Body scanners vs. privacy and data protection

Olga Mironenko

[Paper to be published in *Computer Law & Security Review*, 2011, vol. 27, issue 2; not to be cited without permission of the author]

Abstract: In recent history, the world has experienced dramatic events which have had a substantial effect on the balance between human rights protection and security measures. Body scanners installed at airports are intended to protect our lives. But at the same time they have a serious impact on privacy and data protection. The international legislation allows limiting people's rights and freedoms, but only if it is in accordance with the law and is proportionate and necessary for national security, public safety and for the protection of the rights and freedoms of others. Do body scanners respect these principles? The article examines the current situation, its background and future prospects. It discusses and analyzes the key terms and legal instruments, problems, disputes and proposed "safeguards". The work concludes by pointing out the unlawfulness of current regimes and sets forth perspective on the possible solutions.

Keywords: privacy, data protection, body scanner, security scanner, scanning technology, advanced imaging technology, security, aviation, civil aviation, air passenger, international law, personal data

1. Introduction

Installation of body scanners at the airports under the motto of combating terrorism continues to raise serious fundamental rights and health concerns. Of course everybody wants to travel safely and it is believed that effective security must be ensured in the civil aviation sector. Full body scanners may be one of the technical solutions required to keep a high level of security. Ultimately they are intended to protect our lives. But at the same time the use of scanners has a serious impact on passengers' rights, such as the right to privacy and data protection, as well as other fundamental rights. As a result, a conflict arises between the use of such machines and the protection of these rights. The principal objective of this article is to examine the legal problems, issues and disputes deriving from this conflict and to set forth the author's perspective on how the problems could be resolved. This article will focus on the privacy and data protection rights, mentioning other values where necessary. It will analyze the applicable international instruments, citing the EU regulations as the principal sources. The USA, the UK and some other countries' regimes will be discussed as examples where applicable.

2. Current situation

The International Civil Aviation Organization (ICAO), a specialized agency of the United Nations charged with coordinating and regulating international air travel, sets out the basis for aviation security.[1] At present it does not give any guidance on the body scanning technology and does not require member states to implement them. The usage or non-usage of the devices is based on the decision of a particular state, and there is no common definition of a "body scanner". Various terms are in use, such as "security scanner", "whole-body scanning", "advanced imaging technology". The machines are also often derisively referred to as "naked scanners" or "digital strip searchers".

Several forms of radiation differing in wavelength and energy emitted are used in order to identify hidden objects worn on the body or in the clothing of the screened person. The first body scanner was created by Dr. Steven W Smith in the USA in 1992. It was an ultra-low-dose Secure 1000

[1] Chicago Convention (1944), Annex 17 – Security (1974). ICAO also adopts the Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Doc 8973 (restricted) and Standards and Recommended Practices (SARPs).

backscatter X-ray scanner. Several technologies have been developed since then, including those based on natural thermal radiation (heat from the body), but the most commonly deployed security scanners use two competing technologies: backscatter[2] and active millimeter wave imaging technology.[3] Another method, X-ray transmission imaging technology, which can produce images like a medical X-ray, is not currently used because of high radiation doses. In addition, there are several emerging technologies which are either still under development or have not been thoroughly tested.

The attack on 11 September 2001 in the USA and other acts of terrorism such as the train bombings in Madrid in 2004 and car bombings in Glasgow and London in 2007 had resulted in the adoption of new anti-terrorist security measures throughout the world, including state-of-the-art imaging technologies. The first airport in the world to implement body scanners was the Schiphol in the Netherlands in 2007.

After 25 December 2009, when the so-called "underwear bomber" Umar Farouk Abdulmutallab attempted to detonate plastic explosives hidden in his underwear on Flight 253 from Amsterdam to Detroit, many other states became concerned with installation of the devices as well. The list of airports currently deploying scanners is constantly growing and includes airports in the USA, Canada, the UK, Russia, etc.[4] These governments claim that the use of the machines is justified and necessary in order to heighten security measures at airports and better protect the traveling public. The machines are considered to be more effective than walk-through metal detectors as they are capable of identifying both metallic and non-metallic objects, including plastic and liquid items. They are supposed to improve passenger flow by performing screening at a very acceptable speed. Such an enhanced detection performance might also be achieved by a full physical hand search (so-called "pat-down") or strip-search, but the use of scanners are thought to be quicker and less invasive.

The privacy issues around body scanners arose as soon as the first machines appeared. But while privacy advocates, data protection authorities and different parliaments believe that the use of scanners violates passengers' rights to privacy and dignity, the vast majority of representatives of the aviation and security authorities and organizations, industry, airports, operators, etc., are mainly concerned about the security issues and seem not to be fully aware of the actual problem: What is the issue relating to privacy? Is there any problem at all? Body scanners are effective and less intrusive than hand or strip-searches, so why worry about other issues?

2.1. USA

According to a bill introduced in the US Senate in 2010 entitled Securing Aircraft From Explosives Responsibly: Advanced Imaging Recognition Act (S.A.F.E.R. A.I.R. Act), advanced imaging technology means a device that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body as applicable, including narcotics, explosives and other weapons components.

The Transportation Security Administration (TSA) began deploying advanced imaging technology in 2007. According to the official TSA's web-site, there are currently 486 imaging technology units at 78 airports.[5] By 2014 the USA plans to deploy 1800 scanners in order to gradually introduce them as a primary screening method, that is, as a method for initial examination of travelers using the scanner device rather than a metal detector.

---

[2] Backscatter (low X-ray) technology is based on the X-ray compton scattering effect. It detects the radiation reflected from the object to form a 2D image. Images are taken from both sides of the human body. This technology is used in the USA and in the UK.

[3] In this technology, clothing and other organic materials are translucent in extremely high frequency (millimeter wave) radio frequency bands. The millimeter wave is transmitted simultaneously from two antennas rotating around the body. The wave energy reflected back from the body or other objects on the body is used to construct a three-dimensional image. This technology is used in the USA; is being tested in the Netherlands, France and Germany.

[4] A list of airports with body scanners can be found at http://www.bigbrotherwatch.org.uk/home/2010/06/airports-with-body-scanners.html (last visited 30.11.2010).

[5] TSA: *Advanced Imaging Technology*, http://www.tsa.gov/approach/tech/ait/index.shtm (last visited 13.01.2011).

But on 22 April 2009 the US House of Representatives passed legislation to prevent the use of body scanners as primary screening devices ("Aircraft Passenger Whole-Body Limitations Act of 2009"). In a petition dated 21 April 2010, the Electronic Privacy Information Centre (EPIC) and 30 other organizations urged the TSA to suspend the body scanner program due to constitutional, statutory, health, and effectiveness concerns. EPIC argued that the TSA had violated the Administrative Procedures Act, the Privacy Act, the Religious Freedom Restoration Act, and the Fourth Amendment.

The TSA strongly supports the use of scans. In a response dated 28 May 2010, the TSA claimed that the machines are safe, effective, and neither violate existing statutes nor impermissibly infringe on Americans' constitutional rights. On its official website the TSA states that in the course of testing, 99 percent of the US passengers chose this technology over alternative screening procedures, and that independent pollings indicate that the public generally supports the use of scanners.

At the same time, opinions of opponents receive wide coverage in the press and on the Internet as well. For example, the incident at San Diego Airport on 13 November 2010 received much public attention worldwide, when an American citizen, John Tyner, refused to go through both scanners and pat-down, facing a lawsuit and a potential fine of USD 10 000 for violation of airport security regulations.

In 2009, EPIC filed two requests to the US Department of Homeland Security (DHS)[6] under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, seeking information pertaining to the TSA body scanner program. On 14 April 2009, EPIC requested all documents concerning (i) the capability of passenger imaging technology to obscure, degrade, store, transmit, reproduce, retain, or delete images of individuals, (ii) all related contracts, and (iii) all related instructions, policies, and/or procedures. On 2 July 2009, EPIC requested all images captured by body scanning technology held by the TSA, all complains related to scans, etc. As a result of these lawsuits, the DHS released some responsive documents (procurement specifications, operational requirements, traveler complaints, and several vendor contracts), that were subsequently made available to the public. But DHS withheld more than 2000 images as well as full 376 pages of security training material, arguing that these documents were exempt from disclosure under FOIA because they were predominately internal materials, and that any further release would constitute a threat of transportation security.

EPIC commenced a first lawsuit on 5 November 2009 and a second lawsuit on 13 January 2010 with regard to its two requests respectively. DHS filed a motion for summary judgment, asserting that it had produced all of the information that FOIA requires. EPIC then filed a cross-motion for summary judgment challenging DHS's refusal.

On 12 January 2011, the US district court for the district of Columbia granted DHS's motion for summary judgment and denied EPIC's cross-motion for summary judgment.[7] According to the Court, the withheld images relate to the rules and practices of TSA because their disclosure would reveal TSA's detection standards. Thus they fall within FOIA's exemption high (b)(2)[8] and need not be released. The Court stated that there was no basis to question TSA's conclusion that the disclosure of the images may constitute a threat of transportation security. According to EPIC's press release, EPIC may appeal the district court's decision.[9]

Nevertheless, the S.A.F.E.R. A.I.R. Act mandates the deployment of body scanners. If it passes, the new statute will make scanners the primary screening technology by 2013. It states as follows: "It is the policy of the US to aggressively seek, develop, and deploy, in a timely fashion and 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." There are several locations already where the scanners are used for primary screening, for example, Miami International Airport.

[6] TSA is a department of DHS.

[7] Case No. 1:09-cv-02084 (RMU), EPIC v. DHS.

[8] FOIA's exemption high (b)(2) applies to information "prescribing the methods and strategy to be followed by the law enforcement agents in the performance of their duties".

[9] EPIC. http://epic.org/2011/01/court-grants-government-motion.html (last visited 13.01.2011).

2.2. The European Union

In the European Union (EU), the term "security scanner" is used, a generic term used for a technology that is capable of detecting objects carried under clothes.[10]

The EU adopted its first common rules in the field of civil aviation security in 2002.[11] But the use of body scanners is not currently regulated at the EU level. In accordance with the existing EU law, member states may introduce the use of the scanners at their airports either by exercising their right to apply security measures that are more stringent than existing EU requirements[12] or by exercising their right to conduct trials of new technical processes or methods for a maximum period of 30 months.[13] In this case, the member state decides if and under what conditions to use scanners.

On 5 September 2008 the European Commission (Commission) proposed to the Council and the European Parliament (EP) a draft regulation including basic screening requirements to be further developed in legislation. But in Resolution (2008)0521 of 23 October 2008 (Resolution) the EP requested the Commission to carry out an impact assessment relating to fundamental rights and health, to consult the European Data Protection Supervisor, the Article 29 Working Party[14] and the EU Agency for Fundamental Rights, and to provide economic, commercial and cost-benefit impact assessment.

As a response, in June 2010 (much later than the expiry date of the proposed three-month deadline), the Commission adopted a technical and factual report which assesses the current situation with regard to the use of security scanning technology in terms of detection capacity, and compliance with fundamental rights and health protection regulations (Commission's Report).[15]

The Commission's view is that where member states decide to authorize security scanners, a common EU-wide framework would be the best way to legally guarantee the uniform application of security rules at all airports and provide strict and mandatory safeguards to ensure compliance with European guarantees of fundamental rights and health provisions.

The point is that the Commission's Report is presented as "starting a debate" on issues of privacy, dignity, and health despite the fact that such debates had been going for at least eighteen months since the EP's request. According to some privacy advocates, instead of weighing the pros, cons and costs of scanners, the Commission demonstrates a firm intention to legitimize their EU-wide use (Ludford, 2010).

In the meantime, formal trials of scanners were undertaken in Finland, the UK, the Netherlands, France, Italy and Germany, under a patchwork of different national operational procedures and standards. While some of the states, happy with the experimental results, are planning to deploy more devices, some of them are dissatisfied and have stopped using them.

For example, in the UK, the machines are deployed at Heathrow and Manchester airports, and the government intends to deploy scanners at all UK airports by the end of 2010. In Germany, two body scanners have been installed for a six-month trial period at Hamburg's Fuhlsbuettel Airport in October 2010, and more scans may be deployed soon.

In Finland, where the device was introduced in Helsinki in October 2007, the Civil Aviation Authority decided to discontinue the use of the scanner after 18 months. It was reported that privacy

[10] Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at European airports, 15.06.2010. COM(2010) 311 final.

[11] Regulation EC No 2320/2002.

[12] Article 6 of Regulation (EC) 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security.

[13] Commission Regulation (EU) No 185/2010, Chapter 12.8.

[14] Working Party on the Protection of Individuals with regard to the Processing of Personal Data established pursuant to Article 29 of the Directive 95/46/EC (Article 29 Working Party). This organ consists of representatives from each EU Member State's data protection authority. It acts independently of the Commission and other EU organs, but has advisory competence only.

[15] Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at European airports, 15.06.2010. COM(2010) 311 final.

concerns influenced the decision, specifically, the EP Resolution, which failed to recognize the machine as an appropriate security measure.[16]

Italian Corriere della Sera of 23 September 2010 reported that after a six-month test, the Italian government would also drop the use of body scanners, deeming them slow and ineffective.

3. Human rights concerns

As mentioned above, the use of body scanners has an impact on fundamental human rights enshrined in different human rights conventions, such as the Universal Declaration of Human Rights of 1948 (UDHR), in particular human privacy and dignity, respect for private and family life and rights of the child. They breach the data protection rights since the production and processing of persons' images amounts to a processing of personal data. Some persons might face difficulties reconciling their religious beliefs with a procedure entailing their body image being viewed by a human screener; thus, scanners have an impact on freedoms of thought, conscience and religion.[17]

There are also potential consequences to passengers' health, including possible harms from radiation. The states and manufacturers claim that scanners deliver a "safe" dose and are not harmful, the long-term effects are not yet known. Potential harms may exist to the frequent traveler, children, persons with specific medical conditions such as pregnancy, chronic health conditions, and to security and airport personnel who are repeatedly exposed to radiation?

Finally, if faced with the dilemma of going through the scanner or not flying (which is the case if no alternative screening method is provided), the persons right to freedom of movement may be restricted. According to Article 13 of the UDHR, everyone has the right to freedom of movement and residence within the borders of each state. Everyone has the right to leave any country, including his or her own, and to return to his or her country.

The UDHR Article 29 provides that "in the exercise of their rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."

With the exception of human rights that cannot be derogated for reasons of national security in any circumstances (peremptory norms or jus cogens, which include the right to life, the right to be free from slavery, the right to be free from torture and the right to be free from retroactive application of penal laws.), the enjoyment of some human rights may be restricted during times of war or public emergency.[18]

Routine screening of passengers in airports can hardly be seen as a measure of national emergency. It is normally related to aviation security and is carried out in the interest of routine national security and public safety. Thus screening specifically serves the protection of the rights and freedoms of others and takes into account the threat of terrorist attacks, the right to life of air passengers and crew.[19] But is it possible to reach a situation when the persons' rights to life and safe travelling would not be in conflict with their rights to dignity and privacy?

It should also be noted here that, in accordance with some views, the rationale of human rights limitation as well as the key definitions should be reconsidered due to the changed reality, affected by the threat and by fear. What may have seemed unreasonable before 11 September may now be deemed reasonable. This means that the principles and standards of human rights protection can be interpreted according to new approaches. For instance, in the USA researchers note that the historical evolution of the law as it applies to airport screenings reveals a number of disturbing points concerning Fourth

---

[16] Helsingin Sanomat International Edition. *Helsinki-Vantaa Airport discontinues X-ray scanning of passengers.* http://www.hs.fi/english/article/Helsinki-Vantaa+Airport+discontinues+X-ray+scanning+of+passengers/1135249838862 (last visited 23.11.2010).

[17] For example, according to the information website Dubai.com, the Dubai Airport authorities have rejected the use of body scanners at the Emirates' airports as they violate ethical principles relevant to Islamic culture.

[18] Article 4 of the International Covenant on Civil and Political Rights (1966).

[19] The applicability of scans to the crew members and their rights in this regard constitute a separate question for discussion. Currently there is no common consensus concerning whether the flight crews should be obligated to go through the machines under the same rules as passengers.

Amendment protections. A review of the cases illustrates that the private person rarely wins and that searches are almost always found to be reasonable (Kornblatt, 2007, p.403).

3.1. Right to privacy

Privacy is a fundamental human right. It is recognized around the world in diverse regions and cultures. The concept of privacy has broad historical roots in sociological, philosophical and anthropological discussions. There is no single definition of privacy, but normally it is associated with the private sphere, family and domestic life, the individual's "right to be left alone" (Warren and Brandeis, 1890). Protection of privacy is frequently seen as a way of drawing the line for how far society can intrude into a person's private affairs.

The basic principles can be found in Article 12 of the UDHR. According to the European Convention on Human Rights of 1950 (ECHR), "everyone has the right to respect for his private and family life, his home and his correspondence" (Article 8 (1)). "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" (Article 8 (2)).

Privacy is also protected in many other international and regional human rights treaties and in the national constitutions and/or legislation of many countries. In the USA, the citizens' constitutional rights against warrantless searches and seizures are enshrined in the Fourth Amendment: "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."[20]

Thus, the most critical point for privacy advocates in the USA is that which applies to "unreasonable" searches and seizures. According to Katz v. United States (1967), a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. In United States v. Davis (1973), the Court stated that administrative searches, to be valid, must meet the standard of reasonableness as required by the Fourth Amendment. To be reasonable, a passenger screening search must be as limited in its intrusiveness as it is consistent with satisfaction of the administrative need that justifies it. But the amount of danger posed to the public by a person trying to blow up an airplane has created a situation where the danger satisfies the reasonability test, and the courts may view passenger airport screening searches as virtually reasonable per se (Kornblatt, 2007, pp.393 and 396).

With reference to the EU, the questions that arise concern whether the use of body scanners engages the provision of ECHR Article 8 (1), and if applicable, whether Article 8 (2) applies to permit the limitation of this right.

3.1.1. ECHR Article 8 (1)

The main purpose of the body scanners is to see objects carried under clothes. In the Resolution of 2008 the EP stated that the machines produce "scanned images of persons as if they were naked, equivalent to a virtual strip search." Now this conclusion is arguable in view of the development of different measures and operational procedures designed to ensure the privacy of people who step into the portal.

The deployed technologies produce a black and white silhouette - a gray image of the human body and any objects concealed on it. The faces and other areas of the body can be blurred, and any distinguishing features such as hair or skin tone are not displayed so that it is impossible to identify people from their facial features. But despite these attempts to provide anonymity, the scanners still penetrate the whole of a person's physical identity. 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

[20] The Fourth Amendment to the Bill of Rights in the U.S. Constitution.

(Mountfield and Gearty, 2010, p.5). 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. Members of particular groups including disabled people, transgendered people, older people, children, women and religious groups can experience additional negative effects on privacy.

Another measure is that the system enables analysts to be stationed in separate rooms, where they cannot see the individual being screened in person. Some scanners are designed in a way that the analyst does not know which scanner generated the image. But there are still doubts that the reviewer would be unable to discover who was going through the machines if he really wanted to do so. For example, according to Nigerian newspaper This Day of 21 September 2010, the security officials at Lagos airport hurried over to the line in order to catch a glimpse of some of the passengers entering the machine and then immediately returned to view the naked images in order to match the faces of their favorites with the images.[21]

Furthermore, the EU proposes that detailed reviewing of images might be undertaken by a person of the same gender. The UK passengers can ask for same gender screening if they wish. The USA does not provide such an option. "The blurring of body parts and "detailed reviewing" of images by staff of the same gender are both invoked as safeguards. But these provisions are contradictory. When will the scanner produce a blurred image that respects privacy, and when will it produce a clear image for detailed review? And if the image is so anonymous and innocuous, why make the stipulation for a same-sex reviewer?" (Ludford, 2010). Thus, despite the measures undertaken, the abovementioned EP's statement may still be valid.

But if a person is given an opportunity to be screened by an alternative method, will this constitute a safeguard? In the USA at the present time, those who refuse to go through scanners can undergo a pat-down search. The S.A.F.E.R. A.I.R. Act would provide alternative methods entailing either (i) both passing through a metal detector and undergoing a pat-down search, or (ii) screening using such other method or combination of methods for screening passengers as the Secretary determines and certifies to Congress as appropriate and effective.

The UK Government does not propose to offer an alternative method to those who decline to be scanned. It is stated that "when persons chose to fly they accept that they must comply with security requirements and that if persons do not want to be subject to security scans, then they do not have to fly."[22]

The EU Commission's Report proposes that any possible future EU harmonization in this area needs to provide for alternative security checks for vulnerable groups including pregnant women, babies, children and people with disabilities. But according to the Report, under the existing rules relating to the screening methods recognized today, passengers are not offered any possibility to refuse the screening method or procedure chosen by the airport and/or the screener in charge. In addition, several airports would not dispose of the needed capacity and staff resources necessary to provide a regular alternative to security scanners.

Thus despite the fact that some proposals consider alternative methods as safeguards, it is unclear whether they can ever be put into practice. Moreover, the issue as to what is less invasive – pat-downs or scans – is still questionable.

Apart from alternative methods, there is an idea of simply making exemptions for the vulnerable groups. In the UK, for instance, the scanners may violate the Protection of Children Act of 1978 by creating images or pseudo-images of nude children. The Guardian of 4 January 2010 reported that "Ministers now face having to exempt under 18s from the scans or face the delays of introducing new legislation to ensure airport security staff do not commit offences under child pornography laws." But with such exemptions, there is a concurrent risk that terrorists would then recruit children.

The European Court of Human Rights (ECtHR) has given ECHR Article 8 a very broad interpretation. In S and Marper v United Kingdom (apps 30562/04 and 30566/04, 4 December 2008),

[21] Chinedu Eze. *Now Showing at MMIA: Nude Images of Passengers.* http://allafrica.com/stories/201009210101.html (last visited 23.11.2010).

[22] The UK Department for Transport. Code of practice for the acceptable use of advanced imaging technology (body scanners) in an aviation security environment. A consultation paper, January 2010. www.dft.gov.uk/orderingpublications (last visited 23.11.2010).

the ECtHR referred to some other ECtHR cases and stated that the concept of "private life" is a broad term not susceptible to exhaustive definition; it 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 fall within the personal sphere protected by Article 8; beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family; information about the person's health is an important element of private life; an individual's ethnic identity must be regarded as another such element; the concept of private life moreover includes elements relating to a person's right to their image. According to the ECtHR, the mere storing of data relating to the private life of an individual amounts to an interference within the intent of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

In the case of scanners, an intimate image described above is captured and then scrutinized by a security officer in order to identify whether or not the imaged passenger needs to be further examined. Even if it is true that the image would not be saved by the authorities and would be destroyed after the process is completed (this issue will be discussed in 3.2 below), it is nonetheless retained for the brief time required for analysis, with the examination being conducted by a human operator, not a machine. The breach of privacy as stipulated by Article 8 therefore is constituted by first the production and then the analysis of the image (Mountfield and Gearty, 2010, p.6).

But one can argue that the right to privacy can be considered as waived by the passengers since the travelers make agreements with airlines to transport them to the places of destinations and that such agreements may involve acceptance of various conditions, including security requirements. Thus they might be considered as giving their consent to breach of Article 8 in the interests of security at the moment they purchase an airline ticket. However not all such waivers are automatically effective: the ECtHR case law is clear that a waiver, to be successful, must be unequivocal and attended by minimum standards commensurate with its importance (Clayton and Tomlinson, 2009, pp. 398-401). A contract between two parties cannot be taken to have produced a waiver simply on account of its existence.[23] Thus a passenger can hardly be considered as waiving Article 8 rights by flying.

3.1.2. ECHR Article 8 (2)

Given applicability of Article 8 (1), it is important to indicate whether the interference is in accordance with the law and if the scans satisfy to the legitimate aim, proportionality and necessity principals pursuant to Article 8 (2).

In Gillan and Quinton v United Kingdom (application no. 4158/05, 12 January 2010), the ECtHR unanimously found the discretionary powers of stop and search in the UK Terrorism Act 2000 to be a breach of Article 8, notwithstanding that it was provided for by a statutory measure, on the ground that the provision of Article 8 stipulating "in accordance with the law" was not met. As it was mentioned above, the use of scanners is not currently regulated at the EU level, and member states are allowed to apply more stringent measures on the basis of either Regulation (EC) 300/2008, or Commission Regulation (EU) No 185/2010 as trials not exceeding 30 months. Article 6 of the former document provides that such measures are permitted if the measures adopted are "relevant, objective, non-discriminatory and proportional to the risk that is being addressed, and communicated to the Commission as soon as possible."

But the point is that in Resolution of 2008 (although non-binding), the EP noted that the Commission had proposed a draft regulation supplementing the common basic standards on civil aviation security to include body scanners. This implies that the Commission did not consider that such scanners were clearly included within the existing common basic standards contained in the Annex to the Regulation. The question that arises, therefore, is whether or not the above-mentioned

[23] Rommelfanger v Germany (1989) 62 DR 151.

Regulations and the member states' rules for operating within them have the quality of law (Mountfield and Gearty, 2010, p.17).

The European Court of Justice in Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission (C-402/05 P and C-415/05 P, 3 September 2008) has established that even provisions with an ostensible basis in European law may yet lack the qualities of law by contravening common European human rights standards and thereby may be contrary to common European law.

Thus, there is a good argument that the introduction of body scanners cannot be regarded as being "in accordance with the law", because the regime under which this has been done fails to contain sufficient safeguards to protect fundamental rights from arbitrary interference. If so, then the presumptive breach of Article 8(1) described above is not saved by Article 8(2).

There are a number of aims behind the introduction of scanners, including the interests of national security, public safety, the prevention of crime and the protection of the rights and the freedoms of others, which are covered by Article 8 (2).

The breach of the right to privacy is also likely to be considered proportionate to the threat which the scanners are supposed to prevent (although the EP raised doubts on this issue in its Resolution). However, how can the use of scans be proportionate if they are not universally deployed in all member states, but unilaterally in some of them, and, in addition, only at some airports and according to different rules and procedures?

As for the necessity and effectiveness, there are many discussions about whether the scans actually add value in serving the abovementioned interests, in particular in the war on terrorism and crime. Pro arguments have been discussed in section 2; con arguments will be considered below.

Firstly, neither millimeter-wave technology nor backscatters can detect explosives carried inside the body. The first known attempt when the internal method was used by the Al-Qaeda suicide bomber Abdullah Hassan Tali al-Asiri in July 2009. The second major incident was the previously mentioned attempt by the "underwear bomber". Al-Asiri's target was not the aircraft, but he took two flights and passed through two airport security screening systems to reach his intended target. The "underwear bomber" boarded the flight at Schiphol airport, which already had 15 body scanners. The scanner's manufacturers admitted that they would not have detected the underwear bomb because it was in a light powdered form and the detonator was hidden in a body cavity.

Secondly, the technology may not be able to distinguish foreign objects such as prosthetics and weapons. Thus the percentage of false positives is high and it therefore may increase the need for manual searches (despite the fact that the governments claim scanners reduce such need).

In contrast to manual searches requiring 2–3 minutes, the machines take only seconds to produce and interpret passenger data. In the TSA demonstration, the millimeter-wave scan took about one second, and the entire process took 20 to 40 seconds, while the backscatter scan took about five to seven seconds, and the entire process 10 to 20 seconds. On the negative side, scans, like all technology, ultimately rely on human operators to do visual scanning. An extremely finite period of time means evidence might be missed. Moreover, the operators may not have the required technical expertise to intercept the data and may have only minimal training before being posted.

Use of the scanners means considerable costs. A price of a basic scanner ranges between EUR 100 000 and EUR 200 000 per item, excluding training, installation, and maintenance costs. Theoretically, if the amounts paid for the scanners could be spent on different security measures providing more security, this would mean that deploying scanners actually reduces security.

Similar to other aviation security measures, the scanners are being implemented as a reaction to past situations. It was the "underwear bomber" who prompted the states' interest in scanners. According to many security experts, such an approach will fail to anticipate the next bomber.

Finally, measures taken to address privacy concerns over the use of the scanners may dampen the machines' effectiveness in locating arms and explosives (this was presented by Italian authorities as one of the grounds for suspending the use of scanners).

While it can be acknowledged that there is a legitimate aim for the invasion of privacy, the effectiveness of scanners is questionable. Even if it is accepted that their use is necessary and proportionate, serious concerns about whether the intrusion is in accordance with the law still remain. Thus, it can be hardly stated that Article 8 (2) permits the limitation of privacy.

3.2. Right to data protection

This right is protected by Article 8 of the Charter of Fundamental Rights of the European Union (2000) and other international legislation on data protection,[24] Directive 95/46/EC (Directive) being the most comprehensive of the instruments. While the EU has historically enacted broad legislative protection of personal data, protection afforded by the US law is different. The USA is not legally bound by any of the international instruments on data protection. The US Constitution and interpreting case law provide general protection, and there are some statutes that limit the use of data, for example the Privacy Act (1974), which protects personal information when it is processed by the federal government.

The Directive requires the EU member states to create legislation implementing its provisions. However, according to Recital 16, the processing of image data does not fall within the scope of the Directive if it is carried out for the purposes of public security, defense, and national security or in the course of state activities which do not come within the scope of Community law. Article 3(2) states that the Directive does not apply to the processing of data which falls outside the scope of Community law, such as activities relating to security, defense or crime. Nevertheless, member states may apply the Directive's principles in a uniform way to all processing activities both inside and outside the scope of Community law. The EP and the Commission explicitly state that the scanners' deployment falls under EU legislation on data protection (Commission's Report §51).

The Directive provides the key definitions in Article 2. According to it, the images created by the scans fall within the realm of "personal data" because it is information relating to an identified or identifiable natural person ("data subject"). The latter would thus be a traveler whose image is scanned; an identifiable person is one who can be identified, directly or indirectly, among other things by reference to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The use of these data, even if it is not recorded, falls within the definition of "processing", which means any operation performed upon personal data. The legal body which determines the purposes and means of the processing of personal data, that is, operator of the scanner, is the "controller".

Moreover, the images include sensitive data, because they consist of data revealing the data subject's racial or ethnic origin, religious beliefs, and data concerning health and sex life (Article 8 (1)). The processing of sensitive data is prohibited. The provided exemptions and derogations from this rule are very strict, enabling processing only with the explicit consent of the data subject. If the data subject is physically or legally incapable of giving his consent, the processing is possible if it is necessary to protect the vital interests of the data subject or another person.

The data protection legislation provides basic principles for personal data processing:[25]

Collection limitation principle: Personal data must be collected and processed fairly and lawfully and kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Data quality: Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, be accurate, kept up to date.

Purpose specification: Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with purpose specification principle except with the consent of the data subject or by the authority of law.

---

[24] The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981; the 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 personal data and on the free movement of data.

[25] Directive 95/46/EC Articles 6, 7, 10–12, 16-17, 22-23; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) Paragraph 14; the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

Security and confidentiality: Collected data should be kept secure from any potential abuses.

Transparency and data subject participation: Data subjects should be informed of the data processed, purposes of such processing and the identity of who is collecting their data. They should be allowed to access their data and make corrections to any inaccurate data.

Accountability: Data subjects should have a method available to them to hold data collectors accountable for following the above principles.

These principles are potentially engaged in the case of scans.

"Lawfulness" has the same meaning as under Article 8 ECHR, thus the discussion above on privacy issue is applicable to the data protection issue as well. In addition, since the data is sensitive, the requirements on explicit consent should be met.

The storage and retrieval of images created by scanners present one of the most controversial points for discussion. The governmental agencies and manufactures say the scanned images cannot be stored, transferred, copied, or printed, and are permanently removed after security personnel review them. But can this be true?

The security organs actually need to retain the images as evidence, should they actually find a real terrorist, and probably also for testing and training purposes. In the EU Commission's Report it is stated that there is no need for images to be captured or stored for future use such as, for example, evidence in a Court case since it would be the discovery of an actual forbidden object on the person, and not the discovery of an image on a machine, that would be the basis for prosecuting a person. But who can decide for the Court how to treat such cases in the future? In the event the person later states that the object did not belong to him and appeared during the arrest, important evidence which could prove the opposite may be missed. Thus the Commission's conclusion can be changed by the Courts' practice any time.

Moreover, the machines would need the capability to save images for later inspection to find out what went wrong with the scans if there were a successful terrorist attack.

From a technical point of view, the manufactures claim that, if so requested by the customer, they are in the position to make technical changes to the machines so that they will not save the images (the TSA states that the scanners used in the US airports do this). But 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.[26] According to a letter from 15 April 2010 from TSA to EPIC, the TSA possesses about 2000 body scanner photos from devices that the TSA said earlier "could not store or record images".

The experts also admit that the images are still being captured and stored by these "changed" devices, that is, the actual images still exist somewhere inside the machines. Thus a risk of possible abuse emerges. One solution might be that a system of encryption or similar security, regulated by law, could be introduced to allow limited access to the images. In addition, the law requires that if the images are saved and kept, mechanisms should be provided allowing the travelers to access and rectify the data. As long as the governments state that they do not save the data, this may be difficult. Thus, information concerning how the scans actually work is essential. The technical requirements should be established by law, with enforcement mechanisms. But at present the governments and producers' controversial statements and assurances seem to be one-sided and difficult to rely on. The privacy advocates' opinions may be one-sided as well. Therefore, as long as there is lack of complete, comprehensive and reliable information about what the devices actually are, all discussions can be only speculative.

Further, according to the US S.A.F.E.R. A.I.R. Act, passengers shall be provided with (i) information about the images; (ii) information regarding the privacy protections; (iii) sufficiently detailed notice and an explanation of the alternative option for primary screening. The EU Commission proposes that appropriate, comprehensive and clear information on all aspects of scanner usage should be provided to the public at airports, before travelling. But these proposals do not give sufficient details about how appropriate, comprehensive and clear information can be provided to the passengers in reality, before travelling and before purchasing the tickets, and who will be responsible for the information provision. This could at least enable the passengers to make an informed decision

[26] Procurement specification for whole body imager devices for checkpoint operations, U.S. Department of Homeland Security, TSA. FINAL, Version 1.02, 23 September 2008.

as to whether they wish to be scanned or not (if alternative methods are available) and/or whether or not to fly.

Finally, if alternative and less intrusive screening methods are available, and if an individual is concerned about the implication of scans (due to disability, pregnancy, or other reasons) and consents to the alternative methods, then it may be considered excessive to require such a person to go through a scan.

The Directive 95/46/EC provides exemptions in Article 13, which stipulates that the member states may restrict the scope of the principles mentioned above when such a restriction constitutes a necessary measure to safeguard, among other things, national security, defense, public security, the protection of the data subject or of the rights and freedoms of others. But according to some views the indication of "a necessary measure" means that these exemptions are restricted only for specific investigations, a case by case request, and not to the case where the personal data processing is systematic as it is foreseen by the scanners usage. This approach is questionable, but even if we consider that the exemption is applicable, many of the issues which have been discussed under the analysis of Article 8 ECHR may still be applicable to data protection legislation issues as well.

In summary, it can be concluded that deployment of scanners cannot be currently regarded as in compliance with all the established data protection requirements and privacy standards.

4. *Future*

Will new technologies determine the future in aviation security?

One of the companies states that it is working on a millimeter-wave system that would take up less space and would not require passengers to stop and stand still. Another proposal is a Flight Assistance Security Trolley, which would allow a passenger to go through the security check points taking along all clothes, shoes and baggage, including liquids, and be scanned without even noticing it. Software is in the works that would recognize anomalies automatically rather than depending on humans to interpret images (Automatic Threat Recognition).

The X-ray transmission imaging technology can detect explosives carried internally. The technology is currently used in prisons, diamond mines and at airport arrivals areas for catching "drugs mules". The only machines of this type being used for screening boarding passengers are in Nigeria, but they are being used exclusively for drug interdiction and only for passengers flying directly to the USA (Kingham, 2010). The use of X-ray technology to screen passengers could prove to be highly effective. The X-ray body scanner producers are already represented in the security market. They promote their products for airports and claim that the radiation doses are safe and that all privacy concerns are satisfied, that is, absolutely the same claims made by their competitors. Thus it will not be surprising when they are deployed sooner or later.

The new technologies, applied first in aviation, can later spread to other means of transportation and other spheres where surveillance is critical. But overreliance on technology, that is, the belief that the machines can take care of an issue so that one does not need to worry, will not ensure total security and may have a negative effect. The security experts agree that technology can never be the "sole solution", but only a means of reacting, and 100% security can never be achieved.[27]

The latest tendencies and ideas from the aviation security professionals show that what is really needed is to change the system. According to them, there should be an intelligence-led system, with an element of randomness and unpredictability in security screening and the use of technology. An intelligence-led system would enable recognition of individuals who pose a possible threat from the moment they appear at the airport. For example, so-called "behavioural analysis techniques" are intended to help the professionally trained security staff to spot passengers acting unusually and target them to further search. It would then be at the discretion of the security staff to choose the appropriate screening techniques or technology: pat-downs, body scanning, cavity searches, etc, and if they are still not satisfied, a no-fly order. Another technique supporting decisions concerning the persons who should be subjected to additional security measures is "targeted passenger profiling" (although these techniques may raise separate human rights and equalities issues) (Mountfield and Gearty, 2010, p.2).

[27] Materials from Transport Security Expo 2010, Olympia, London, 14-15 September 2010. For example, Mower, Nick. (European Regions Airline Association) *Aviation Security-A Roadmap For Change*.

The manufactures also state that X-ray body scanners are best used for targeted individuals who have been identified by other means. With such an approach there may be no need to scan all passengers, No mass scanning of the general public would mean fewer privacy concerns. Unfortunately, it is not known if these plans will ever be adopted.

5. Conclusion

As with most security issues, it is always a question of balancing interests. But while there are doubts about whether the security agencies are capable of making the most effective use of scanners and whether they add value to the war on terrorism and crime, it is quite obvious that this technology exposes passengers to a significant loss of privacy and dignity and constitutes a limitation of other rights and freedoms.

However, there are a lot of political and economic issues and policies which greatly affect the security and privacy regimes. There is a huge industry behind the screening equipment with their own lobbies in legislatures and governmental agencies. From the other hand, the governments need to ensure the public that they "are doing something" and the scanners seem to be perfect means for this. It is not surprising that the majority of citizens are ready to give up some of their rights when this is aimed at combating terrorism. "Go through a scanner or get blown up. I know which I prefer. Or if you don't like it - don't travel on a plane."[28] It is extremely difficult for the privacy advocates to champion their views in this climate.

The point is that breaching people's rights and freedoms can be justified under human rights legislation, if it is done in accordance with the law and is proportionate and necessary for national security, public safety and for the protection of the rights and freedoms of others. If it is accepted that the security benefit outweighs the health and privacy risks, this does not automatically mean that privacy and other values should be given up or that standards should be reduced. Increased security does not always mean reduced privacy.

Nevertheless, in the meantime the governments have failed to demonstrate that the body scanner security policy is currently justifiable within the law. Existing legislation and proposals suffer from various weaknesses and need improving. From the EU Commission's Report and other consultation papers we can see some endeavors to incorporate and ensure the aforementioned standards, but they all contain weak privacy provisions that ignore many of the problems already identified in relation to the devices.

While halting the deployment of scanners would be unrealistic, a more practical solution would be to adopt appropriate legal, policy and technical measures focusing on two key aspects: regulate and control (i) the adoption of the scans and (ii) the use of the scans. In addition to legal norms, the means for ensuring their effective application should be established as well.

The deployment of the machines should be restricted by law and permitted only under conditions where it is necessary. From the effectiveness prospects, as long as the technology detects such sensitive items as prosthetics, breast implants, diapers, etc. and may fail to tell the difference between them and weapons, the law should provide that body scanners may neither be used as the only or primary method of screening passengers, nor as a method for screening any person unless another method of screening, such as metal detectors or behavior analysis, gives cause for additional searches. Any derogations and exceptions should be provided by law and applied strictly.

In order to evaluate the necessity, reasonableness and proportionality of the technology applications, several factors should be taken into consideration: available alternatives, types of scans chosen, technical features, etc. Different devices may differ in the effectiveness levels and privacy impacts. To decide which kind of technology to choose an evaluation of all relevant factors should be fulfilled. Much expectation is also made to the new generation of scanners which would enable a technical solution to some of the 'privacy issues'.

[28] Comments to: Sarah Ludford. European commission is fence-sitting on body scanners. Guardian.co.uk. 24 June 2010

An option of alternative security methods should be further developed and made available to people with 'privacy concerns' and ⁄or who do not consent. States should concentrate on developing alternative solutions that are non-invasive or less invasive for passengers.

Data protection framework could be improved by establishing detailed mechanisms to enable individuals to enforce their rights. Passengers should be provided with appropriate, comprehensive and clear information about the applicable security measures – along with information regarding the protection of their rights – before travelling and before purchasing the tickets.

Complete and reliable information regarding the functioning and technical specifications of the devices, reviewed and examined by competent authorities (including independent reviewers), should be provided and made publicly available in an appropriate form.[29] Moreover, there should be specific requirements regarding the quality of the machines. Technical specifications should include limitations on image capture, storage, or copying. The requirement of a system of encryption, password or similar security, different identification/authentication mechanisms as well as usage of other technical measures enhancing privacy and data protection should be provided and regulated by law. These requirements should concern all the stages of the technology operation, with the measures being integrated into the devices already at the design phase. All technical requirements should not only be established by law, but be accompanied by control and enforcement mechanisms.

Since the images produced by scans include sensitive information, they should receive stricter privacy protection. The potential of extracting health information should not be underestimated. A simple general prohibition is unlikely to be a practical solution. Further research is needed to deal with such risks (Liu, 2010).

In addition to general privacy and data protection regulations such as the Directive 95/46/EC, other regulatory models may be used for the scanners. It would be a good idea if the ICAO took the initiative to establish global common rules and standard approaches for the image screening technologies, particularly in relation to ensuring passengers' rights, as has already been done with some other security measures. Although the ICAO's regulations and guidelines are recommendations only and not obligatory for contracting states, they could become helpful in efforts to establish global, standard approaches in the aviation industry, which by definition is international in scope. Furthermore, the ICAO's role could be revised, so that it might be enabled not only to establish, but to enforce such rules. Another option would be adoption of industry self-regulations in the form of Code of conduct. Such combination of general privacy and data protection legislation with special guidelines and regulations on the technology may be a promising solution.

Olga Mironenko (olga.mironenko@jus.uio.no) Ph.D. Candidate, Norwegian Research Center for Computers and Law (NRCCL), University of Oslo, Norway http://www.jus.uio.no/

Olga Mironenko holds a diploma in law from the State University – Higher School of Economics in Moscow and an LLM from the University of Oslo in Information and Communication Technology Law. She formerly worked as a lawyer in the civil aviation industry in Russia.

Bibliography

Bygrave, L. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*. Kluwer Law International, 2002.

Clayton, R. and Tomlinson, H. (2009) *The Law of Human Rights*. 2nd ed., 2009. pp 398-401.

Harris, D. (2009) *Law of the European Convention on Human Rights.* 2nd ed., Oxford University Press, Oxford, 2009.

Kingham, T. (2010) *Airports Exposed*, Intersec. January 2010.

Kornblatt, S. (2007) *Are Emerging Technologies In Airport Passenger Screening Reasonable Under The Fourth Amendment?* Loyola of L.A. Law Review. Fall 2007. p.403

[29] Release of such information of course should be done with due care, in order not to constitute a threat to transportation security by enabling terrorists determine all the capabilities and limitations of the devices.

Kuner, C. (2007) *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed., Oxford University Press, Oxford, 2007.

Liu, Y. (2010) *Bio-privacy: legal challenges for privacy regulations of biometric identification and authentication*. Norwegian Research Center for Computers and Law, Oslo, 2010.

Ludford, S. (2010) *European commission is fence-sitting on body scanners.* Guardian.co.uk. 24 June 2010.

Mountfield, H. and Gearty, C. (2010) *Advice in the matter of the human rights and equality implications of the introduction of full body scanners at airports.* Matrix Chambers, 8 February 2010.

Solove, D., Rotenberg, M. and Schwartz, P. (2006) *Information Privacy Law*. 2nd ed., Aspen Publishers, New York, 2006.

Warren, S. and Brandeis, L. (1890) *The Right to Privacy*. Harvard Law Review Boston Vol. IV No. 5, 1890.