subsequent (targeted) patdown or, if legitimately justified, an ordinary strip search if challenged by the defendant. This may also be helpful to satisfy the access/participation principle. On the other hand, the retention of body scanner images may not be required at all. Nevertheless, in these very exceptional circumstances, if indeed required, an additional secure password, entered only by the Supervisory Transportation Security Officer (STSO), could override the built-in restriction and enable the image to be retained. This event must be automatically recorded.

In order to ensure the image data transmitted between the backscatter body scanners at the security checkpoint and the remote operator consoles is not intercepted, based on the security principle, the images must be encrypted and on top of that transmitted via a secure cable connection. The manufacturer must equally be required to ensure that the software fixes and built-in restrictions cannot be easily undone or bypassed.

Perhaps, in order to undeniably diminish the intrusive capability of body scanners, the images generated can also be monitored, like in Brijot’s imaging system, by an intelligent detection engine. However, intelligent detection software (also known as automatic threat recognition or ATR) may still require further advancement and testing in

---


289 Marc Rotenberg, Executive Director of EPIC, made this point during a brief discussion at the third annual international conference Computers, Privacy and Data Protection (29-30 January 2010, Brussels).
order to be a trustworthy replacement of well-trained screeners.\textsuperscript{290} Indeed, the development and testing is occurring. Software, developed by L-3, capable of analyzing body scanner images for threats, locating those threats and raising an alarm, could replace the need for human operators to view the images altogether. The software is currently being tested at Amsterdam’s Schiphol Airport and the initial results are reportedly positive.\textsuperscript{291} In addition to removing the need for a remote operator or viewer, the ATR capabilities can also potentially reduce the security implications of human errors. With ATR capabilities, security checkpoint personnel will only need to resolve the alarms by conducting, for instance, a targeted patdown of the area on a person where the (potential) threat (metallic or non-metallic object) was detected. The TSA is also evaluating the viability and effectiveness of the ATR capabilities, with ongoing trials, and a successful certification process is expected.\textsuperscript{292}

Essentially, once the intrusive capabilities of backscatter body scanners are without a doubt considerably and permanently narrowed, as guaranteed by the various technological limitations, including validated and trustworthy privacy algorithm/software solutions, their use will not qualify as a \textit{strip search by other means} and will be less intrusive than a patdown. Therefore, strictly under these conditions, body scanners may qualify as a routine search and may constitutionally replace (full body) patdowns as a mandatory means of secondary screening at airports and even perhaps legitimately replace the use of WTMDs altogether for primary screening, which does not require reasonable suspicion. This is contrary to Mock’s (2009) view that backscatter body scanners may not replace WTMDs, since a “drawing” or “chalk outline” of one’s body is more intrusive than a magnetometer search (Mock, 2009, p. 238).

Evidently, body scanners, even with the employment of a privacy algorithm, are considerably more effective than WTMDs, patdowns and other alternative devices in

\textsuperscript{290} As pointed out by Eckard Seebohm, Head of the Aviation Security Unit of the European Commission during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels.

\textsuperscript{291} During the second meeting (which I also attended) of the Task Force on Security Scanners, established by the European Commission, representatives from the Netherlands (the National Coordinator for Counterterrorism –NCTb) explained the success of the ATR software. The representatives also noted that the Data Protection Authority in the Netherlands has referred to the body scanners currently in use at Schiphol Airport as a “perfect example” of privacy by design.

helping to detect a variety of potential threats to aviation security. The mandatory use of modestly intrusive body scanners for secondary screening should satisfy those who argue that consent or offering a choice will cancel the security benefits of body scanners. This is a valid point, since terrorists will more than likely choose an ordinary patdown over being body scanned, as there is a far greater chance of finding a hidden threat with body scanners, especially if that threat is a relatively small amount of chemical or plastic explosive hidden very near to his or her genitals. The mandatory use of minimally intrusive body scanners for primary screening on all passengers should satisfy those who warn of the terrifying insufficiency of WTMDs and should eliminate the concerns over the discriminatory manner in which body scanners may be used. While minimally intrusive body scanners are more intrusive than WTMDs, here the significant security gains are arguably proportional to the somewhat greater privacy intrusion.

Nonetheless, proponents of body scanners argue that privacy algorithms could compromise the security benefits of the devices. A virtual fig leaf, for instance, could prevent a backscatter body scanner from revealing a plastic explosive attached to or near an individual’s genitals. The immense intrusive capability of backscatter body scanners and the full-body graphic images they generate is indeed what makes them very effective security devices. If, however, the images generated by body scanners remain fully intrusive, then the law must strictly regulate their use to ensure it is proportional to the security gains and that the right to privacy and freedom from unreasonable search and seizure is preserved.

Focus on user-level regulations/laws

Regulating the use, legislation should essentially harden the policies and self-regulations of the TSA, guaranteeing that they remain unchanged and are legally binding.

In addition to built-in restrictions on storing, printing and transmitting the images produced by body scanners, in line with the use limitation and purpose specification principles, the TSOs who view the images (Image Operators) should in no way be able to see simultaneously in person the passengers while being scanned. This can be accomplished through the continued use of remote operator/viewer consoles. The passenger being scanned should also remain unidentified, except in circumstances when a weapon or contraband is revealed. The law should also explicitly mandate that an Image Operator of the same gender must inspect the images, unless under extraordinary circumstances, which may occur where a TSO of the same gender is not available due to staff shortages or emergencies, in accordance with the Screening Management SOP.
with regards to patdowns.\textsuperscript{293} Moreover, to better ensure the images do not exist anymore than is needed for the purpose for which they were created and are not publicly disclosed in any way, cameras and mobile phones must also be absolutely forbidden within a remote operator console. This will prevent airport security personnel from taking photographs of the computer screens that display the images. Accordingly, based on the \textit{use limitation principle}, the law must prohibit any (unlawful) storage, photograph or public disclosure of the images.

Furthermore, in accordance with child pornography laws, the use of body scanners, at their full intrusive capability, on children and pregnant women must be restricted. The law must therefore specifically mandate that the images of children must always, without exception, employ software cloaking. The creation of body scanner images of children without software cloaking should be explicitly criminalized.

A “trusted passenger program”\textsuperscript{294} could be implemented, whereby qualified frequent flyers, which have volunteered sensitive data and have gone through an extensive security assessment/background check, are exempted from body scanners, unless they also arouse a reasonable level of suspicion. The TSA has already rolled out a similar program, known as “Precheck”, whereby approved travelers go through WTMDs instead of body scanners.

Based on the \textit{enforcement principle}, a dedicated screening supervisor at each airport or the corresponding STSO, under the management of the Transportation Security Manager (TSM), should conduct the direct supervision of the compliance of these binding rules (rather than simply general uniformed personnel of the TSA or TSOs). Thus, the responsible individual should have the power to initiate the dismissal of any airport screener who repeatedly fails to comply. In addition, a dedicated oversight committee, together with the DHS Office of Civil Rights and Liberties, DHS Privacy Office, and the Privacy & Civil Liberties Oversight Board,\textsuperscript{295} could direct the nationwide compliance of the rules.

In addition to the capacity of air travelers to bring a claim against the US Government (or private security screeners that act on behalf of the government, for the unreasonable or unlawful use of body scanners), the DHS Traveler Redress Inquiry

\textsuperscript{293} see the Screening Management SOP (Implementation Date: June 30, 2008).

\textsuperscript{294} see Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 109.

\textsuperscript{295} The Privacy and Civil Liberties Oversight Board (PCLOB) was established after recommended by the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission). The PCLOB is as an independent agency within the executive branch.
Body scanners: A strip search by other means

Program (DHS TRIP)\textsuperscript{296} or a dedicated redress program, in accordance with the \textit{redress principle}, must facilitate an immediate investigation of such claims. While the Privacy Act 1974 limits judicial remedy, under the legislative act, to US citizens or US lawful permanent residents (LPRs), significant to the use of body scanners at airports, TRIP is open to all individuals regardless of whether they are US citizens, LPRs or simply visitors to the US. Therefore, as a matter of DHS policy, foreign passengers or non-US persons could also have the right to seek (administrative) redress for the wrongful use of body scanners. However, preferably the law should open the door for foreign passengers or non-US persons to seek judicial remedy for the unlawful, disproportional or inappropriate use of body scanners.\textsuperscript{297}

Based on the \textit{principle of proportionality}, the use of backscatter body scanners, \textit{at their full intrusive capability}, must require the same level of reasonable suspicion as a strip search and must not be equated with an appropriately conducted patdown. In order to do so, the definition of a strip search must be modified to equate the use of backscatter body scanners and other similarly intrusive technology to a virtual strip search, thereby causing their use to be considered a non-routine search. For clarity, the content of the definition would need to accommodate for the fact that a strip search is possible by electronic means and without the need for a person’s clothes to be removed. A definition of a strip search, in line with backscatter technology, and anticipatory of the further advancement of similarly intrusive technology, such as active millimeter wave portals, should read as follows:

\textit{A strip search shall mean the visual inspection of the genitals, buttocks, anus, female breasts, or undergarments of an individual either in person or through any electronic means.}

Above and beyond the laws that regulate the manufacture and/or use of body scanners, the airports that have opted out of federal screening and switched to qualified, authorized private airport security screening companies, in accordance with the Aviation and Transportation Security Act of 2001,\textsuperscript{298} should perhaps have the freedom to decide

\textsuperscript{296} DHS TRIP serves as a means for individuals who believe they have been improperly denied entry or identified for additional screening by a DHS component at a transportation hub to file a request for redress.

\textsuperscript{297} The legal fact that the Privacy Act of 1974 limits judicial remedy to US citizens or US legal permanent residents has been criticized by the EU in the negotiations with the US over a transatlantic binding agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof; see the Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, May 2008.

\textsuperscript{298} Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 108.
whether or not they want to deploy body scanners in the first place. However, the decision to permit this option is certainly debatable.

The deployment of *minimally intrusive* body scanners at other locations (e.g. train stations or major sports stadiums) may also be permissible on a case-by-case basis. Nevertheless, even if privacy algorithms and other technical measures are permanently employed to safeguard privacy, the law must also prohibit the deployment and use of body scanners by private actors (other than authorized, private airport screening companies).

Lastly, in order to improve security overall, similar to the California Penal Code, Federal law should prohibit the commercial manufacture of knives undetectable to WTMDs by mandating that all knives contain a minimum quantity of metal.

### 5.11 MANUFACTURER-LEVEL OR USER-LEVEL REGULATION?

Whether manufacturer-level or user-level laws/regulations for regulating body scanners should be predominantly chosen depends on which is a better approach or policy option for balancing privacy with security.

The automatic, permanent incorporation of privacy filters or algorithms, within the images generated by body scanners, can implement the privacy principles and, in doing so, can lawfully and justifiably increase both the deployment and employment of body scanners at airports. Therefore, the manufacturer-level approach can, at the same time, both increase security gains and protect the privacy of a person’s body by reducing the level of graphic detail contained in the images. In addition, privacy algorithms do not necessarily cancel the security gains of body scanners, but rather can potentially help airport screeners, albeit with some further training and technical advancement, to objectively detect threatening objects. The potential for developing effective intelligent detection software can further aid in this detection. Any questionable identification of objects to the airport screener could perhaps be compared with the images of known objects before a decision is made to proceed with a patdown.

Since the user-level regulatory approach will maintain the full graphic details of the images generated by body scanners, their use will only constitutionally replace strip searches, and therefore will neither address the flaws of the primary nor secondary means of security screening.

In the long run, therefore, the manufacturer-level regulatory approach may favor both privacy and security, but nonetheless manufacturer-level regulations/laws will

---

299 see Section 12001.1 of the California Penal Code.
need to be combined with some user-level regulations/laws, in order to ensure the fulfillment of all the principles of privacy.

5.12 INTERNATIONAL DEPLOYMENT, DEVELOPMENTS AND RESPONSES

The deployment of backscatter body scanners and active millimeter wave portals is gradually spreading around the world. In Europe, the Netherlands and the UK are leading the way in testing and deploying body scanners. In Italy, the Italian Civil Aviation Authority has also deployed and tested body scanners in Rome and Milan and, in Rome’s second largest airport, Brijot’s passive millimeter wave imaging technology was also tested. Body scanners were also tested in France and Germany.

The UK began testing active millimeter wave portals in 2006 at London’s Heathrow Airport and Paddington Railway Station, and began testing backscatter body scanners at Manchester’s international airport. Body scanners are being deployed in more airports across the UK. Previously, there were even proposals to install millimeter wave portals throughout London’s tube stations, but this was later rejected due to impracticalities. Instead of offered as an alternative to patdowns, passengers in the UK are randomly chosen. There are also calls and initiatives for the compulsory use of body scanners in all UK airports. Concerns previously emerged that the body scans deployed in the UK allow the images to be printed, after it was reported that body scanner images of the ‘Bollywood’ movie star Shah Rukh Khan were distributed among London’s Heathrow Airport security personnel.

On the other hand, Her Majesty’s Revenue and Customs (HMRC), a UK governmental department responsible for administering screening measures at points of entry and exit, had also previously took a step in the right direction for privacy and awarded a contract to Brijot Imaging Systems Inc. for its privacy-friendly BIS-WDS® GEN 2 millimeter wave systems, which will be deployed at airports.

300 Webster, Ben. “Body scan machines to be used on Tube passengers” (Times Online, 8 July 2005), available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article541746.ece


In the Netherlands, active millimeter wave portals were deployed in 2007 at Schiphol International Airport. However, rather than initially being used on a trial basis, they have already been formally introduced into the screening process at several security checkpoints. As a joint initiative of the National Coordinator for Counterterrorism (NCTb), Customs authorities and Schiphol Airport, the use of millimeter wave portals, like in the US, is self-regulated. However, these self-regulations are backed by comprehensive privacy/data protection legislation in the Netherlands. According to the self-regulations, the image analyst sits in a closed space and cannot see in person the passenger who is being scanned and the images are not saved. Rather than using a modesty filter, only the face of the passenger is made “unrecognizable” in the images. Although the millimeter wave portals are voluntary, meaning that passengers have a choice between millimeter wave portals or going through regular security procedures, this is only for the time being and, like the self-regulations of the TSA, is subject to change. Already, Schiphol Airport is planning to deploy more body scanners and all passengers flying to the US must go through body scanners since the so-called “Christmas Day attack”.

The EU was en route to adopting body scanners as a common method of passenger screening, but that was previously put on hold. Article 4(2) of Regulation (EC) No 300/2008 on common rules in the field of civil aviation security requires the European Commission (EC) to adopt general measures on aviation security, which must include the ‘methods of screening allowed’. The EC then proposed in a draft regulation the use of body scanners as a means of screening passengers at airports. In response, the European Parliament voted overwhelmingly to demand a full study on the impact of body scanners relating to fundamental rights, privacy and health before taking a decision on the introduction of body scanners at airports, noting that the use of body scanners is “equivalent to a virtual strip search” and has “a serious impact on the fundamental rights of citizens”.

As a result, the EC, and more specifically the Body Scanners Task Force, prepared a communication, in consultation with the Article 29 Working Party, EDPS and other interested parties and stakeholders, and based on the answers received to a questionnaire.

305 Schiphol International Airport, available at: http://www.schiphol.nl/
Body scanners: A strip search by other means

made available to the public.\textsuperscript{308} The communication addresses the European Parliament’s concerns and questions and briefly provides an assessment on the effectiveness of body scanners on enhancing aviation security. Meanwhile, as a consequence of the so-called “Christmas Day attack”, the US upped the pressure on Europe to deploy body scanners.\textsuperscript{309} But, the EU remained steadfast on its previous commitment to wait until the EC completes their assessment of the privacy concerns and validated security benefits of body scanners before deciding on whether or not to bring forward legislation on a common EU approach to deploying and using body scanners as a method of screening at EU airports and under what conditions. During the second meeting of the Task Force on Security Scanners, the EC announced that an impact assessment on body scanners will be launched and completed next year (2011).\textsuperscript{310} The EC urged that a common EU approach

\textsuperscript{308} The first meeting/public consultation of the Task Force on Security Scanners was held on 12 December 2008 at the Centre Albert Borschette in Brussels, of which I was an active participant. The meeting was chaired by Eckard Seebohm, Head of the Aviation Security Unit of the European Commission. Present at the meeting were numerous relevant stakeholders, including representatives of the manufactures of the different body scanners on the market (L3, Brijot, Rapiscan, Millivision and others), the International Air Transportation Association (IATA), ACI Europe, Schiphol Airport, the Dutch Ministry of Justice, the CEBRN programme of the UK Home Office, the Article 29 Working Party, European Data Protection Supervisor (EDPS), Fundamental Rights Agency (FRA), the European Cockpit Association (ECA), and the assistant to MEP Philip Bradbourn, an outspoken critic of body scanners. There was essentially a consensus among the stakeholders that body scanners are significant for enhancing aviation security, but certain privacy safeguards are required. Indeed, the EDPS and FRA are not completely against body scanners, but are instead hesitant. I pointed out the need to incorporate ‘privacy by design’ solutions, which representatives from the Article 29 Working Party, FRA and EDPS equally advocated. Representatives of L3 and Rapiscan confirmed that design solutions are feasible and already available and may include anything from blurring the face to converting the body scanner images into animations or even holograms. The representative from L3 further expressed the concern that manufacturers of body scanners have not been given any clear standards to follow during the design and development of the body scanners. I raised the notion that passive millimeter wave imaging is a privacy-friendly alternative to backscatter body scanners or active millimeter wave portals, which of course delighted the representative of Brijot. However, the representatives from Schiphol Airport objected to this point and noted that Brijot’s systems do not provide images that are clear or detailed enough to offer the same degree of security benefits of active millimeter wave portals or backscatter body scanners.

In a follow-up email to a Policy Officer at the Aviation Security Unit, nearly a year after the task force meeting and closing of the public consultation, I learned on 26/11/09 that no summary for that consultation was published, no further meeting was scheduled and a legal initiative was yet to be foreseen. In other words, the EC was taking their time to develop the report/communication requested by the European Parliament. However, as a consequence of the “Christmas day attack”, the EC accelerated the adoption of this communication on body scanners, which was published in June 2010.

\textsuperscript{309} see Hsu, Spencer S. “U.S. to push foreign governments to use body scanners at airports” (Washington Post, 8 January 2010), available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/07/AR2010010704282.html

\textsuperscript{310} Upon invitation, I also attended the second meeting of the Task Force on Security Scanners, held 14 September 2010 in Brussels. The meeting served to further debate some of the key privacy and health issues/impacts surrounding body scanners, and to discuss the detection performance of body scanners. In addition to representatives from various stakeholders, representatives from EU Member States were also present at the meeting.
be taken, in order to better ensure both the protection of privacy and other fundamental rights and the maintenance of aviation security. The EC also urged that a combination of technical specifications and operational rules is the way forward.\textsuperscript{311}

In 2011, the European Parliament approved the deployment of body scanners at EU airports, but banned the use of the backscatter type and insisted that passengers continue to have the right to refuse to be scanned. Although the EU has in the end approved of the use of body scanners, at least there is an apparent agreement within the EC and among most EU Member States that specific, fixed and binding legislation should regulate the development, deployment and use of body scanners throughout the EU, unlike in the US where there is still an excessive reliance on altering self-regulations. Since air passengers travel from the US to the EU and vice-versa, they arguably deserve the same level of privacy protection. For that reason, US and EU regulations on body scanners should be similar. On the other hand, if the EU does not adopt a common position on the deployment and use of body scanners, then it will be up to EU Member States to adopt their own regulations.

Body scanners were also tested at Melbourne International Airport in Australia, which at the time decided not to blur out the genitals in the images,\textsuperscript{312} and the Australian Government announced its decision to deploy body scanners at airports throughout the continent.

According to a survey study conducted by the IT firm Unisys in April 2010, as part of the Unisys Security Index, the vast majority of air travelers in the UK, Germany, Netherlands and Australia, with the exception of Spain, are apparently willing to support, to a certain degree, the deployment and use of body scanners, in return for greater aviation security.\textsuperscript{313}

The US has also been pressuring additional countries to deploy body scanners and urged the International Civil Aviation Organization (ICAO) to adopt an agreement on improving security standards with the help of body scanners. Whether or not the deployment of body scanners will be globally accepted is yet to be seen.


\textsuperscript{313} The survey results are available at: http://www.unisyssecurityindex.com/
5.13 CONCLUDING REMARKS

Although the legal framework in the US does not require a complete overhaul, in order to ensure that the deployment and use of body scanners is both constitutional and proportional and does not erode the right to (bodily) privacy, specific statutory laws are required.

The use of body scanners potentially offers immense security benefits and should certainly not be outright prohibited. However, until the necessary binding laws are adopted and put into effect concerning their manufacture, use and deployment, the violation of privacy is disproportionate. In the meantime, there are alternative means of ensuring the security of commercial aviation, albeit probably not as effectively, which can also ensure privacy and uphold the integrity of the Fourth Amendment.