Health Matrix: The Journal of Law-Medicine

Volume 22 | Issue 2

2013

Security Scanners in Comparative Perspective

Gregory S. McNeal

SECURITY SCANNERS IN COMPARATIVE PERSPECTIVE

Gregory S. McNeal[†]

INTRODUCTION

In this article, I will take a comparative look at regulations governing the use of airport full-body security scanners. A comparative look is valuable because the use of scanners, while controversial, is not solely an American phenomenon. In fact, the European Union (EU) analyzed the implementation of security scanners and placed regulatory controls on their use before the controversy in the United States erupted. This essay proceeds in two parts. In Part I, I explain the EU regulations governing the use of security scanners. In Part II, I present an overview of relevant U.S. laws governing the use of security scanners and demonstrate the similarity between the challenges and solutions implemented under the European and U.S. fielding of security scanners. I conclude by arguing that the concerns raised by security scanners can be sufficiently mitigated with advanced technology that maximizes the interest in security while also protecting individual liberty.

Prior to discussing the law dealing with security scanners, it is necessary to provide some background on the plots which prompted their implementation. In the aftermath of the terrorist attacks of September 11, 2001, governments around the world rushed to address the strategic vulnerabilities, particularly in intelligence and aviation, made so apparent on that fateful day. A massive effort ensued in the United States to reorganize the infrastructure and increase the ability of government to prevent another terrorist attack. The flow of resources to executive agencies was dramatically increased under the assumption that it would enhance their operational capabilities. The United States was not alone in these efforts. Europe, Canada, and other nations around the world took note of the devastation caused by only nineteen

---

[†] Gregory S. McNeal, Associate Professor of Law at Pepperdine University School of Law. Thanks to the symposium editors at Case Western Reserve University School of Law for organizing this issue.

hijackers and took steps to restructure civil aviation security standards. Despite these efforts, the chief concern for politicians, intelligence, and security officials became not if, but when and how severe the next terrorist strike would be.

Since September 11, 2001, al-Qaeda and its off-shoots have evolved, changing their tactics in response to U.S. and European security practices. While al-Qaeda took enormous pride in its ability to successfully carry out the 9/11 attacks,[1] it also knew that such an opportunity would not remain available for very long, especially after security measures on civilian aircraft changed to prevent terrorists from taking control of the cockpit. Nevertheless, al-Qaeda and associated terrorist groups retained their obsession with exploiting the vulnerabilities unique to civil aviation. Instead of aiming to take control of airplanes and use them as weapons, al-Qaeda realized it could instill fear by detonating bombs onboard civilian airplanes while in flight. On December 22, 2001, Richard Reid (popularly known as the "Shoe Bomber"), attempted to detonate explosives concealed in his shoe while on board American Airlines Flight 63.[2] In 2006, British law enforcement uncovered a plot to detonate liquid explosives that were to be carried on board seven transatlantic flights travelling from the U.K. to the United States and Canada.[3] These two plots stick out in the minds of many air travelers because the attempts prompted security authorities to require passengers to remove their shoes at checkpoints and institute the 3-1-1 liquid and gel policy.[4]

There have been several foiled attempts in the past decade; however, two attempts in particular drew special attention from intelligence and security officials. Both plots were ultimately traced back to a group that many intelligence officials now believe constitutes the

---

[1] *See, e.g.*, LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11 358 (2006) ("The accomplishment of striking the two towers was an overwhelming signal of God's favor . . . ."); Mike Boettcher, *Detainees Reveal bin Laden's Reaction to Attacks*, CNN.COM (Sept. 10, 2002), http://articles.cnn.com/2002-09-10/us/ar911.osama.exclusive_1_bin-terrorist-leader-khalid-shaikh-mohammed (recounting bin Laden's behavior while events unfolded, which included him weeping, praying, telling his followers to "'Be patient,'" and holding up two, three, then four fingers before each subsequent plane crash).

[2] Michael Elliott, *The Shoe Bomber's World*, TIME, Feb. 25, 2002, at 46, 46.

[3] John Ward Anderson & Karen DeYoung, *Plot to Bomb U.S.-Bound Jets Is Foiled*, WASH. POST, Aug. 11, 2006, at A1, A11.

[4] *See Make Your Trip Better Using 3-1-1*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/311/index.shtm (last visited Jan. 4, 2012); Sheldon H. Jacobson, *Watching Through the "I"s of Aviation Security*, 5 J. TRANSP. SECURITY 35 (2012).

greatest terrorist threat to the United States, and civil aviation in particular: al-Qaeda in the Arabian Peninsula (AQAP).[5]

The first notable attempt was the assassination plot by Abdullah Hasan al-Asiri against Saudi Arabian Prince and Chief of counterterrorism Mohammed bin Nayef.[6] Al-Asiri detonated a carefully concealed explosive device that tore the terrorist operative's body into seventy pieces.[7] Questions about the assassination attempt quickly mounted. How was al-Asiri able to get a bomb so close to such an important member of the Saudi family—the chief of counterterrorism no less? Al-Asiri had been searched several times, he had spent 24 hours with the prince's guards, and had even flown on the prince's aircraft.[8] Less than four months later, on December 25, 2009, a twenty-three year old Nigerian man named Umar Farouk Abdulmutallab (commonly known as the "Christmas Day Bomber" or the "Underwear Bomber") boarded Northwest Airlines Flight 253 en route from Amsterdam to Detroit.[9] As the flight was approaching Detroit, Abdulmutallab went to the bathroom where he remained for approxi-

---

[5] *See Al-Qa'ida in the Arabian Peninsula (AQAP)*, NAT'L COUNTERTERRORISM CTR., http://www.nctc.gov/site/groups/aqap.html (last visited Jan. 4, 2012); Jonathan Masters, *Al-Qaeda in the Arabian Peninsula (AQAP)*, COUNCIL ON FOREIGN REL. (Dec. 7, 2011), http://www.cfr.org/yemen/al-qaeda-arabian-peninsula-aqap/p9369 ("President Barack Obama has described AQAP as 'al-Qaeda's most active operational affiliate,' echoing an acknowledgment from U.S. counterterrorism officials that the threat from AQAP has supplanted that of the al-Qaeda core."); FRANK J. CILLUFFO & CLINTON WATTS, HOMELAND SEC. POLICY INST., YEMEN & AL QAEDA IN THE ARABIAN PENINSULA: EXPLOITING A WINDOW OF COUNTERTERRORISM OPPORTUNITY (June 24, 2011), http://www.gwumc.edu/hspi/policy/issuebrief_yemenaqap.pdf ("The Foreign Operations Unit's special knowledge of the U.S. and unique destructive capabilities make AQAP an immediate threat to the U.S."); *see generally* SAMUEL LINDO, MICHAEL SCHODER & TYLER JONES, CTR. FOR STRATEGIC & INT'L STUD., AL QAEDA IN THE ARABIAN PENINSULA (July 2011), *available at* http://csis.org/files/publication/110722_Lindo_AQAP_AQAMCaseStudy3.pdf (describing past and future threats of AQAP).

[6] *See* Michael Slackman, *Would-Be Killer Linked to Al Qaeda, Saudis Say*, N.Y. TIMES, Aug. 28, 2009, at A9; David Gardner, *Air Passengers Face Full Body X-rays After Suicide Bombers Hide Devices INSIDE Their Bodies*, DAILY MAIL (Oct. 8, 2009) http://www.dailymail.co.uk/news/article-1218562/Bombers-hide-devices-inside-bodies-Travellers-Europe-face-body-X-rays.html.

[7] *See* Gardner, *supra* note 6.

[8] *See id.*

[9] *See* Mark Hosenball, *The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK (Jan. 1, 2010, 7:00 PM), http://www.thedailybeast.com/newsweek/2010/01/01/the-radicalization-of-umar-farouk-abdulmutallab.html; *From Shoes to Soft Drinks to Underpants: The Attempted Bombing of an Airliner Highlights Gaps in Intelligence-Sharing and Airport Security*, ECONOMIST, Jan. 2, 2010, at 21, 21 [hereinafter *From Shoes to Soft Drinks*].

mately twenty minutes.[10] After returning to his seat with a blanket covering his midsection, passengers sitting nearby began to hear popping noises and watched as Abdulmutallab's leg caught fire.[11] A passenger who was sitting close by managed to subdue Abdulmutallab while flight attendants used fire extinguishers to put out the flames.[12] It was revealed shortly thereafter that Abdulmutallab had attempted to detonate a six-inch package of PETN[13] and triacetone triperoxide (TAPN) that had been sewn into his underwear.[14] It was also revealed through his confession that he had been trained and directed by AQAP, which subsequently claimed credit for the attempt.[15]

Both attempts originated in Yemen, the headquarters of AQAP. Both attempts utilized the explosive powder, PETN. Most importantly however, both attempts concealed explosive devices in such a way that standard search practices, by hand or by metal detector, would not reveal their presence. For this reason, these two attempts had a major impact on intelligence and security officials. Although TSA officials were already exploring the use of X-ray systems at security checkpoints, these attempts prompted policymakers to expedite the process of deploying such technology to airports across the United States, Europe, and Canada. It is in the context of these types of plots that government officials are analyzing the use of security scanners.

I. EUROPEAN UNION REGULATIONS

After 9/11, the EU took steps to review and reorganize aviation policies and procedures into a common aviation security framework for EU member states. The European Parliament and Council insti-

---

[10] *See* Hosenball, *supra* note 9.

[11] *See id.*; *From Shoes to Soft Drinks*, *supra* note 9, at 21; Kenneth Chang, *Explosive on Flight 253 Is Among Most Powerful*, N.Y. TIMES, Dec. 28, 2009, at A14.

[12] *See* Hosenball, *supra* note 9; *From Shoes to Soft Drinks*, *supra* note 9, at 21.

[13] *See generally* Malcolm W. Browne, *Readily Available, PETN Is Easily Molded and Hidden*, N.Y. TIMES, Aug. 23, 1996, at B6 (providing information on accessibility and use of PETN).

[14] *See From Shoes to Soft Drinks*, *supra* note 9, at 21; Aliyah Shahid, *What is PETN? US-Bound Packages Contained the Explosive, Similar to Christmas Day Underwear Bomber*, N.Y. DAILY NEWS (Oct. 30, 2010) http://articles.nydailynews.com/2010-10-30/news/27079712_1_suspicious-packages-petn-semtex; Indictment at 2, United States v. Abdulmutallab, No. 2:10-cr-20005 (E.D. Mich. Jan. 6, 2010), 2010 WL 229849.

[15] *See* Hosenball, *supra* note 9; Anahad O'Connor & Eric Schmitt, *Terror Attempt Seen as Man Tries to Ignite Device on Jet*, N.Y. TIMES (Dec. 25, 2009) http://www.nytimes.com/2009/12/26/us/26plane.html; *From Shoes to Soft Drinks*, *supra* note 9, at 21.

tuted Regulation (EC) 2320/2002, which was among the first of such measures to establish basic security standards for civil aviation common to all EU member states in order to prevent "acts of unlawful interference."[16] Regulation (EC) 300/2008 has since superseded Regulation (EC) 2320/2002;[17] however, the provisions regarding passenger screening have remained largely unchanged. The opening provision of Regulation 2320/2002 proclaimed that, "[t]he criminal acts committed in New York and Washington on 11 September 2001 show that terrorism is one of the greatest threats to the ideals of democracy and freedom and the values of peace, which are the very essence of the European Union."[18]

The minimal standards required by the regulation are rooted in the security provisions set forth in Annex 17 of the Convention on International Civil Aviation.[19] The International Civil Aviation Organization (ICAO), a United Nations agency tasked with regulating international air travel, first outlined international aviation standards in the Convention on International Civil Aviation, which was signed by fifty-two nations at the Chicago Convention on December 7, 1944.[20] In March 1974, the ICAO adopted Standards and Recommended Practices for international civil aviation, which were designated as Annex 17 of the Chicago Convention.[21] Although there have been eight sub-

---

[16] Council Regulation 2320/2002, art. 1, 2002 O.J. (L 355) 1, 2 (EC) [hereinafter Regulation 2320/2002], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:355:0001:0021:EN:PDF.

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

[18] Regulation 2320/2002, *supra* note 16, at Preamble.

[19] *See* Regulation 300/2008, *supra* note 17, at Preamble ("It is desirable, in the interests of civil aviation security generally, to provide the basis for a common interpretation of Annex 17 to the Chicago Convention on International Civil Aviation of 7 December 1944.").

[20] *See* Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1207–11, 15 U.N.T.S. 360–72 [hereinafter Chicago Convention], *available at* http://www.icao.int/publications/Documents/7300_orig.pdf. For a more detailed history of the Chicago Convention and the work of the ICAO with respect to aviation security, see generally Paul Stephen Dempsey, *Aviation Security: The Role of Law in the War Against Terrorism*, 41 COLUM. J. TRANSNAT'L L. 649 (2002); *see also* R.I.R. Abeyratne, *Some Recommendations for a New Legal and Regulatory Structure for the Management of the Offense of Unlawful Interference with Civil Aviation*, 25 TRANSP. L.J. 115 (1998).

[21] *Annex 17*, INT'L CIVIL AVIATION ORG., http://www2.icao.int/en/AVSEC/SFP/Pages/Annex17.aspx (last visited Mar. 9, 2012). Annex 17, entitled "Safeguarding International Civil Aviation Against Acts of Unlawful Interference," has been amended several times including shortly after 9/11. Dempsey, *supra* note 20, at 677 n.140, 690.

sequent editions of Annex 17, the original version outlined its fundamental purpose in the preamble, declaring the following:

> the undersigned governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically.[22]

In accordance with this purpose, Regulation 2320/2002 set forth basic tenets to establish secure civil aviation programs. The regulation requires each EU member state to adopt a national civil aviation security program, a quality control program, and a training program.

On the subject of passenger screening, section 4.1 of the Annex to Regulation 2320/2002 describes methods that EU member states must employ in order to satisfy the minimum security standards for air travel. In short, passengers may be screened by hand or by using walk-through metal detection (WTMD) equipment.[23] Passengers must be searched by hand if they trigger the WTMD alarm.[24] Also, continuous random searches must be carried out for passengers who do not trigger the WTMD alarms.[25] The regulation, however, does not require the use of X-ray equipment for passenger screening. Although the regulation provides the purpose and manner in which X-ray equipment should be operated, it only does so in the context of baggage screening.[26] It is also important to note that while section 4.1 allows for screening by hand or WTMD, airports need not provide passengers with a choice of screening method. In other words, airports are not required to screen a passenger by hand if the passenger refuses to be scanned.[27]

There are two provisions that form the basis for EU member states to deploy X-ray equipment specifically for screening passengers. The first such provision can be found in Article 6 of Regulation (EC) 300/2008. Article 6 allows member states to "apply more stringent

---

[22] Chicago Convention, *supra* note 20, at Preamble.

[23] Regulation 2320/2002, *supra* note 16, at 4.1(1) (a)-(b).

[24] *Id.* at 4.1(1)(b).

[25] *Id.*

[26] *Id.* at 4.3 ("Screening of Cabin Baggage"), 5.2 ("Screening of Hold Baggage"), and 13.2 ("Standards and Testing Procedures for X-ray Equipment Applicability").

[27] *See* Olga Mironenko, *Body Scanners Versus Privacy and Data Protection*, 27 COMPUTER L. & SEC. REV. 232, 236 (2011) (noting that UK government does not propose to provide alternative screening method for passengers who decline the security scanning method).

measures than the common basic standards referred to in Article 4."[28] Article 6 clearly gives EU member states a great deal of discretion in employing methods that they feel will best enhance security. The only limitation to this discretion is that in employing such methods, EU member states are required to "act on the basis of a risk assessment and in compliance with Community law. [The] measures shall be relevant, objective, non-discriminatory and proportional to the risk that is being addressed."[29] The regulation does not give further detail on the meaning of relevance, objectivity, nondiscrimination, or proportionality beyond what is provided in Article 6.

The other provision that allows EU member states to justify the use of X-ray technology for screening passengers can be found in Chapter 12.8 of the Annex to Regulation (EC) 185/2010. Chapter 12.8.1 provides that:

> A Member State may allow a method of screening using new technologies other than those laid down in this Regulation, provided that: (a) it is being used for the purpose of evaluating a new method of screening; and (b) it will not negatively affect the overall level of security being attained; and (c) appropriate information that a trial is being conducted shall be given to those affected, including passengers.

Chapter 12.8 is another area in the regulations that provides member states some discretion in their use of security practices because the regulations recognize that screening technologies "will develop over time."[30] However, there are protocols that EU member states must comply with in order to test such technologies. For instance, a member state is required to provide written notification to the European Commission (EC) and member states, four months in advance of the use of any new technologies that are not specifically addressed by the regulations.[31] The EC then has three months to approve the new technology that the member state intends to utilize.[32] If the EC gives a positive reply or fails to respond within that three month period, the member state is authorized to use the technology for an evaluation

---

[28] Regulation 300/2008, *supra* note 17, at art. 6(1).

[29] *Id.*

[30] Commission Regulation 185/2010, Laying Down Detailed Measures for the Implementation of the Common Basic Standards on Aviation Security, Preamble, 2010 O.J (L 55) 1, 4 (EU), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:055:0001:0055:EN:PDF.

[31] *Id.* at 12.8.2.

[32] *Id.* at 12.8.3.

period that cannot exceed eighteen months.[33] However, a twelve-month extension may be granted if the member state provides adequate justification.[34] The EC retains the right to suspend the use of any new technology if it feels that the new screening method fails to provide adequate security.[35] On September 5, 2008, the EC issued a draft regulation to the European Parliament and Council (EP) to develop legislative screening requirements. In response, the Parliament requested that the EC conduct an impact assessment in order to address fundamental rights and health concerns raised by the use of security scanners.[36] In formulating its assessment, the EC was asked to consult the European Data Protection Supervisor, the Article 29 Working Party, and the EU Agency for Fundamental Rights,[37] each of which had expressed reservations in 2009 about the use of security scanners.[38] The EC agreed to conduct the impact assessment and dropped the provisions on security scanners from its legislative proposal, which became Regulation (EC) 272/2009.[39]

The EC issued a report on June 15, 2010, addressing the use of security scanners at EU airports.[40] Many interpret the EC Communication as wholly endorsing the widespread use of security scanners across Europe.[41] While the report seeks to address fundamental rights

---

[33] *Id.* at 12.8.3, 12.8.4.

[34] *Id.* at 12.8.4. Commission Regulation (EU) 185/2010 does not allow evaluation periods to exceed 30 months. *Id.* at 12.8.7.

[35] *Id.* at 12.8.6.

[36] *See* European Parliament Resolution of 23 October 2008 on the Impact of Aviation Security Measures and Body Scanners on Human Rights, Privacy, Personal Dignity and Data Protection. European Parliament, EUR. PARL. DOC. P6 TA(2008)0521 (2008) [hereinafter EP Resolution of 23 October 2008]; Paul De Hert & Rocco Bellanova, *Mobility Should Be Fun. A Consumer (Law) Perspective on Border Check Technology*, 11 SCI. WORLD J. 490, 492 (2011).

[37] *See* EP Resolution of 23 October 2008, *supra* note 37; De Hert & Bellanova, *supra* note 36, at 492.

[38] *See Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU Airports*, at ¶ 31, COM (2010) 311 final (June 15, 2010) [hereinafter *EC Communication*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF.

[39] Commission Regulation 272/2009, 2009 O.J (L 91) 7, 10 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:091:0007:0013:EN:PDF.

[40] *See generally EC Communication*, *supra* note 38; De Hert & Bellanova, *supra* note 36, at 492.

[41] *See Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU Airports,'* 2011 O.J. (C 107) 49, 50 [hereinafter *EESC Opinion*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:107:0049:0052:EN:PDF ("[T]here are doubts as to whether the main objective of the legislative act in question

and health concerns, its primary goal is to steer the EU security scanner policy away from the ad hoc basis it currently operates under and establish a clear legal framework for screening requirements and safeguards.

A. Human Dignity, Privacy, and Data Protection

In the process of standardizing security measures, the European Parliament and Council recognized the need to address human rights in general and civil liberties in particular. Regulations 2320/2002 and 300/2008 clearly observe and support the principles established by the EU Charter of Fundamental Rights (CFR). Nevertheless, questions continue to be raised as to whether the use of security scanners at EU airports violates any provisions of the CFR or the European Convention on Human Rights (ECHR). These instruments deal primarily with health, human dignity, privacy and data protection, and discrimination.

1. *EU Charter of Fundamental Rights*

Those invoking the EU CFR typically reference human dignity (Article 1); respect for private and family life (Article 7); protection of personal data (Article 8); freedom of thought, conscience, and religion (Article 10); nondiscrimination (Article 21); the rights of the child (Article 24); and, ensuring a high level of human health protection in the definition and implementation of all EU policies and activities (Article 35).

Article 1 on human dignity and Article 8 on the protection of personal data have been the primary source of ammunition for critics of security scanners. Article 1 of the CFR declares, "[h]uman dignity is inviolable. It must be respected and protected."[42] Article 8 provides the following:

(the widespread introduction in all EU airports of 'Security Scanners' is the most suitable way to achieve maximum aviation security."). *Cf.* Sarah Ludford, *European Commission is Fence-Sitting on Body Scanners*, GUARDIAN (U.K.) (June 24, 2010), http://www.guardian.co.uk/commentisfree/libertycentral/2010/jun/24/european-commission-fence-sitting-body-scanners ("I was expecting some strong conclusions rooted in a rigorous weighing up of pros, cons and costs. Instead we get a fig leaf of fence-sitting masking a firm intention to legitimize their EU-wide use."). For more on the EESC Opinion, see *infra* notes 86–103 and accompanying text.

[42] Charter of Fundamental Rights of the European Union, art. 1, 2000 O.J. (C 364) 9, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:364:0001:0022:EN:PDF.

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.[43]

Using security scanners at airports has generated a great deal of controversy because the scanner technology allows systems to generate an image of the passenger without clothing.[44] Some critics of security scanners maintain that the technology subjects passengers to "virtual strip searches,"[45] while other commentators dismiss this characterization as ridiculous and point out that there can be no nudity when no skin is featured in the virtual image.[46] Nevertheless, the EC Communication concedes that security scanners have human dignity implications because use of the technology can "reveal a detailed display of the human body (even blurred) . . . and medical conditions, such as prostheses and diapers."[47] Moreover, there are Article 8 data protection[48] concerns over the possibility that security personnel will have the ability to store these sensitive images.

---

[43] *Id.* art. 8, at 10.

[44] *See* BART ELIAS, CONG. RESEARCH SERV., R41502, CHANGES IN AIRPORT PASSENGER SCREENING TECHNOLOGIES AND PROCEDURES: FREQUENTLY ASKED QUESTIONS 5 (2011), *available at* http://www.fas.org/sgp/crs/homesec/R41502.pdf; *see also EC Communication*, *supra* note 38, at ¶¶ 32, 33 ("What are Security Scanners and what can be their role in aviation security.").

[45] *ACLU Backgrounder on Body Scanners and "Virtual Strip Searches,"* ACLU (Jan. 8, 2010), http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches.

[46] *Controlling When You Relieve Yourself, Not Body Scan, Invades Privacy*, DENNIS PRAGER SHOW (Jan. 5, 2010), http://www.dennisprager.com/columns.aspx?g=5bf1740d-cd49-4815-a857-bebbdd9e1a35&url=controlling_when_you_relieve_yourself,_not_body_scan,_invades_privacy.

[47] *EC Communication*, *supra* note 38, at ¶ 50 (discussing "[t] he protection of human dignity."); *see* Mironenko, *supra* note 27, at 236 ("The process reveals a person's gender and the precise construction of his or her body, together any usually concealed physical features that the 'owner' of the body in question may wish to conceal from strangers or even friends and family. Moreover, screening technologies are capable of revealing very sensitive areas of a person's private life, medical aids and conditions, such as prostheses, breast implants, bras with gel pads, diapers, menstrual pads, etc.") (citation omitted).

[48] *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of

In light of these concerns, there are criteria against which the scanning should be assessed. It must be determined (1) whether the measure proposed is appropriate to achieve the objective, (2) whether it goes beyond what is necessary to achieve this objective, and (3) whether there is less intrusive means of achieving the objective.[49] Limited use of security scanners seems to meet the criteria in this case. The purpose of the scanners is to detect prohibited nonmetallic items that could pose a security threat.[50] Critics contend that the method goes beyond what is necessary; however, there are limited ways in which security officials can effectively detect concealed nonmetallic items.[51]

The EC Communication made a number of recommendations to address human dignity, data protection, and other fundamental rights concerns.[52] The recommendations advocate reducing interaction between screener and passenger in order to make the process as anonymous as possible.[53] Reviewers should not be able to see the passenger being screened, link the image to any person in any way, or store the image after the passenger has been cleared.[54] Furthermore, only reviewers of the same gender as the passenger should conduct detailed reviews when necessary.[55] The recommendations also mention the possibility of having mannequin or stick figure representations of the passenger,[56] which seems to be where the technological trend is heading due to the backlash over privacy and human dignity concerns.

There are other technological innovations that may also mitigate privacy concerns. For example, the EC Communication discusses the

---

Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 40 [hereinafter Directive 95/46/EC], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

[49] *See EC Communication*, *supra* note 38, at ¶ 51 (addressing "[d]ata protection.").

[50] *See* ELIAS, *supra* note 44, at 2; *see also How It Works: Advanced Imaging Technology*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/approach/tech/ait/how_it_works.shtm (last visited Jan. 5, 2012) ("Advanced imaging technology safely screens passengers for metallic and nonmetallic threats including weapons, explosives and other objects concealed under layers of clothing without physical contact to help TSA keep the traveling public safe.").

[51] *See* ELIAS, *supra* note 44, at 9–10; Mironenko, *supra* note 27, at 233.

[52] *See EC Communication*, *supra* note 38, at ¶ 2.3 (addressing "[c]oncerns raised in relation to the use of Security Scanners at EU airports").

[53] *See id.* at ¶ 54 (outlining "[p]ossible ways to address the protection of human dignity, data protection and other fundamental rights concerns").

[54] *See id.*

[55] *See id.*

[56] *See id.* at ¶ 53.

use of Automatic Threat Recognition (ATR) software,[57] which can be used to assist screeners in identifying threatening items or carry out interpretation functions automatically.[58] The efficacy of ATR software continues to be tested, but the EC believes that ATR software is ready for a trial in airports.[59]

2. *European Convention on Human Rights (ECHR) of 1950*

Although the EC Communication and the majority of current opinions on security scanners address human dignity, privacy, and health concerns in the context of the EU CFR, it is still important to consider the ECHR. It has a number of provisions[60] that correspond with articles from the CFR. In the context of security scanners, however, Article 8 is of particular importance. The ECHR states that, "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[61] Furthermore, the ECHR provides:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[62]

Interpreting Article 8 of the ECHR, especially in regard to security scanners, is a difficult task. Some scholars conclude that the European Court of Human Rights applies a very broad interpretation of

---

[57] *See id.* at ¶¶ 57, 58 ("ATR is based on specific software, designed to recognise dangerous and forbidden objects.").

[58] *See id.* at ¶57. Screeners are assisted with the identification of threatening objects by "computer algorithms included within the screening protocol [that] allow for automatic identification of threat objects and anomalies instantly, at the time a passenger exits the portal. If an anomaly is identified, a screener is alerted to provide secondary screening." Tim Hudson, *Advanced Passenger Screening Technologies: 'It's Not Just About the Passenger,'* 5 J. AIRPORT MGMT. 114, 121 (2011).

[59] *See EC Communication*, *supra* note 38, at 13.

[60] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 (entered into force Sept. 3, 1953), *available at* http://treaties.un.org/doc/Publication/UNTS/Volume%20213/volume-213-I-2889-English.pdf.

[61] *Id.* at art. 8(1).

[62] *Id.* at art. 8(2).

what Article 8 protects.[63] The concept of private life can extend to a person's body, social status, health, and a number of other personal identifiers. Even if images are prevented from being stored, they are still collected and analyzed for an amount of time that is arguably sufficient to violate a passenger's privacy.[64] Yet these considerations must still be scrutinized under the exceptions provided by Article 8(2).

There have also been objections based on Article 8 of the ECHR because of the limited methods of screening offered to passengers.[65] As noted above, European airports are under no obligation to screen passengers by hand who refuse to partake in the security scanning method. The UK government for instance, does not provide such an alternative.[66]

B. Standards and Effectiveness

The issue of security scanner effectiveness has a direct consequence on determining whether its use violates Article 8 of the EU CFR and Article 8 of the ECHR. As mentioned above, the use of security scanners is not specifically regulated by the EU. However, Article 6 of Regulation (EC) 300/2008 provides the basis for EU member states to apply more stringent security measures, which a number of European nations have done with the introduction of security scanners. Article 6 states that such measures are permissible if

---

[63] *See* Mironenko, *supra* note 27, at 237 (discussing S and Marper v. United Kingdom, 2008 Eur. Ct. H.R. 1581; according to the court, "the concept of 'private life,'" inter alia, "covers the physical and psychological integrity of a person; it can embrace multiple aspects of the person's physical and social identity; elements such as gender identification, name and sexual orientation and sexual life . . . ." *Id.*

[64] *See id.* at 241 (noting that scanners need to save the images for later inspection in the event that a scanner unit fails to detect contraband that is later used in terrorist attack). Although security scanner manufacturers claim that the image storage feature can be turned off at the customer's request, which TSA claims to have done with the scanner units deployed, "these statements contradict the TSA's own Procurement Specs which specifically require that the machines have the ability to record and transmit images, even if those features might be initially turned off on delivery." *Id.; see also* U.S. DEP'T OF HOMELAND SEC., TRANSP. SECURITY, ADMIN., PROCUREMENT SPECIFICATION FOR WHOLE BODY IMAGER DEVICES FOR CHECKPOINT OPERATIONS, FINAL VERSION 1.02 (2008), *available at* http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf.

[65] *See* Mironenko, *supra* note 27, at 236 (noting that the UK government does not offer an alternative method of screening for those who decline the security scanner method).

[66] *See id.*

their use is "relevant, objective, non-discriminatory and proportional to the risk that is being addressed."[67]

Considering the fact that two terrorist attacks provided the primary impetus for using security scanners at airports,[68] the appropriate question is whether security scanners actually could have prevented these attacks. Such an inquiry can help determine whether the use of security scanners is in fact "relevant . . . and proportional to the risk that is being addressed."[69]

It is unclear whether security scanners would have detected the explosives used in either the attempt on al-Asiri or the Christmas Day Bombing by attempted by Abdulmutallab described above.[70] In Abdulmutallab's case, security scanner manufacturers stated that the scanners "would not have detected the underwear bomb because it was in a light powdered form and the detonator was hidden in a body cavity."[71] Of course, the government's continued use of the scanners suggests that they believe that the scanners are a useful tool. Thus, the effectiveness of security scanners in addressing the threat to which they respond remains largely inconclusive. There may be some cases where security scanners are able to detect explosives concealed *on* someone's person, but explosives concealed *in* someone's person remain an entirely different story.[72] Independent researchers have af-

---

[67] Regulation 300/2008, *supra* note 17, at art. 6(1).

[68] *See* Mironenko, *supra* note 27, at 233; *see supra* notes 6–15 and accompanying text.

[69] Regulation 300/2008, *supra* note 17, at art. 6(1).

[70] *See* ELIAS, *supra* note 44, at 4 (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-401T, BETTER USE OF TERRORIST WATCHLIST INFORMATION AND IMPROVEMENTS IN DEPLOYMENT OF PASSENGER CHECKPOINT TECHNOLOGIES COULD FURTHER STRENGTHEN SECURITY (2010)); Gardner, *supra* note 6; Mironenko, *supra* note 27, at 240 (noting that "neither millimeter-wave technology nor backscatters can detect explosives carried inside the body"); Spencer S. Hsu, *GAO Says Airport Body Scanners May not Have Thwarted Christmas Day Bombing*, WASH. POST (Mar. 18, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031700649.html; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-484T, TSA IS INCREASING PROCURMENT AND DEPLOYMENT OF THE ADVANCED IMAGING TECHNOLOGY, BUT CHALLENGES TO THIS EFFORT AND OTHER AREAS OF AVIATION SECURITY REMAIN (2010) ("[I]t remains unclear whether the AIT would have detected the weapon used in the December 2009 incident . . . .").

[71] Mironenko, *supra* note 27, at 240.

[72] *See id.* ("[N]either millimeter-wave technology nor backscatters can detect explosives carried inside the body."); Leon Kaufman & Joseph W. Carlson, *An Evaluation of Airport X-ray Backscatter Units Based on Image Characteristics*, 4 J. TRANSP. SECURITY 73, 73–74 (2011)\ ("The purpose of these is to find contraband hidden under clothing but on the surface of the traveler."). Pelle Neroth, *Technologies to Read the Terrorist Mind*, ENGINEERING & TECH. (Aug. 15, 2011), http://eandt.theiet.org/magazine/2011/08/beyond-body-scanners.cfm. Body scanners

firmed this, stating that "[e]ven if exposure were to be increased significantly, normal anatomy would make a dangerous amount of plastic explosive[s] with tapered edges difficult if not impossible to detect."[73] This fact makes it more difficult to justify the use of security scanners under the relevant and proportional standards adopted by EU law.

C. Health Concerns

The EC urges EU member states to conduct their own risk assessments in determining whether the use of non-ionizing or ionizing radiation is appropriate and justified. The exposure to radiation caused by security scanners creates an obvious health concern. Different security scanner systems use different technologies; thus, these health concerns must be considered on a system-by-system basis.[74] The EU Communication addresses the four primary technologies utilized in security scanners: passive millimeter-wave imaging systems, active millimeter-wave imaging systems, X-ray backscatter, and X-ray transmission imaging.[75]

> (1) The passive millimeter-wave imaging system does not emit any radiation.[76] It measures thermal radiation emitted by the body and the environment. Since this system does not emit any radiation dose, studies have concluded that it does not raise health concerns.[77]
>
> (2) The active millimeter-wave imaging system uses non-ionizing radiation, which is generally considered less harmful than ionizing radiation (used in X-ray systems).[78] While there is some radiation exposure, studies have suggested that the levels are equal

---

have "been criticised for missing the items they are supposed to spot, due to the fact that the rays will not always penetrate thick folds of clothing. Neither can they penetrate skin, thereby missing bomb material that may be hidden inside body cavities." *Id.*

[73] Kaufman & Carlson, *supra* note 72, at 73. According to Kaufman and Carlson, a dangerous amount of PETN packed in a fashion similar to normal antomy could be missed by the scanners yet easily detected on pat down. *See id.* at 93.

[74] *See* Mironenko, *supra* note 27, at 233.

[75] *See EC Communication*, *supra* note 38, at ¶ 35 (discussing the various technologies of security scanners that are commercially available).

[76] *See id.* at ¶ 35(1) (describing "[p]assive millimetre-wave")

[77] *See id.*; *see also id.* at ¶ 61 ("The consulted studies do not raise health concerns when using passive millimetre wave technology.").

[78] *See id.* at ¶ 35(2) (discussing "[a]ctive millimetre-wave"). *Id.* at ¶ 63 ("Non-ionising radiation is generally considered not harmful compared to ionising radiation, such as X-rays.").

to or less than "exposure levels arising from natural and everyday activities (e.g., mobile phones and microwaves)."[79]

3) The X-ray backscatter system[80] uses ionizing radiation and as such, is subject to the dose limits established by Euratom.[81] Although security scanners will expose passengers to ionizing radiation, the dose is low. The EC concluded that it would take approximately forty screenings per day for a passenger to reach the dose limit provided by Euratom.[82]

4) The X-ray transmission imaging system emits a much higher dose than the backscatter system. Therefore, transmission imaging is not intended for systematic screening uses.[83] X-ray transmission screening is generally reserved for police purposes. Due to the aforementioned risks and the availability of non-ionizing or low dose ionizing radiation systems, the transmission imaging system is not used in Europe for aviation security.[84]

On February 16, 2011, the European Economic and Social Committee (EESC) an important and powerful advisory body that represents civil society organizations across Europe, issued a very critical opinion on the 2008 EC Communication to the EP.[85] While the EESC

---

[79] *Id.* at ¶ 65 (citing the centre for Occupational Health and Safety, which measured the intensity of electromagnetic waves at 2 W/m2 (watt per square meter) the leak level for domestic ovens; this value is considerably lower than the 10 W/m2 (50 W/m2) official power density exposure limit).

[80] *See generally* Kaufman & Carlson, *supra* note 72 (discussing efficacy of x-ray backscatter machines for scanning airport passengers); George Zentai, *X-ray Imaging for Homeland Security*, 3 INT'L J. OF SIGNAL & IMAGING SYS. ENGINEERING 13, 14–15 (2010) (discussing use of x-ray technology for luggage and packages).

[81] *See EC Communication*, *supra* note 38, at ¶ 35(3) (discussing X-ray backscatter technology). *Id.* at ¶ 66 (discussing health effects of X-ray backscatter technology); Council Directive 96/29, 1996 O.J. (L 159) 1, 7–9 (Euratom), *available at* http://ec.europa.eu/energy/nuclear/radioprotection/doc/legislation/9629_en.pdf.

[82] *See EC Communication*, *supra* note 38, at ¶ 67.

[83] *See id.* at ¶ 35(4) (discussing "X-ray transmission imaging" technology). *Id.* at ¶ 69 (discussing health effects of X-ray transmission imaging).

[84] *See id.* at ¶ 70.

[85] *See EESC Opinion*, *supra* note 41. According to the EESC website: "The EESC contributes to strengthening the democratic legitimacy and effectiveness of the European Union by enabling civil society organisations from the Member States to express their views at European level. This Committee fulfils three key missions:

- helping to ensure that European policies and legislation tie in better with economic, social and civic circumstances on the ground, by assisting the European Parliament, Council and European Commission, making use of EESC members' experience and representativeness, dialogue and efforts to secure consensus serving the general interest;
- promoting the development of a more participatory European Union which is more in touch with popular opinion, by acting as an institutional forum representing, informing, expressing the views of and securing dialogue with organised civil society;

does not wholly oppose the use of security scanners at EU airports, it stated that, "All in all, there are serious doubts, not as to the legality, but rather the legitimacy of the communication . . . the Commission should have taken far greater care when drawing up such a controversial proposal."[86] The EESC even criticized the EC for using the term "security scanners," as opposed to "body scanners," which was the term previously used by the EP.[87] The EESC claimed that the EC's new terminology constitutes "an attempt to make the communication more politically attractive with a view to its adoption."[88]

Despite its criticisms of the EC Communication, the EESC's reservations primarily concern the extent to and manner in which the EC endorses the use of security scanners. The EESC's objections focus on (1) the lack of alternative screening methods offered to passengers,[89] (2) the legal justifications for exposing passengers to potentially harmful doses of ionizing radiation,[90] (3) concern that the EC has not conducted an adequate proportionality test that weighs the need to adopt the use of security scanners with other relevant factors,[91] and (4) the EC's suggestion that security scanners can replace existing methods of screening like searches by hand and WTMD.[92]

The EESC insisted that legislation be introduced guaranteeing passengers the right to undergo alternative screening methods. It stated that "passengers should be allowed to opt out of such checks and should always maintain the right to fly, regardless of the option they choose."[93] While the EC Communication does not rule out the idea of offering alternative screening methods to passengers, it does not force member states to do so. Thus, the EESC opinion challenges the stance taken by the UK government, which does not require airports to offer passengers alternative methods after they have refused to be scanned. Moreover, the EESC maintains that there should be legisla-

---

- promoting the values on which European integration is founded and advancing, in Europe and across the world, the cause of democracy and participatory democracy, as well as the role of civil society organisations.

About the Committee, EUROPEAN ECON. & SOC. COMM., http://www.eesc.europa.eu/?i=portal.en.about-the-committee (last visited Feb. 20, 2012).

[86] *See EESC Opinion*, *supra* note 41, at 3.8 – 3.8.2.

[87] *Id.* at 3.7.1.

[88] *Id.* at 1.2, 3.7.2.

[89] *Id.* at 3.1.2, 3.6.1.

[90] *Id.* at 3.6.

[91] *Id.* at 3.1.2.

[92] *Id.* at 3.7 – 3.7.6.

[93] *Id.* at 1.2.

tion preventing airports from subjecting passengers to undue delays after they have refused scanning.[94]

On the subject of health, the EESC urged the EC to provide conclusive studies on the health risks associated with the use of security scanners.[95] As noted above, EU member states are bound by the Euratom Treaty, which sets radiation dose exposure limits on an ad hoc basis. Before exposing passengers to radiation, the appropriate authorities must provide a legitimate justification and demonstrate that there are sufficient protective measures in place to ensure the lowest possible levels of exposure.

The EESC opinion also noted that point 34 of the EC Communication suggests that scanners may replace existing methods of security screening, which the EESC argues is too narrow of an approach at a time when there are so many uncertainties as to the legality, technology, health risks, and effectiveness of security scanners.[96] The EESC therefore concluded, that, rather than try to expedite the use of security scanners in as many EU airports as possible, "it would be more logical, given the fast-developing market, to wait for other technology that is more advanced, less intrusive and more in line with the objective to be achieved—namely, aviation security."[97]

The EESC urged the EC to establish a clear legal framework for including security scanners in the acceptable methods of screening. In doing so, the EC must satisfy the standards provided by EU law. According to the EESC, the EC Communication "does not appear to comply fully with the criteria of necessity, proportionality, and legality that must be displayed by any measure adopted by the public authorities."[98] As to the principle of necessity, the EESC considers the link between the scanners and higher levels of security to be "tenuous."[99] Regarding proportionality, the EESC urged the EC to weigh "the need for its adoption with other factors, such as the potential costs of setting up such security scanners."[100] Finally, in terms of legality, the EESC demanded that the EC address the concerns raised in regard to the CFR and the ECHR in a manner that creates a sense of clarity.[101] The EESC noted that the "rights and freedoms most affected are almost exclusively those forming what the European Court of

---

[94] *Id.*
[95] *Id.* at 1.3, 3.5.
[96] *Id.* at 3.7.3 – 3.7.6.
[97] *Id.* at 3.1.2.
[98] *Id.* at 3.2.
[99] *Id.* at 3.2.1.
[100] *Id.* at 3.1.2.
[101] *Id.* at 1.2, 3.3.3

Human Rights considers the untouchable hard core of public policy established by the European Convention of Human Rights."[102] Therefore, procedural safeguards must be put in place that protect the individual rights of passengers, most notably in terms of human dignity, data protection, and health.

On July 6, 2011, the European Parliament (EP) adopted a nonbinding resolution on the use of security scanners at airports in EU member states.[103] In many ways, the EP resolution mirrors the suggestions made in the EESC opinion. The EP called on the EC to add security scanners to the list of authorized screening methods, under the condition that such authorization will be accompanied by minimum standards and procedural safeguards.[104] For instance, the EC must demonstrate that the use of security scanners will not "constitute a risk to passenger health, personal data, the individual dignity and privacy of passengers."[105] The EP recognizes that the majority of member states acknowledge that security scanners can contribute greatly to the goal of enhancing aviation security, particularly when it comes to nonmetallic and liquid explosives. However, like the EESC opinion, the EP insisted that passengers should be able to opt out of the scanning process and participate in an alternative method.[106] Furthermore, passengers who refuse to be scanned should not be looked upon with a greater level of suspicion than those who submit to the scanning process.[107]

In regard to health and privacy, the EP expressed confidence that technology can help alleviate these concerns.[108] Nevertheless, it made clear that security scanners equipped with technology that uses ionizing radiation must be excluded from the list of acceptable screening methods.[109] This would essentially preclude the use of X-ray backscatter and transmission imaging systems. The EP Resolution also encouraged member states to continue testing the long-term ef-

---

[102] *Id.* at 3.3.3.

[103] European Parliament Resolution of 6 July 2011 on Aviation Security, with a Special Focus on Security Scanners, EUR. PARL. DOC. P7_TA-PROV(2011)0329 (2011) [hereinafter EP Resolution of 6 July 2011], *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-0329.

[104] *Id.* at ¶ 9.

[105] *Id.*

[106] *Id.* at ¶ 20.

[107] *Id.*

[108] *Id.* at ¶¶ 22, 24.

[109] *Id.* at ¶ 23.

fects of radiation exposure while trying to develop scanning systems that have no harmful side effects.[110]

This EP Resolution embodies a more positive view on the ability of technology to alleviate privacy concerns. It explicitly stated that member states must ensure a random selection process for scanning passengers, body images must be limited to stick figures, data may only be used for the amount of time it takes to detect threatening items, and the data must be destroyed immediately after the passenger has passed through the screening checkpoint.[111] In order to provide further assurances for these safeguards, security scanner use must remain consistent with Directive 95/46/EC[112] on data protection.[113] In addition, the EP member states should take steps to provide comprehensive information to passengers regarding the use of security scanners.[114] Lastly, the EP affirmed its commitment to end the ban on liquids in 2013, which should prompt member states to develop technology to address the carrying of liquids in order to ensure that the end of the ban does not compromise security.[115]

The EP resolution provides insight into the future use of security scanners at European airports. Notwithstanding provisions on human dignity, health, data protection and privacy rights, the EP still recommended that the EC add security scanners to the list of authorized screening methods. Taking this into consideration, it appears safe to say that security scanners will not be phased out at European airports anytime soon. In all likelihood, the use of security scanners will increase as the technology improves and helps alleviate human rights concerns.

II. THE UNITED STATES

Shortly after 9/11, the United States took a number of steps to reorganize executive agencies tasked with protecting the American pub-

---

[110] *Id.* at ¶ 25.

[111] *Id.* at ¶¶ 27 – 29, 31 – 32.

[112] *See* Directive 95/46/EC, *supra* note 48, at 38. Directive 95/46/EC, commonly referred to as the Data Protection Directive, provides a regulatory framework for protecting personal information across all EU countries. *Id.* Article 29 of the Directive established the "Article 29 Working Party," an independent advisory entity with representatives from each EU country tasked with examining questions and providing opinions regarding data protection and privacy. *See id.*, art. 29, 30 at 48; Mironenko, *supra* note 27, at 234 n.14; *Article 29 Working Party*, EUR. COMM'N DIRECTORATE-GEN'L FOR JUST., http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Jan. 6, 2012).

[113] EP Resolution of 6 July 2011, *supra* note 103, at ¶ 33.

[114] *Id.* at ¶¶ 35 – 36.

[115] *Id.* at ¶¶ 42 – 44.

lic from the threat of terrorism. The Aviation and Transportation Security Act of 2001 created the Transportation Security Administration (TSA). Originally part of the Department of Transportation, the TSA was later placed under the Department of Homeland Security (DHS), a cabinet level department with a staff of more than 240,000 employees.[116]

A. TSA and Whole Body Imaging/Advanced Imaging Technology

In 2007, the TSA began deploying what are commonly referred to in the United States as Whole Body Imaging (WBI) or Advanced Imaging Technology (AIT) systems in airports across the United States.[117] In a recent comment regarding this deployment, TSA administrator John Pistole said, "'[t]he terrorists keep adapting and evolving to try to defeat our security.'"[118] These systems add an additional layer of security to address such threats. There are currently 488 WBI systems in use at seventy-eight U.S. airports. In September 2011 the TSA purchased 300 more millimeter-wave units and plans to implement WBI at an additional twenty-nine airports.[119] The TSA uses both the millimeter-wave and X-ray backscatter systems,[120] but it does not require passengers to submit to WBI screening.[121] Passengers who refuse to be scanned can receive alternative screening methods, such as a pat-down search. Also, the TSA claims that images

---

[116] *About DHS*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/about-dhs (last visited Aug. 20, 2012); *Our History*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/research/tribute/history.shtm (last visited Aug. 20, 2012).

[117] *See Advanced Imaging Techonology: Innovation & Technology*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/approach/tech/ait/index.shtm (last visited Jan. 6, 2012).

[118] Ross Wilkers, *TSA Boss: Patdowns, Scanners Work*, EXECUTIVEGOV.COM (Aug. 11, 2011), http://www.executivegov.com/2011/08/tsa-boss-patdowns-scanners-work/.

[119] For a list of U.S. airports that currently have imaging technology systems, see *Advanced Imaging Techonology: Frequently Asked Questions*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/approach/tech/ait/faqs.shtm (last visited Jan. 6, 2012). *See also* Press Release, Transp. Sec. Admin, TSA Announces Advanced Imaging Technology Deployments at U.S. Airports (Oct. 6, 2011), http://www.tsa.gov/press/releases/2011/1006.shtm.

[120] *See Frequently Asked Questions: Advanced Imaging Techonology*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/approach/tech/ait/faqs.shtm (last visited Jan. 6, 2012).

[121] *See id.* ("[I]maging technology screening is optional for all passengers."). *See also* ELIAS, *supra* note 45, at 1 ("If an individual considers this screening method too invasive or revealing or prefers not to undergo AIT imaging for any other reason, TSA provides the option of submitting to a pat-down search instead.").

from WBI systems cannot be stored, printed, or transmitted and are immediately deleted after the passenger has passed through the security checkpoint.[122]

There are obvious differences between the legal approaches taken by the United States and Europe. For instance, EU members have the added burden of trying to institute uniform procedures and regulations for a number of member states. In contrast, the United States is principally bound by internal laws, namely the Aviation and Transportation Security Act, and above all, by the Fourth Amendment.

Just as in Europe, there are many critics of WBI in the United States, and many air travelers believe that the use of WBI is an invasion of privacy.[123] There have been a number of publicized cases where passengers and airline staff have been denied clearance at security checkpoints after refusing to submit to scanning and the alternative pat-down search. For example, on October 15, 2010, a pilot named Michael Roberts was prevented from passing through a security checkpoint at Memphis International Airport.[124] Although Roberts had passed through a WTMD without triggering the alarm, a TSA official informed him that he had to remove his shoes for WBI scanning.[125] Roberts refused the scanning and the official told him that as an opt-out, he would have to submit to a pat-down search or else he would not be allowed to pass through the checkpoint.[126] Roberts again refused and was not allowed to pass through the checkpoint. The Rutherford Institute, a civil liberties organization that provides free legal services to individuals involved in constitutional disputes, has agreed to represent Roberts in making the case that WBI scanning constitutes a violation of the Fourth Amendment.[127] Less than a

---

[122] *See Advanced Imaging Techonology: Privacy*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/approach/tech/ait/privacy.shtm (last visited Jan. 6, 2012) ("Advanced imaging technology cannot store, print, transmit or save the image, and the image is automatically deleted from the system after it is cleared by the remotely located security officer."). *Cf.* Mironenko, *supra* note 27, at 241 (positing that images would need to be retained in the event screeners find a real terrorist or in the aftermath of a successful attack to see what went wrong).

[123] *See* Agyemang Frimpong, *Introduction of Full Body Image Scanners at the Airports: A Delicate Balance of Protecting Privacy and Ensuring National Security*, 4 J. TRANSP. SECURITY 221, 223–25 (2011).

[124] *See* Roberts v. Napolitano, 798 F. Supp. 2d 7, 9 (D.D.C. 2011); *see also The Rutherford Institute Agrees to Represent Michael Roberts, Airline Pilot Who Refused to Submit to Virtual Strip Search*, RUTHERFORD INST. (Oct. 21, 2010), https://www.rutherford.org/publications_resources/press_release_channel/The_Rutherford_Institute_Agrees_to_Represent_Michael_Roberts_Airline_Pilot/.

[125] *Id.*

[126] *Id.*

[127] *Id.*

month later, on November 13, 2010, a passenger named John Tyner was prevented from passing through a security checkpoint at the San Diego Airport after he refused to submit to WBI scanning and the pat-down search.[128] There are a number of similarly publicized cases and there are bound to be many more given the intention of the TSA to increase the use of WBI scanning.[129]

There have also been a number of legal and administrative disputes between TSA/DHS and the Electronic Privacy Information Center (EPIC). In 2010, EPIC filed two requests to DHS under the Freedom of Information Act (FOIA).[130] EPIC requested almost every

---

[128] *See* Mironenko, *supra* note 27, at 233; Catherine Saillant, *Traveler Who Resisted TSA Pat-down is Glad His Moment of Fame is Nearly Over*, L.A. TIMES (Nov. 19, 2010), http://articles.latimes.com/2010/nov/19/local/la-me-screening-tyner-20101119.

[129] In *Durso v. Napolitano*, 795 F. Supp. 2d 63, 65 (D.D.C. 2011), a complaint filed on behalf of three airline passengers alleged screening methods violated their rights under the Fourth Amendment. Durso, a recent breast cancer survivor who had undergone a mastectomy, alleged that TSA officials had inappropriately groped her. *Id.* Daniels, another of the complainants and a frequent business traveler, alleged to have been aggressively groped in his genital area when undergoing an enhanced pat-down search. *Id.* The third complainant, C.N., a twelve-year-old girl, was subjected to an AIT scan without the consent of her guardians. *Id.* at 65–66. The complaint was dismissed by the U.S. District Court for the District of Columbia for lack of jurisdiction. *Id.* at 73. Represented by The Rutherford Institute, the plaintiffs along with pilot Roberts, filed a consolidated appeal in the D.C. Circuit. *See supra* notes 124–27 and accompanying text. *See also Rutherford Institute Appeals Dismissal of Airline Passenger, Pilot Lawsuit Against DHS & TSA Over Scanners, Virtual Strip Searches & Full-Body 'Rub-Downs'*, RUTHERFORD INST. (Jan. 3, 2012), https://www.rutherford.org/publications_resources/on_the_front_lines/rutherford_institute_appeals_dismissal_of_airline_passenger_pilot_lawsuit_a. In *Tobey v. Napolitano*, No. 3:11CV154-HEH, 2011 WL 3841929, at *1-2 (E.D. Va. Aug. 30, 2011), prior to entering the AIT scanner unit, plaintiff removed his shirt revealing the text of the Fourth Amendment, which he had written on his chest with a marker. Plaintiff was subsequently arrested by the police at Richmond International Airport and later filed suit alleging that defendants violated his rights under the First, Fourth, Fifth, and Fourteenth Amendments. *Id.* at *3. The Court granted defendants' motion to dismiss all counts against TSA and DHS officials on the basis that plaintiff had failed to state a claim with sufficient specificity. *See id.* at *18. Finally, in *Redfern v. Napolitano*, No. 10-12048-DJC, 2011 WL 1750445, at *2 (D. Mass. 2011), plaintiff brought Fourth Amendment suit against TSA and DHS officials after being selected for AIT scanning on six different occasions, three of which he chose to opt out and was subjected to the enhanced pat-down. The complaint was dismissed for lack of jurisdiction. *See id.*, at *8.

[130] *See* Letter from Ginger P. McCall, Staff Counsel, Elec. Privacy Info. Ctr. (EPIC) to Mary Ellen Callahan, Chief Privacy Officer/Chief FOIA Officer, U.S. Dep't of Homeland Sec., RE: Freedom of Information Act Request and Request for Expedited Processing (July 13, 2010), *available at* http://epic.org/privacy/backscatter/Body_Scanner_Radiation_FOIA.pdf; *see also* Letter from Ginger P. McCall, Staff Counsel, Elec. Privacy Info. Ctr. (EPIC) to Kim-

piece of information regarding WBI scanning that DHS had in its possession.[131] DHS released a large volume of documentation in response, but withheld a number of images and several hundred pages of training manuals claiming that they were exempt from FOIA because they were internal materials and could constitute a threat to transportation security if released.[132] In response, EPIC filed lawsuits in November 2009 and January 2010, seeking the release of the information that DHS withheld.[133] After both parties filed motions for summary judgment, the District Court sided with DHS and allowed the documents to be withheld.[134] On April 21, 2010, EPIC and thirty other organizations issued a petition to the TSA urging it to stop the use of WBI scanning.[135] EPIC continues to argue that WBI scanning constitutes a violation of the Administrative Procedures Act, the Privacy Act, the Religious Freedom Restoration Act, and the Fourth Amendment.[136]

On April 22, 2009, the U.S. House of Representatives passed the "Aircraft Passenger Whole-Body Limitations Act of 2009," which prevents the use of WBI as a primary screening method.[137] Similar to the EESC, Congress was worried that the TSA might begin to rely too heavily on WBI and use it as a primary method in lieu of pat-down searches and WTMD.[138] In fact, a bill introduced in the Senate in 2010 attempted to do just that.[139] The Securing Aircraft From Explo-

---

berly Walton, Special Counselor, Transp. Sec. Admin., RE: Freedom of Information Act Appeal on TSA10-0674 (Aug. 27, 2010), *available at* http://epic.org/privacy/body_scanners/Body_Scan_Rad_Appeal.pdf.

[131] Letter from Ginger P. McCall to Mary Ellen Callahan, *supra* note 130.

[132] For documentation released by the DHS, see generally *Epic v. Department of Homeland Security – Body Scanners – Freedom of Information Act Documents*, EPIC.ORG, http://epic.org/privacy/airtravel/backscatter/epic_v_dhs.html#foia (last visited Mar. 11, 2012).

[133] Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 760 F. Supp. 2d 4, 9 (D.D.C. 2011).

[134] *Id.* at 14; *see also* Mironenko, *supra* note 27, at 234.

[135] *See* Petition from Electronic Privacy Information Center et al. to Janet Napolitano, Sec'y, Dep't of Homeland Sec. & Mary Ellen Callahan, Chief Privacy Officer, Dep't of Homeland Sec. (Apr. 21, 2010) *available at* http://epic.org/privacy/airtravel/backscatter/petition_042110.pdf.

[136] *See id.*; Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 5–11 (D.C. Cir. 2011).

[137] *See* H.R. 2027, 111th Cong. §§ 1–2 (2009).

[138] *See id.* at § 2 ("Whole-body imaging technology may not be used as the sole or primary method of screening a passenger under this section. Whole-body imaging technology may not be used to screen a passenger under this section unless another method of screening, such as metal detection, demonstrates cause for preventing such passenger from boarding an aircraft.").

[139] Securing Aircraft from Explosives Responsibly: Advanced Imaging Recognition Act of 2010 (SAFER AIR Act), S. 3536 111th Cong. § 4.

sives Responsibly: Advanced Imaging Recognition Act (SAFER AIR Act) would have mandated the deployment of WBI to airports across the country as the primary method of screening for the next two years.[140] The bill, however, failed to gain traction and died at the committee level.[141] Nevertheless, given the recent trend towards WBI systems combined with the TSA initiative to increase the deployment of WBI, more legislation will likely be introduced in Congress seeking to make WBI systems the primary method of screening.

B. The Fourth Amendment

While European human rights protections against invasions of privacy rest on the principles of relevance, objectivity, nondiscrimination, and proportionality, privacy protections in the United States rest primarily on the Fourth Amendment prohibition of unreasonable searches. The Fourth Amendment to the Constitution provides:

> 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.[142]

In order to trigger the protections of the Fourth Amendment, it first must be determined that the actions of the government or administrative agency amounted to a search or seizure. Once it has been determined that a search was conducted, the inquiry then turns on whether the search was reasonable.

The special needs doctrine constitutes an exception to the Warrant Clause requirement of standard Fourth Amendment searches.[143] The special needs doctrine acknowledges that in some circumstances, including administrative stops or inspections (e.g. systematic screenings required for transportation security), the probable cause standard un-

---

[140] *Id.* at § 3 ("It is the policy of the United States to aggressively seek, develop, and deploy, in a timely fashion and in sufficient numbers, primary screening technologies capable of detecting and protecting against threats to domestic and international aviation travel that cannot be effectively and efficiently detected by other technologies currently more commonly utilized in airports, such as metal detection.").

[141] *See* Bill Summary & Status, 111th Congress (2009-2010), S.3536, LIBR. OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.03536 (last visited Jan. 5, 2012).

[142] U.S. CONST. amend. IV.

[143] *See* Ferguson v. City of Charleston, 532 U.S. 67 (2001).

der the Warrant Clause becomes impracticable.[144] The justification for administrative stops and inspections remains a subject of debate.[145] While some legal scholars maintain that "inspections do not amount to a 'search' for Fourth Amendment purposes," others reason that "passengers 'consent' to the search when they purchase their tickets."[146] Courts typically assess reasonableness on either an ad hoc basis or by applying a balancing test.[147] That is, the individual's Fourth Amendment privacy rights are balanced against the societal interests at stake, which in this case include aviation security.

The balancing test largely parallels the relevance and proportionality tests applied by the EU in interpreting the CFR. Therefore, while there are differences in terms of art, the main differences between the U nitedStates and European approaches relate to administrative, procedural, and legitimacy issues related to the propriety of using systems that may impact upon privacy. The United States is bound by a number of Federal Acts, but principally by the Constitution. Conversely, the EU consists of a collection of nations, which do not always see eye-to-eye on matters that have profound security and legal implications. EU human rights laws on the use of security scanners consist of a variety of charters, conventions, resolutions, and regulations that are interpreted differently and are given different weight by a number of committees, organizations, and agencies.

C. TSA Solutions

TSA has taken steps to protect the rights of passengers while using enhanced security measures. Although TSA continues to use WBI systems with ionizing radiation doses (which the EP resolution forbids), some of the changes being made are consistent with the requests in the EP resolution. For instance, TSA announced that it will begin installing ATR software on all the millimeter-wave systems in use and begin testing similar software for X-ray backscatter systems.[148] This

---

[144] *See* M. Madison Taylor, *Bending Broken Rules: The Fourth Amendment Implication of Full-Body Scanners in Preflight Screening*, 52 RICH. J.L. & TECH. 1, 22–25 (2010); Stuart A. Hindman, *Full-Body Scanners: TSA's New "Optional" System for Airport Searches*, 10 ISSUES AVIATION L. & POL'Y 337, 342–43 (2011).

[145] MARC L. MILLER & RONALD F. WRIGHT, CRIMINAL PROCEDURES: THE POLICE: CASES, STATUTES AND EXECUTIVE MATERIALS 108 (4th ed., 2011) (citing United States v. Hartwell, 296 F. Supp. 2d. 596, 602 (E.D. Pa. 2003), noting, "'no consensus has been reached as to the grounds justifying' an airport search").

[146] *Id.*

[147] *See* Taylor, *supra* note 144, at 25, 27.

[148] Press Release, Transp. Sec. Admin, TSA Takes Next Steps to Further Enhance Passenger Privacy (July 20, 2011), http://www.tsa.gov/press/releases/2011/0720.shtm.

will eliminate "passenger-specific images" and replace them with the "stick figure" like images requested by the EP.[149] Due to this change, the screen will no longer have to be hidden from the passenger and the reviewing TSA officer will not have to be in a remote viewing room.[150] It seems clear that policymakers and airport authorities in the United States and Europe feel confident that technology can eliminate, or at least sufficiently mitigate, the legal concerns over the use of WBI technology for airport screening.

CONCLUSION

This essay explains the type of plots for which security scanners were implemented. It describes the history of al-Qaeda's attempts to use hidden explosives in attacks on government officials and civil aviation. The piece explains how the European Union and the United States implemented measures aimed at protecting privacy, dignity, and individual liberty while balancing those values against the interest in protecting civil aviation from terrorist plots.

The discussion suggests the following conclusions. First, the security scanners and similar systems can, with advancements in technology, become more protective of privacy interests. Specifically, as technology advances, some systems will also be developed which will allow the government to maximize its interest in security while also maximizing the citizenry's interest in remaining free from excessive governmental intrusions into their private lives. Second, there are obvious differences between the legal approaches taken by the United States and European nations (such as the fact that the EU has the added burden of trying to institute uniform procedures and regulations for a number of member states). Despite these differences, both the EU and the United States have implemented similar air travel procedures to protecting passenger's privacy rights. Policymakers and airport authorities in the United States and Europe have proven that technology can eliminate, or at least sufficiently mitigate, the legal concerns over the use of WBI technology for airport screening.

---

[149] *Id.*
[150] *Id.*