



# POLICY Report

## Whole Body Imaging at airport checkpoints: the ethical and policy context



CENTRE FOR SCIENCE, SOCIETY AND  
CITIZENSHIP

**HIDE & RISE Projects**

POLICY Report

[This page has been left intentionally blank]

## HIDE & RISE PROJECTS

# Whole Body Imaging at airport checkpoints: the ethical and policy context



(Adi Nes, 1991, *Untitled*, Sommer Contemporary Art Gallery, Tel Aviv)

POLICY Report No. 2010/01  
February 2010

All rights reserved.

No part of this publication may be reproduced, distributed or utilized in any form or by any means, electronic, mechanical, or otherwise, without the prior permission in writing from the Centre for Science, Society and Citizenship (CSSC)

Download and print of the electronic edition for non commercial teaching or research use is permitted on fair use grounds. Each copy should include the notice of copyright.

Source should be acknowledged.

© 2010 CSSC

<http://www.cssc.eu>

### **HIDE & RISE Partnership**

- *Centre for Science, Society and Citizenship (Italy) – Coordinator HIDE & RISE*
- *Aristotle University of Thessaloniki (Greece) RISE*
- *Centre for Policy on Emerging Technologies (United States) RISE*
- *Data Security Council of India (India) RISE*
- *European Biometric Forum (Ireland) RISE*
- *Eutelis (Italy) HIDE*
- *Fraunhofer Institute (Germany) HIDE*
- *Global Security Intelligence (United States) RISE*
- *International Biometrics Group (United States) HIDE*
- *Lancaster University (United Kingdom) HIDE & RISE*
- *National Cheng Chi University (Taiwan) RISE*
- *National University of Singapore (Singapore) HIDE*
- *Optel (Poland) HIDE*
- *Sagem Sécurité (France) HIDE*
- *The Hasting Center (United States) HIDE*
- *The Hong Kong Polytechnic University (Republic of China) RISE*
- *University of Ljubljana (Slovenia) HIDE*
- *University of Tartu (Estonia) RISE*
- *Zuyd University (The Netherlands) HIDE*



**HIDE** - *Homeland Security, Biometric Identification & personal detection ethics (GA 217762)*, and **RISE** - *Rising pan-European and international Awareness of Biometrics and Security Ethics (GA 230389)* are two triennial, multicenter, research project funded in the scope of the EC RD&T Framework Programme 7 (FP7), Capacities (Science in Society)

### **Contact Details**

All correspondence should be addressed to the HIDE & RISE Coordinator, Centre for Science, Society and Citizenship, Piazza Capo di Ferro 23, 00186 Rome, Italy

The telephone number for general enquiries is 0039 0645551042

The email address is: [cssc@cssc.eu](mailto:cssc@cssc.eu)

# Executive Summary

---

## CONCLUSIONS

**WE BELIEVE** that the primary aim of security is to safeguard the human person in his or her physical, mental, and social integrity. Respect for human dignity, body integrity and privacy (both physical and informational) are thus essential components of any security policy. Security measures which impair human integrity of those which should be protected are self-contradictory and eventually are also less effective. The primary purpose of WBI technology and systems is only to detect prohibited items concealed on the body. We think that WBI is legitimate as far as it fulfils its original purpose. Any different goal, like people identification or profiling, or detection of anatomic and/or medical details, is not legitimate and is not respectful of personal integrity.

**WE ARE CONCERNED** that body scanners could humiliate people by unravelling anatomic and/or medical details, and by hurting their feelings of modesty. We are concerned by the lack of clarity about WBI operating procedures, and by confusion and inconsistencies about primary and secondary screenings, voluntariness and compulsion. We are also concerned that body scanners can be used to discriminate against certain groups of travellers. Moreover, we are concerned that WBI technologies and systems can be (mis)used for wider purposes than the detection of concealed objects.

**WE REGARD** the European Charter of Fundamental Rights as the general framework for the introduction in the EU of new technologies for passenger screening and aviation security.

**WE RECOMMEND** that respect for the primacy of the human person and attention to his or her needs are the leading principles followed in the establishment of aviation security. We also recommend that the European Commission should propose a specific framework for detection, profiling, and identification technologies for aviation security. We recommend that WBI operating procedures should be subject to a public, democratic scrutiny. Appropriate exemptions can be provided only for those parts of SOP manuals which directly deal with technically sensitive details. We finally recommend that the European Commission should encourage the use of codes of practice and ethical codes at MS level, and promote the establishment of a system of complaints and remedies at EU level.

**WE WELCOME** the regular use of privacy enhancing and “privacy-by-design” technologies in WBI system design. We also recommend that technologies should be selected and systems should be designed in order to make it practically impossible to fulfil illegitimate purposes. We recommend that the European Commission, in conjunction with the European Data Protection Supervisor and the Art.29 Working Party, promote independent, publicly available, Privacy Impact Assessments (PIAs) prior to the adoption of any new WBI technology and system.

**WE URGE** the European Commission to commit to a plan of action to promote further research on ethical, legal, and social implications (ELSI) of technologies for aviation security, their likely effect on public trust and their communicational and symbolic dimensions. In particular we recommend that the European Commission and the European Parliament promote the adoption of an ethical framework for trials with new WBI technologies.

## MESSAGES TO EUROPEAN POLICY MAKERS

1. Practices which concern the body are unavoidably invested with cultural values, and in their turn produce new values. **WBI impact assessment should consider the symbolic dimension**, which is often more relevant to policy setting than conventional technology assessment.
2. In order to make WBI technology consistent with respect for human dignity, integrity and physical privacy **WBI should not show the “naked” body but merely the objects the person is holding**. This general tenet implies two converging strategies. First the officer viewing the image should not see the scanned person. The use of modesty filters is also advisable. Second, WBI systems should be selected according to their capacity to detect prohibited items without providing anatomic and medical details. In any case the adoption of WBI technology for routine screening is ethically tenable only if its effectiveness and proportionality are convincingly demonstrated.
3. Assuming all other conditions equal, **there is no reason to adopt X-ray backscatters**, which expose the subject to an additional – although negligible – source of ionizing radiations. Other WBI technologies should be preferred for standard use. The use of X-ray transmission systems for selected checks (i.e., explosives hidden inside the body) should be avoided and alternative technologies using non-ionizing radiations should be investigated.
4. **All forms of modesty deserve to be fully respected**– no matter how far they are from the western ethos. Some people could perceive WBI screening as an humiliating experience. Their objections should always be taken into account. No one should ever be obliged to undergo any security measure that he feels humiliating and degrading. In particular no one should be offered the option to accept such a measure in exchange for a benefit. This would make it still more humiliating.
5. **Emerging WBI technologies should be addressed as soon as possible**. In this field technology evolves very rapidly and once the use of WBI systems becomes standard in airports, there is a concrete risk that more advanced and privacy intrusive systems would then be introduced, and that they could also be used for more mundane applications.
6. **Privacy Enhancing Technologies (PETs) can alleviate privacy concern only if PETs cannot be “switched-off”**. The “privacy-by-design” approach is the right approach. In addition, given the highly sensitive policy area, it would be advisable to introduce an independent and legally binding control that PETs are properly implemented. In terms of communication with the public, it is

paramount that any privacy complaint – although unrealistic – is seriously considered and overtly discussed.

7. Although images are not retained, there is no doubt that **WBI systems are generating data**. Reaching an international consensus about whether these data are personal and to what extent they are sensitive is certainly important. Yet it is still more important to find a consensus about 1) what data are actually generated; 2) how they should be protected. WBI systems could be hacked and there is a common interest from both security agencies and privacy advocates to improve body scanner security and to build more and more secure systems.
8. If we want to implement trusted body scanners, we should **define a legal framework** and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy. This should be substantiated in appropriate standards and certification procedures. If WBI has to be implemented, **European standards and certifications** must be developed as soon as possible.
9. **Reviews of WBI technologies** and the rationale which justifies their use, notably as far as the proportionality principle is concerned, must be carried out on regular basis. Citizens input during the system application phase should also be part of the total review system. Although specific contents of these reviews could be partly restricted, **review results should always be public**.
10. Selective screening procedures are hardly consistent with fundamental rights and should be avoided. We welcome the EDPS and Art.29 WP suggestion that **body scanner screening should be universal**, say, no specific subgroup of travellers should be targeted or exempted on the basis of considerations about nationality, race, ethnicity, religion, gender, and age. Yet we understand that **specific security conditions could oblige the selection of specific categories of people** for body scanner screening. Such a procedure should always be convincingly justified and should be temporary.

## CONTENTS

---

CHAPTER 1: INTRODUCTION .....	10
Background.....	10
CHAPTER 2: THE TECHNOLOGICAL CONTEXT .....	14
Technologies and Systems .....	14
Trials and Standards .....	17
Needs addressed by WBI.....	18
CHAPTER 3: HEALTH AND PRIVACY IMPACT ASSESSMENT.....	19
CHAPTER 4: BODILY INTEGRITY.....	25
Dignity and Physical Privacy .....	26
Physical Integrity .....	31
Mental Integrity.....	32
CHAPTER 5: PRIVACY ISSUES.....	34
Privacy Enhancing Technologies .....	36
Does WBI generate personal data?.....	37
CHAPTER 6: GOVERNANCE .....	38
Regular Review .....	39
WBI operating procedures .....	39
The airport as a total institution .....	42
CHAPTER 7: CONCLUSIONS .....	43
Acknowledgments.....	45



[This page has been left intentionally blank]

# Whole Body Imaging at airport checkpoints: the ethical and policy context

## CHAPTER 1: INTRODUCTION

---

### Background

1. One of the main tasks of security checkpoints (e.g., border checkpoints, airport checkpoints, mobile, random, checkpoints) is to screen people for detecting objects and materials, like weapons and explosives. The main methods used for object and material detection rely both on non-technological (e.g., physical observation; hand searches, also including body orifice search; explosive detection dogs) and technological methods (e.g., hand-held metal detectors, HHMD; walk-through metal detectors, WTMD; explosives trace detection, so called “puffer machine”; sensors for the detection of chemical and biological contaminants). Not all these methods are routinely used in all kinds of checkpoints – selection is based on various factors, including portability (e.g., in case of mobile checkpoints), intrusiveness (e.g., in case of large scale applications), risk evaluation (e.g., airports, access to critical infrastructures). In the early 2000s<sup>1</sup> a new class of technological devices was introduced for the detection of objects and materials hidden on the bodies of individuals, the Whole Body Imaging (WBI) devices - also known as *body scanners*, or *Advanced Imaging Technology* (AIT) - where improving security is of paramount importance<sup>2</sup>.
2. According to Regulation 2320/2002<sup>3</sup>, and then Regulation EC 300/2008, the EC is allowed<sup>4</sup> to adopt measures designed to amend non-essential elements of common basic standards on aviation security. These measures include inter alia

---

<sup>1</sup> The first backscatter X-ray security screening system (The Secure 1000) was developed in 1992 by Steve Smith and commercialized by RAPISCAN, <http://www.dspguide.com/secure.htm>

<sup>2</sup> Ironically enough, in 2005 the European Parliament bought six WBI scanners “following a security-risk analysis and on the advice of an outside consultant” (C6-0416/2008 – 2008/2276(DEC), EP Committee on Budgetary Control) that were never used but could have been installed in the event of a serious terrorist alert. Three of them were delivered to the parliament’s seat in Strasbourg, the other three to the Brussels Chamber. Following the EP Resolution banning WBI technology, the Committee on Budgetary Control asked the Secretary-General “to look into the possibility of selling the scanners”.

<sup>3</sup> Prior to September 11, aviation security in Europe was managed on a national basis, and no EU common policy existed until 2002.

<sup>4</sup> Article 4(3) of Regulation 300/2008

“methods of screening, individually or in combination, as a primary or secondary means and under defined conditions”<sup>5</sup>. Draft Regulation 300/2008 included WBI systems amongst allowed European airport screening technologies. Following the EP Committee on Transport and Tourism’s request for more details<sup>6</sup>, the EU Commissioner for Transport, Mr Antonio Tajani, clarified that body scanners were to be considered “only as an additional option for the screening of passengers, not as an obligation”, and agreed on the need to examine more closely “some aspects such as impact on health and, in particular, the question of passengers privacy”<sup>7</sup>.

3. The European Parliament was not completely satisfied and with a Resolution of the 23 October 2008<sup>8</sup> MEPs blocked Regulation 300/2008, and called for a full ethical and legal impact assessment of WBI technologies on the basis that “the measures in question cannot be considered mere technical measures relating to aviation security, but have a serious impact on the fundamental rights of citizens”. MEPs asked the Commission to “carry out a fundamental human rights impact assessment”, and to “consult the EDPS, the Article 29 Working Party and the FRA”. The EP also asked the competent authorities to carry out medical and economical assessments, in order to provide a clearer picture on the possible impact on health, and a costs/benefits analysis. Further to the EP resolution, the Commission carried out a comprehensive public consultation (also including Art.29 WP, the EDPS the FRA)<sup>9</sup>. In addition to a questionnaire, the Commission also launched a 'public-private dialogue' that took the form of a “Body Scanners Task Force”, which in December 2008 convened a workshop to exchange information. Eventually the EC decided to skip mentioning WBI in the final version of Regulation 300/2008, and to postpone any decision about WBI until its privacy and health impacts were fully assessed.
4. After the failed 2009 Christmas day attack on a flight from Amsterdam to Detroit<sup>10</sup>, WBI systems again became a priority on the political agenda. Although it is arguable that they might have headed off the attack, the fact that explosive was hidden in the would-be terrorist’s underwear revived the attention on body scanners at airport checkpoints. In the US, the Transportation Security Administration (TSA) ordered 300 more WBI machines to be added to the 40 scanners being currently used at 19 US airports. The Netherlands announced they would immediately begin using this technology for screening passengers of flights heading to the United States. British Prime Minister Gordon Brown

---

<sup>5</sup> Ibid.

<sup>6</sup> TRAN/D/2008/57605, 26.09.2008

<sup>7</sup> Mr A. Tajani Letter to Mr. P. Costa, 7.10.2008

<sup>8</sup> European Parliament, Resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, RSP/2008/2651

<sup>9</sup> [http://ec.europa.eu/transport/air/consultations/2009\\_02\\_19\\_body\\_scanners\\_en.htm](http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm)

<sup>10</sup> On Christmas Eve, December 24, 2009, a 23-year-old Nigerian, attempted to set off plastic explosives concealed in his underwear as the plane in which he was travelling was on its final descent. The plane made an emergency landing in Detroit without any fatalities. At the Amsterdam airport, the Nigerian guy was subjected to the same screening as other passengers—he passed through a metal detector, which didn’t detect the explosives that were sewn into his clothes. see [http://en.wikipedia.org/wiki/Northwest\\_Airlines\\_Flight\\_253](http://en.wikipedia.org/wiki/Northwest_Airlines_Flight_253)

announced that the UK was going to include WBI among airport security measures, and the French government did the same. The Italian government also decided to install WBIs at three airports, in Rome, Milan and Venice. Yet other EU Member States (MSs) such as Finland, Spain and Germany, remained uncommitted and expressed scepticism about the need for this technology.

5. On Jan 21, 2010, the Spanish Presidency of the European Union convened in Toledo an informal meeting of Ministers of Justice and Home Affairs of the EU (JHA), jointly with the United States Secretary of Homeland Security, Janet Napolitano, to discuss boosting airport security. At the end of the meeting the Ministers agreed with Ms Napolitano that aviation security priorities include 1) *To identify individuals who pose a risk to our security as early as possible by bolstering the security of and our confidence in travel documents, the use of biometrics, and passenger screening,* and 2) *To identify the illicit materials that such people may be carrying, sending via cargo, or transporting, including through enhanced technologies, to prevent the entry of such materials onto aircraft.*<sup>11</sup> Ministers also agreed that decisions about the deployment of WBI in European airports are to be made by general consensus.
6. On Jan 14, 2010, in his hearing before the European Parliament's Transport Committee, Commissioner Siim Kallas backed the idea of a single EU regulation on body scanners and deplored that some MSs already use WBI in the absence of EU common standards. Although "body scanners are not the panacea for airline security" – added Mr Kallas – EU citizens' fear "must be addressed" and he called for common rules to be adopted.<sup>12</sup>
7. In the light of these developments, the HIDE and RISE projects decided to undertake an inquiry into the ethical and policy context of the adoption of WBI technology at airport check-points in Europe. The Coordinator of the two projects, Prof. Emilio Mordini, and the staff at the Centre for Science, Society and Citizenship, took the responsibility to physically write this report. Some of the questions we sought to answer included:
  - What do we know about the likely health and privacy impact of WBI technology?
  - To what extent do WBI for people screening in airports comply with the Charter of Fundamental Rights and respect for privacy?
  - What technical provisions (if any) are necessary to make WBI consistent with ethical and privacy principles?
  - What is the appropriate level of governance for WBI?
8. We acknowledge that many of these questions are far reaching, and that finding answers to them may not be easy. With this policy report, the HIDE and RISE projects aim to contribute to the wider debate on WBI launched by the European Commission, and to convey some messages to European policy makers.

---

<sup>11</sup> EU-US Joint Declaration on Aviation Security,  
<http://www.eu2010.es/en/documentosynoticias/otrasdeclarac/jaieuusa.html>

<sup>12</sup> EP Hearings , Summary of the hearing of Siim Kallas -Transport

TIMELINE OF MAIN EVENTS	
1992	The first X-ray backscatter (The Secure 1000) is developed by Steve Smith
2002	Backscatters are tested in a few US airports for secondary screening
2002	MM-waves machines are tested in UK at Gatwick Airport
2004	Backscatters are tested in UK at Heathrow Airport
2004	US National Council on Radiation Protection and Measurements, <i>Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems</i>
2006	Final report of the FP5 project “Tera-Hertz radiation in Biological Research, Investigation on Diagnostics and study of potential Genotoxic Effects”
2007	Committee on Assessment of Security Technologies for Transportation of the US National Research Council, <i>Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons</i>
2007	MM-waves are tested in NL at Schipol Airport
2007	Backscatters are tested in Finland
2007	The US TSA starts piloting MM-wave technology in 19 US airports
Oct 2008	US Department of Homeland Security, <i>Privacy Impact Assessment for Whole Body Imaging</i>
Oct 2008	Draft EC Regulation 300/2008 on aviation security including body scanner as allowed screening method
Oct 2008	EP Resolution of the 23 October 2008 calls for a full ethical and legal impact assessment of WBI prior of their adoption
Dec 2008	The EC launches the public consultation <i>The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection</i> and set up a “Body Scanners Task Force”
Feb 2009	MM-wave systems are used in lieu of WTMD in six of the biggest US airports, in order to evaluate the operational efficiency of WBI for primary screening.
Feb 2009	Joint Opinion on body scanner issued by the Art.29 Working Party and the European Data Protection Supervisor
March 2009	Privacy Commissioner of Ontario, <i>Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy</i>
March 2009	EC Regulation 300/2008 on aviation security is approved by the EP. The chapter on “methods of screening allowed” is suppressed.
Oct 2009	Canadian Air Transport Security Authority, <i>Privacy Impact Assessment in anticipation of the deployment of MM-Wave technology at selected Canadian airport</i>
12/24/09	Failed Christmas day attack
Jan 2010	The US TSA orders 300 WBI machines to be employed in US airports. Some EU MSs declare their will to adopt a similar decision (e.g., UK, NL, FR, IT), while others remain uncommitted (e.g., FL, ES, DE)
Jan 2010	US Government Accountability Office (GAO), <i>Homeland Security: Better Use of Terrorist Watch list Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security</i>
14 Jan 2010	Confirmation hearing of Commissioner Siim Kallas, who backs the idea of a single EU regulation on body scanners and deplors that some MSs use WBI in the absence of EU common standards
21 Jan, 2010	EU-US jointly declaration on aviation security stating that “enhanced technologies” will be used to identify the illicit materials that people may be carrying
28 Jan 2010	EC Commissioner responsible for Justice, Fundamental Rights and Citizenship, Viviane Reding, declares that “I cannot imagine this privacy-intrusive technique being imposed on us without full consideration of its impact”
Feb 2010	UK Department for Transport, <i>Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology</i>

## CHAPTER 2: THE TECHNOLOGICAL CONTEXT

---

### Technologies and Systems

9. Whole Body Imaging is an umbrella term that includes various technologies that can produce images of the body without the cover of clothing. These screening systems increase the threat detection spectrum from weapons and “single threats” to “multi” or “all-threats”, including explosives, and even biological and nuclear contaminants. All WBI technologies can detect metallic objects, plastic and ceramic weapons, explosives and other threats hidden beneath the clothes without the need of a pat down or strip search: they can indeed reveal types of material that a conventional WTMD can’t detect - such as prohibited non-metallic items, which at present, can be found only through hand searching procedures. Another important asset of a WBI system is that – at least theoretically - it provides a comprehensive body search in just a few seconds.
10. There are two main categories of WBI<sup>13</sup>: “walk-in” cabinets, which scan one person at a time; and “stand-off” scanners, which are pointed at crowds. In their turn, each category can use different technologies, based on different kinds of electromagnetic waves. The walk-in systems typically use the reflection of the waves off the skin to detect any unusual shapes on the body. They are active systems, say, they project beams on the subject. Stand-off scanners can be either active or passive (passive systems collect waves emitted, or reflected from the environment, by the body). WBI systems include various technologies with different levels of maturity. Technologies at validation and demonstration phases include *ultrasound imagers*, *SQUID* and *quadrupole resonance analyzers*, *T-ray imagers*. More mature technologies include millimetre-wave holographic imagers, and x-ray scanning systems.
11. **Ultrasonic imaging technology** is largely used in medicine to investigate internal organs (for such an application it must work in contact mode). For security purposes ultrasounds are widely used for object detection and motion detection.<sup>14</sup> Ultrasonic detectors for remote detection of concealed weapons have also been commercialized<sup>15</sup>. JAYCOR has recently developed and demonstrated an Ultrasound Imaging Sensor for detecting and imaging weapons concealed under a person's clothing. The sensor includes a source of high-power

---

<sup>13</sup> [www.newscientist.com/article/dn18343-deployment-of-airport-full-body-scanners-could-be-delayed.html](http://www.newscientist.com/article/dn18343-deployment-of-airport-full-body-scanners-could-be-delayed.html)

<sup>14</sup> NCRP (2004) *Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems* (National Council on Radiation Protection and Measurements, Bethesda, Maryland).

<sup>15</sup> Costianes, P.J. (2005) An overview of concealed weapons detection for homeland security, *Applied Imagery and Pattern Recognition Workshop*. Proceedings. 34th, 5- 6

ultrasounds suitable for remote imaging in air.<sup>16</sup> The producer claims the “sensor can detect metallic and non-metallic weapons concealed on a human body under heavy clothing at ranges up to 8 m and can image concealed weapons at ranges up to 5 m with a centimetre-resolution”<sup>17</sup>.

**12. SQUID**, which stands for *Superconducting Quantum Interference Device*, and **Quadrupole Resonance Analysis**, provide images similar to magnetic resonance imaging. They are currently used chiefly for medical imaging, and are being investigated for the detection of explosives in checked luggage<sup>18</sup>. In principle they could also provide body imaging for security screening purposes, with the advantage of being able to also detect and test different chemicals and substances, including minimal traces of explosives. One potential problem arises from the fact that they can interfere with the function of implanted medical devices (e.g., pacemakers and defibrillators).

**13. T-ray technology**<sup>19</sup> uses electromagnetic radiation from 1,000 GHz to 10,000 GHz, in the so-called tera-band. Terahertz are non-ionizing radiations, thus without the health risks entailed by x-rays. Most T-ray scanners are active systems, say, they emit radiation and detect objects by noting differences in absorption /reflection. Instead a few T-ray scanners, known as passive imagers, rely on the small amount of T-radiation emitted by all warm bodies<sup>20</sup>. They find objects beneath people’s clothing by noting the difference in the amount of radiation emitted between the warm body and the cooler objects. T-ray technology can also detect the nature of hidden objects and materials.<sup>21</sup> Many materials have unique spectral profiles in the terahertz range. This offers the possibility to combine spectral identification with imaging. For instance, plastic explosives reflect terahertz waves in a very specific way, that make them distinguishable from all other materials. T-ray passive systems can be consequently used for "stand-off" scanners, which could remotely detect explosives, and weapons, hidden under clothing by an individual in a crowd. Most current T-ray imagers are still short-range (a few metres) and spectroscopy is often too slow for real life applications<sup>22</sup>. Yet technologists predict that T-ray scanners that can do both imaging and spectroscopy at 50 meters or more will be available within five years.

---

<sup>16</sup> Felber FS, and al. (1996), Fusion of radar and ultrasound sensors for concealed weapons detection, in *SPIE Proceedings Vol. 275, Signal Processing, Sensor Fusion, and Target Recognition*, Ivan Kadar; Vibeke Libby, Editors, pp.514-521

<sup>17</sup> [http://www.jaycor.com/eme\\_sens\\_ultra.htm](http://www.jaycor.com/eme_sens_ultra.htm)

<sup>18</sup> [www.securitymanagement.com/article/new-views-airport-screening-004586?page=0%2C2](http://www.securitymanagement.com/article/new-views-airport-screening-004586?page=0%2C2)

<sup>19</sup> Costianes, P.J. (2005), *ibid.*

<sup>20</sup> Zandonella C (2003), Terahertz imaging: T-ray specs *Nature* 424, 721-722 (14 August 2003) | doi:10.1038/424721a

<sup>21</sup> Committee on Assessment of Security Technologies for Transportation (2007) *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapon*, National Academies Press

<sup>22</sup> *Thruvision Systems* sells scanners (T5000 and T8000) that can be used effectively when the person being screened is between 6 m and 25 m away., yet these devices lack spectroscopy capacities <http://www.thruvision.com/index.html>



- 14. Millimeter Wave (MM-wave) Technology** is based on radiation belonging to the millimetre (from 30 GHz to 300 GHz) and submillimetre (from 300 GHz to 1,000 GHz) regions of the electromagnetic band.<sup>23</sup> Imaging technologies can be either passive or active. **Active MM-wave systems** use non ionizing radio frequency energy to generate an image based on the energy reflected from the body.<sup>24</sup> The waves penetrate clothing but are reflected from the skin and other objects. The three dimensional image resembles a photograph negative. **Passive MM-wave systems** are used to scan remotely, overtly or covertly, large numbers of people as they move in a continual stream through restricted or controlled areas, such as border checkpoints, airport terminals, or outdoor arenas<sup>25</sup>. Images are low resolution body images in which clothing and other materials appear transparent. Some passive systems (e.g., a scanner called SPO, produced by the UK company Qinetiq) activate warning messages when they detect any concealed object.<sup>26</sup> MM-wave receivers can also be coupled with infrared receivers. The two receivers used in tandem, and linked with a computer imaging system, would have a higher discriminating power than MM-wave passive system alone.<sup>27</sup>
- 15.** MM-wave technology also includes a technology consisting of arrays of **microwave dielectrometers** in a portal (*People Portal Full Body Scanner*, produced by the US company Global Security Solutions).<sup>28</sup> The system performs and maps a large number of measurements, which are compared to expected values in order to detect extraneous objects. A material's density and absorption abilities are the criteria for making the decision to declare a material 'offensive'. According to the producer, "the computer takes no action as long as the instant information compares favorably with that stored in the computer. The definition of 'favorable' is operator selectable as the systems sensitivity adjustment. If, during the scanning process, the computer detects an unfavorable comparison it red flags the offending location upon a generic wire-frame figure". This would imply that "unlike competing technologies, no picture of an individual's actual anatomy is ever produced, seen or exhibited. The operator sees only a wire-frame image indicating by red arrows the exact location of the anomalies".
- 16. X-ray scanning systems** include backscatter systems and transmission systems. **X-ray backscatter systems** use low intensity x-rays scanned over the body surface, and reflected back from the body. Backscatter produces a narrow beam that scans the subject at high speed ("flying spot") left to right and top to

---

<sup>23</sup> Costianes, P.J. (2005), *ibid.*

<sup>24</sup> Committee on Assessment of Security Technologies for Transportation (2007), *ibid.*

<sup>25</sup> Duncan WD et al. (2008), An Optical System for Body Imaging from a Distance Using Near-TeraHertz Frequencies, *Journal of Low Temperature Physics*, 151, 3:777-783  
<http://www.springerlink.com/content/j3w220228n21v1g5>

<sup>26</sup> <http://www.qinetiq.com/home/aboutqq.html>

<sup>27</sup> Currie NC, et al. (1996) Infrared and millimeter-wave sensors for military special operations and law enforcement applications, *International Journal of Infrared and Millimeter Waves*, 17, 7:1117-1138 <http://www.springerlink.com/content/t7t70184np215897>

<sup>28</sup> Appleby R, Wikner DA (2007) Passive Millimeter-Wave Imaging Technology, *Proceedings of SPIE* Volume: 6548



bottom. Most of the radiation is scattered near the surface of the skin, this makes the system effective in imaging objects hidden under clothing. The low intensity x rays can hardly penetrate through the skin and cannot detect objects hidden in body cavities. A typical scan lasts about eight seconds, during which a person is scanned twice, once from the front and once from the back. The resulting image is a two dimensional one, similar to a chalk etching.<sup>29</sup> Backscatter X-ray can be also used for partial body scanner to screen persons with casts, bandages and prosthetic limbs for concealed weapons and contraband<sup>30</sup>. Backscatter permits rapid inspection without imposing too much stress, and discomfort to the disabled person. **Transmission systems** are closer to medical x-rays, in the sense that the radiation traverses through the body. Transmission systems can detect objects that have been swallowed or hidden in body cavities and have been used to screen workers in diamond mines in order to replace orifice search.<sup>31</sup>

### **Trials and Standards**

17. The first WBI machines using backscatter technology were deployed in 2002<sup>32</sup> in a few US airports. In February 2007, the US TSA decided to test WBI as an “*alternative to personal searches for secondary screening*”<sup>33</sup>. The initial test involved systems based on x-ray backscatter technology, used for passengers selected for additional screening. In October 2007 the TSA started piloting the MM-wave technology in 19 US airports. In February 2009, the TSA started piloting MM-wave systems *in lieu* of WTMD in six of the biggest US airports<sup>34</sup>, in order to evaluate the operational efficiency of WBI *for primary screening*<sup>35</sup>.
18. In Europe, the technology was first tested in London airports, in Amsterdam’s Schiphol and Helsinki’s Vantaa. In the UK, MM-waves were tested at Gatwick in 2002 and backscatters at Heathrow on October 2004<sup>36</sup>, as part of an initiative of the Department of Transport over a three year period. Passengers sorted out for enhanced inspection had the option of a standard pat-down search or a scan with the WBI technology, and the latter was selected by approximately 90% of passengers. On February 6<sup>th</sup> 2009, Rapiscan Systems announced that it had received an order from the British Airport Association to purchase the three backscatter machines that were used in the trial<sup>37</sup>. In the Netherlands, at

---

<sup>29</sup> NCRP (2004), *ibid*.

<sup>30</sup> <http://www.tek84.com/castscope.html>

<sup>31</sup> Smit KJ (2003), *Regulatory Control of X-ray Equipment Used in the Mining Industry in South Africa to Screen Workers for Security Purposes*. Proceedings 35th National Conference on Radiation Control, (South Africa Department of Health, Bellville, South Africa), quoted by NCRP (2004), *ibid*.

<sup>32</sup> Masterson U (2010), *Airports seek hi-tech security*, <http://www.msnbc.msn.com/id/3071573>

<sup>33</sup> See David Biello, “The Naked Truth: is New Passenger Scanner a Terrorist Trap or Virtual Strip Search?”, *Scientific American*, March 1st 2007.

<sup>34</sup> San Francisco, Miami, Albuquerque, Tulsa, Salt Lake City and Las Vegas.

<sup>35</sup> However passengers could still opt for standard procedures through WTMD and physical inspection, [http://www.tsa.gov/press/happenings/mwave\\_continues.shtm](http://www.tsa.gov/press/happenings/mwave_continues.shtm)

<sup>36</sup> D. Gadher, *Plane Passengers shocked by their x-ray scans*, *The Sunday Times*, November 7, 2004

<sup>37</sup> See the Rapiscan release available at <http://www.securityinfowatch.com/root+level/1279579>

Schiphol Airport a trial with three active MM-wave scanners started in May 2007. Passengers could select between WBI and standard procedures. Most persons, from 85 to 90 %, accepted the scanner, as *“a more client friendly procedure”*<sup>38</sup>. Finally, in Finland, one WBI system has been tested at Helsinki Vantaa Airport *“during the busiest periods in the mornings and evenings since 7 November 2007”* according to a Finavia release<sup>39</sup>.

19. To date there is not a common European legal and ethical framework for WBI trials in airports.
20. Millimetre wave scanners are more frequently deployed at airports rather than backscatter systems for two main reasons: they generate non-ionizing radiation and consequently they pose minimal health risks, and they are faster passenger processing machines<sup>40</sup>. According to the US Transportation Security Administration (TSA)<sup>41</sup>, WBI speeds up the overall scanning process, as *“it takes a passenger about 15 seconds to undergo the screening, as opposed to the several minute pat down procedure”*<sup>42</sup>. According to a report on trials at Schiphol Airport<sup>43</sup>, one of their main weakness was the false alarm rate, which was very high (about 50%), mainly due to objects forgotten in the pockets.
21. WBI also reduces the need of hand searches, making the process less embarrassing and intrusive. However, since both MM-wave and backscatter devices create images showing the surface of the skin and revealing objects that are on the body, and not inside the body, they can't replace body orifice search.
22. To date no WBI has ever been certified by national governments, neither in the US or the EU, and there are no international standards about WBI. The certification problem gets still more complicated because of the number of different technologies and systems.

### Needs addressed by WBI

23. According to the European Economical and Social Committee (EESC) opinion on *Aviation security for passengers*<sup>44</sup>, adopted at its 448<sup>th</sup> plenary session, *“considering the significant increase of passengers travelling by air forecast for the upcoming years, the current security screening of passengers and luggage*

---

<sup>38</sup> Schiphol airport website.

<sup>39</sup> Available at [http://www.finavia.fi/finavia\\_release?id=69470](http://www.finavia.fi/finavia_release?id=69470) . Finavia is the managing body of 25 airports in Finland.

<sup>40</sup> Ontario Information and Privacy Commissioner white paper on *“Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy”*, March 2009

<sup>41</sup> A component of the Department of Homeland Security, created by the Aviation and Transportation Security Act (ATSA) two month after the September 11 attacks.

<sup>42</sup> See [www.tsa.gov](http://www.tsa.gov)

<sup>43</sup> See <http://www.homelandsecurityresearch.net/2009/04/27/schiphol-airport-security-new-screening-technologies-designed-to-improve-passenger-and-luggage-screening>

<sup>44</sup> OJ C 100, 30.04.2009, *“Opinion of the European Economic and Social Committee (EESC) on Aviation Security for Passengers”*, p.41.

does not propose a sustainable model” (art. 6.1). Improving aviation security, notably the detection of prohibited items, while softening the “burdensome process”<sup>45</sup> of people screening is a worldwide priority in airport management.

24. Today passengers who have to undergo to full-body pat down belong to two broad categories: 1) they are passengers holding passports from countries included in a (unofficial) list for enhanced screening, or taking flights that originated or passed through any of these countries; or 2) they have set off the metal detector alarm. As more people have surgical implants (e.g., hip replacements, prosthetics, cardiac implants, etc) and more people are travelling from and through “risky” countries, the number of people who need to undergo to physical search is increasing.
25. Hand searches are time-consuming (they take from two to four minutes) and labour-intensive procedures. They are also only partly effective. In order to perform appropriate pat down search, screeners must avoid touching sensitive areas (e.g., genitalia, breast, etc.) with anything except for the back of the hand and any excessive squeezing or groping of sensitive areas. They must also avoid requiring a passenger to expose private areas of the body, and there is indeed evidence that physical pat-down is not effective in locating items concealed in sensitive body areas<sup>46</sup>. As a consequence – although no systematic studies are available – it is realistic to argue that pat downs can be unreliable.
26. There is also anecdotal evidence that passengers feel pat-down procedures embarrassing and invasive because they involve screeners touching people near sensitive body areas. In particular female travellers have been complaining about pat-downs. Although very specific guidelines and boundaries have been established by national airport authorities, inappropriate pat-down searches are still episodically reported.

### CHAPTER 3: HEALTH AND PRIVACY IMPACT ASSESSMENT

---

27. Further to the EP Resolution of 23 October 2008, the EC public consultation on body scanners (January-March 2009) and the EU-US Joint Declaration on Aviation Security of Toledo ( Jan 21, 2010), the EC Commissioner responsible for Justice, Fundamental Rights and Citizenship, Ms Viviane Reding, declared before the Parliament (keynote speech at the Data Protection Day on 28 January 2010) that “body scanners have a considerable privacy-invasive potential. Their usefulness is still to be proven. Their impact on health has not yet been fully assessed. Therefore I cannot imagine this privacy-intrusive technique being imposed on us without full consideration of its impact”.<sup>47</sup> Earlier, during the

---

<sup>45</sup> Ibid.

<sup>46</sup> United States Government Accountability Office, *Vulnerabilities Exposed Through Covert Testing of TSA’s Passenger Screening Process*, [http://www.tsa.gov/assets/pdf/gao\\_report.pdf](http://www.tsa.gov/assets/pdf/gao_report.pdf)

<sup>47</sup> <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en>

parliamentary confirmation hearing, Ms Reding had also told that scans must be voluntary, not mandatory, and authorities should guarantee that these systems pose no health hazard and their images must be quickly destroyed.<sup>48</sup>

28. As per x-ray scanning systems, the reference document is the **1990 Recommendations of the International Commission on Radiological Protection**, issued by the *International Commission on Radiological Protection (ICRP)* in 1991<sup>49</sup>, which states that “In radiation protection, no exposure is *justified* unless it produces a positive net benefit”. This philosophy “is part of radiation protection regulations of all agencies in the United States and the European Union and is almost universally adopted throughout the world. In the case of screening passengers, visitors, or prisoners, the benefit is increased security and the possibility of preventing terrorist attacks”.<sup>50</sup> One of the first comprehensive reports assessing health impact of x-ray scanning systems was the **Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems** published in 2004 by the *US National Council on Radiation Protection and Measurements*<sup>51</sup>. The report recommends that scanning systems that utilize ionizing radiation are classified into two broad categories: *general use systems* (e.g., backscatter systems) and *limited-use systems* (e.g., transmission systems). “*General-use systems* should adhere to an effective dose of 0.1 µSv or less per scan, and can be used mostly without regard to the number of individuals scanned or the number of scans per individual in a year [...] *Limited-use systems* include all other ionizing radiation scanning systems that require effective doses per scan greater than 0.1 µSv and less than or equal to 10 µSv. These systems should be used with discretion in terms of the number of individuals scanned and the number of scans per individual in a year”.
29. Although a recent study<sup>52</sup> indicates that tera radiations could lead to DNA instability, to date there is no evidence that they could damage biological tissues, on the contrary other evidences show that they cannot. The reference study is the final report of **THz-BRIDGE - Tera-Hertz radiation in Biological Research, Investigation on Diagnostics and study of potential Genotoxic Effects**,<sup>53</sup> a project funded in the scope of the EC FP5 Quality of Life. Aim of THz-BRIDGE was to investigate the potential damage of electromagnetic radiation on biological systems in the millimetre, submillimetre, and tera spectral ranges. After three years research, the project established the safety of millimeter-wavelength/terahertz energy. On the basis of *THz- BRIDGE*, in 2007, the *Committee on Assessment of Security Technologies for Transportation of the US*

---

<sup>48</sup> EP Hearings, Summary of hearing of Viviane Reding - Justice, fundamental rights and citizenship

<sup>49</sup> ICRP Publication No. 60, 1991, *Annals of the ICRP* 21(1-3).

<sup>50</sup> Health Physics Society (2205) *Screening Individuals with Backscatter X-Ray Systems*  
<http://www.hps.org/hpssc/N43Status.html>

<sup>51</sup> <http://www.ncrppublications.org/>

<sup>52</sup> Alexandrov B. S., et al. (2010), DNA Breathing Dynamics in the Presence of a Terahertz Field.  
*Physics Letters A*, 374, 10: <http://arxiv.org/abs/0910.5294>

<sup>53</sup> <http://www.frascati.enea.it/THz-BRIDGE/>

National Research Council published the report **Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons**,<sup>54</sup> which addresses MM-wave and T-ray scanning systems. The report concludes that “Millimeter-wavelength/terahertz technology has potential for contributing to overall aviation security, but its limitations need to be recognized. It will be most effective when used in conjunction with sensor technologies that provide detection capabilities in additional frequency regions”. The report also recommends that “as with x-ray-based passenger imaging, the TSA needs to address issues associated with personal privacy raised by millimeter-wave/terahertz imaging”.

30. Eventually in October 2008, the first comprehensive **Privacy Impact Assessment for Whole Body Imaging** was published by the *US Department of Homeland Security*.<sup>55</sup> The report examines WBI used in the TSA pilot program in the light of the Fair Information Practice Principles (FIPPs). In particular the report focuses on the operating protocol, notably;

- *Sample images are available to individuals at the location of the WBI device to show the image to individuals deciding whether they choose the WBI visual inspection instead of the physical pat down inspection.*
- *Transportation Security Officer (TSO) viewing the image is isolated from the TSO interacting with the individual. The TSO viewing the image communicates with the TSO at the checkpoint through a red/green light system, or via radio, or by highlight an anomaly location on a generic figure that is displayed on a monitor that the checkpoint TSO can read. The TSO at the checkpoint then conducts a physical pat-down that is focused on the particular area and not necessarily of the individual’s entire body.*
- *The image does not present sufficient details to be used for personal identification.*
- *The image storage functions is disabled by the manufacturer before the devices are placed in an airport and cannot be activated by operators. Images are maintained on the screen only for as long as it takes to resolve any anomalies. The equipment does not retain the image.*
- *TSOs are prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras.*
- *Rules governing the operating procedures are documented in standard operating procedures (SOP), and compliance with these procedures is reviewed on a routine basis.*

The report ends by stating that “WBI technology used in the pilot program has the potential to improve threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical pat-down is uncomfortable. The operating protocols of remote viewing and no image retention are strong privacy protections that permit security benefits to be achieved”.

---

<sup>54</sup> *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons* <http://www.nap.edu/catalog/11826.html>

<sup>55</sup> US DHS, Privacy Impact Assessment for TSA Whole Body Imaging October 17, 2008

31. Between December 2008 and March 2009, the EC DIRECTORATE GENERAL FOR ENERGY AND TRANSPORT (DG TREN) carried out a public consultation on ***The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection.***<sup>56</sup> After stating that “the quality of hand searches is very variable at Community airports, as has been seen by the Commission as part of its compliance monitoring programme of airport inspections” and that “passengers often find hand searches intrusive and upsetting to their dignity”, and that “hand searching of passengers is time-consuming and labour-intensive”, the document asks whether body scanners could be used as an alternative to the existing means of screening passengers. Other crucial questions posed by the consultation document concern fundamental rights (“Respect for privacy, human dignity as well as protection of personal data are the fundamental rights most often discussed in relation to body scanners. Are there any other fundamental rights that in your opinion could be affected [...] by the use of body scanners?”), whether personal data of individuals are being processed by WBI systems, eventually whether the use of Privacy Enhancing Technologies (PETs) can help facilitate compliance with data protection rules.
32. On February 2009 the *Art.29 Working Party* (Art.29 WP) and the *European Data Protection Supervisor* (EDPS) jointly answered the consultation document with an opinion on ***The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection.***<sup>57</sup> In the accompanying letter addressed to Mr D.Calleja Crespo, Director Air Transport at DG TREN, Mr A. Türk, Art.29 WP Chairman, expresses a “strong reservation towards body scanners as described in your questionnaire. Aviation security is a legitimate aim but the use of any devices to be introduced in addition to already existing walk through metal detectors (WTMD) and hand scanners needs to be based on sound evidence as to why they are needed and why existing measures are not sufficient [...]. The use of body scanners could only be considered as proportionate if an acceptable balance is struck between their necessity and their effectiveness on the one hand and their impact on the privacy of passengers on the other hand.”<sup>58</sup> The opinion starts by arguing that it is not appropriate to describe “body scanners as an alternative to hand searches as an individual will still need to undergo a hand search if the scanner detects an anomalous object” Further to this argument, counter intuitively the document contends that “making body scanners voluntary undermines the reasons for needing them”. Indeed “giving a choice to the individual might at first sight appear as a more balanced solution but raises serious questions as to the effective necessity and efficiency of body scanners”, which can be justified only on the basis of their absolute necessity. The documents also stresses that “while assessing the necessity of body scanners, a distinction should be made between their *convenience* (gain in time) and their added value in terms of *security*

---

<sup>56</sup> [http://ec.europa.eu/transport/air/consultations/doc/2009\\_02\\_19\\_body\\_scanners\\_questionnaire.pdf](http://ec.europa.eu/transport/air/consultations/doc/2009_02_19_body_scanners_questionnaire.pdf)

<sup>57</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009-others\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm)

<sup>58</sup> <http://ec.europa.eu/justicehome/fsj/privacy/indexen.htm>



(capacity to detect concealed threat objects)”, with only the latter being a valid justification for routine use of WBI technology. For the same reason, Data Protection authorities reject that certain categories of persons (e.g. minors, pregnant women, disabled persons) might be automatically exempted from body scanner. “Excluding some individuals from the screening, whatever the reason (just as giving a choice to the individual), puts into question the real necessity of the system, as any *mala fide* person could use such exemption to bypass the control”. As per issues related the informational intrusiveness of WBI, the Art.29 WP and the EDPS substantially reflect the *Privacy Impact Assessment for Whole Body Imaging* published by the US Department of Homeland Security, but for considering the use of a body scanner as processing personal data (the US DHS PIA denied that body scanner images could be considered personal data, since they would not be any more linkable to an identifiable individual). The document ends by requesting the use of privacy enhancing technologies, notably the “privacy by design” approach, defined as “*the first and essential requirement in the development of body scanners*”.

33. The *Information and Privacy Commissioner of Ontario*, Ms Ann Cavoukian, reached similar conclusions in her privacy impact assessment of WBI systems, published in March 2009, ***Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy***. Also Ms Cavoukian advocates “privacy algorithms” with the main goal of eliminating “*from the imagery all human features that may be considered too intrusive*”<sup>59</sup>. Privacy algorithms, privacy filters, obfuscation, and privacy by design delineate the integrated approach proposed by Ms Cavoukian, who ends her document by stating “Whole Body Imaging technologies that incorporate strong privacy filters – rendering bodily images to mere outlines, to front-line screeners, can deliver privacy-protective security. When combined with appropriate viewing, usage and retention policies, privacy algorithms that obscure personal details, while still allowing potentially threatening concealed objects to be revealed, will allow WBI implementations to satisfy security requirements without sacrificing (and perhaps enhancing) passenger privacy. We believe that this positive-sum paradigm can, and should be, the end goal of such airport security passenger screening technologies – security *and* privacy, not one at the expense of the other”.<sup>60</sup>
34. In October 2009, the *Canadian Air Transport Security Authority* (CATSA) completed a **Privacy Impact Assessment in anticipation of the deployment of MM-Wave technology at selected Canadian airports**. The report concludes that “CATSA is addressing all risks with risk mitigation strategies that are in line with privacy best practices including:

- *making the mm Wave Imager screening process voluntary and anonymous;*

---

<sup>59</sup> Keller P, *Privacy Algorithm for Airport Passenger Screening Portal*, Applications and Science of Computational Intelligence III (1999), Vol. 4055, pp. 476-483.

<sup>60</sup> Ann Cavoukian, *Information and Privacy Commissioner of Ontario*, “Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy”, March 2009.

- ensuring that the images are immediately and permanently deleted once the screening process is complete;
- ensuring that the mm Wave Imager cannot store, print or save the images.
- ensuring that the images reviewed during the screening process cannot be accessed by or transmitted to any other location;
- ensuring that the images are exclusively reviewed by a Screening Officer located in a remote viewing room;
- not correlating the images in any way with the name of the passenger or any other identifying information”<sup>61</sup>

35. In reply to the PIA carried out by the CATSA, the *Canadian Office of the Privacy Commissioner (OPC)* sent a **Letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA)**.<sup>62</sup>

The letter raises various interesting issues, notably about the need to introduce WBI technology: “we continue to urge CATSA to regularly scrutinize implementation of MMW screening technology and justify it against the following four-part test:

- *Is the measure demonstrably necessary to meet a specific need?*
- *Is it likely to be effective in meeting that need?*
- *Is the loss of privacy proportional to the need?*
- *Is there a less privacy-invasive way of achieving the same end?”*

The letter concludes by recommending that “CATSA regularly review its perceived need for WBI screening against updated aviation security threat/risk assessments, as well as against enhancements or refinements to the available technology, such as improved privacy filtering software. New or alternative technologies to achieve the same screening goals in a less privacy-invasive manner should also be considered”. The OPC also suggests that MM-wave technology is used “only as a secondary screening tool, and then, only as a voluntary option to a traveller undergoing a physical pat-down.”

36. The issue of security threat/risk assessments is also addressed in a 2010 report prepared by the *US Government Accountability Office (GAO)* on request of the House Committee on Homeland Security, in the aftermath of the failed 25 December attack, **Homeland Security: Better Use of Terrorist Watch list Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security**.<sup>63</sup> The main argument raised by the document is that to date we still lack an assessment of WBI’s vulnerabilities to determine the extent to which a terrorist could carry out an attack which could evade detection by WBI.

37. On February 1, 2010, the *UK Department for Transport* made public an **Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology** covering privacy, health and safety, data protection and equality issues. The

---

<sup>61</sup> <http://catsa.gc.ca/File/Library/59/English/PIA%20summary.pdf>

<sup>62</sup> [http://www.priv.gc.ca/pia-efvp/let\\_20100108\\_e.cfm](http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm)

<sup>63</sup> GAO-10-401T, January 27, 2010, <http://www.gao.gov/products/GAO-10-401T>



Code requires airports to undertake scanning sensitively, having regard to the rights of passengers. The Department also announced the intention to launch a full public consultation on the requirements relating to the use of body scanners in order to finalize a Final Code of Practice by the end of 2010.<sup>64</sup> The Interim Codes describes WBI operating procedures and privacy requirements, which include separation between the screener (who sees the body image) and the security officer (who supervises the checkpoint), no retention of the image, possibility for the person selected for scanning to request that the screen reader is of the same sex as the person. The code also explicitly affirms that “Passengers must not be selected on the basis of personal characteristics (i.e. on a basis that may constitute discrimination such as gender, age, race or ethnic origin)”.<sup>65</sup>

## CHAPTER 4: BODILY INTEGRITY

---

- 38.** The human body - its legal and moral status, its value, its meanings, and the way in which technologies modify it - lies at the heart of the body scanner debate. The notion of “body” is much more metaphysical than people usually think. What is the body? Say, what is the body “alone”, without “its” mind? The body isolated is just a corpse.<sup>66</sup> Indeed what we call “human body” is a sophisticated metaphysical concept<sup>67</sup>, which results from the binary opposition of mind / body rooted in Platonic dualism, late Greek philosophy, Christian theology, and Cartesianism. The idea of body is a simulation and a partial model, which splits in two the polysemic and ambiguous nature of the human subject. In other words, the concept of body is *a way of seeing* actual human beings. Biomedical practices separate mind and body, and keep the body as a medium of disease. A similar operation is carried out by current security practices, which tend to dissolve the subject into risk categories. The overseer's gaze observes and explores the human body as a source of risks, as a potential threat. The human body under surveillance becomes “an assemblage comprised of myriad component parts and processes which are broken down for purposes of

---

<sup>64</sup> <http://www.dft.gov.uk/press/speechesstatements/statements/adonis20100201>

<sup>65</sup> UK Dept. for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment*, <http://www.dft.gov.uk/pgr/security/aviation/airport/>

<sup>66</sup> “The corpse is, if you will, a dream about the body which, as we have said, imagines the body as dis-membered in two ways. On one hand, this dream is a way of imagining the body as isolated or cut off from its natural context or situation. On the other hand, this dream is a way of imagining the body as fragmented within itself, as a specimen” Romanyshyn R, (1989) *Technology as Symptom and Dream*. New York: Routledge, p.119

<sup>67</sup> The terms psyche and soma were already present in Homer, but with a different meaning: soma indicated the corpse, the dead body, while psyche was the vital breath. Even the biblical tradition ignored concepts like soul, body, spirit. *Nefesh*, then translated psyche, expressed the fragility of the human being, his desire, his incompleteness. *Basar* was not the body, but the weakness of the man who denies God. A man is flesh enlivened by God, away from God he becomes futility and impotence.

observation”.<sup>68</sup> Such a “securitized” body is mirrored by the suicide terrorist’s body being turned into a weapon: both the securitized and the terrorist’s bodies are highly symbolic constructions, whose meanings go well beyond their mere physical reality. The human body is a symbolic field and should be studied as such.<sup>69</sup>

#### KEY MESSAGE TO POLICY MAKERS

Practices which concern the body are unavoidably invested with cultural values, and in their turn produce new values. WBI impact assessment should consider the symbolic dimension, which is often more relevant to policy setting than conventional technology assessment.

39. Bodily issues associated to the adoption of body scanners at airport checkpoints, include various kinds of violation of body integrity. The word integrity literally means “the quality or state of being complete or undivided”. Physical and mental integrity thus refers to the inviolability of a person’s body and mind, say, it refers to the right against being touched (in physical and metaphorical senses) without consent. Historically, the notion of body integrity comes from the legal conception of *Habeas Corpus* (Latin: you shall have the body), originally the legal action through which a person can seek protection against an unlawful detention. The *Habeas Corpus* affirms the right not to be imprisoned arbitrarily and to not have the body violated in any other way (e.g., physical inspection, torture, abusive treatments, and so on). “The violation of the right to physical and psychological integrity of persons is a category of violation that has several gradations and embraces treatment ranging from torture to other types of humiliation or cruel, inhuman or degrading treatment with varying degrees of physical and psychological effects caused by endogenous and exogenous factors which must be proven in each specific case”.<sup>70</sup> Body integrity is threatened by physical pain, injuries, sexual assaults, rape, physical inspections, and the like. Mental integrity is violated any time when emotional and cognitive processes are brutally invaded, abused and/or disrupted.

#### Dignity and Physical Privacy

40. We all have an interest in protecting our physical or mental integrity. This is clearly expressed by the ***Universal Declaration of Human Rights*** (art.3) which states that everyone has a right to the inviolability of his or her person, and by the ***Convention on Human Rights and Biomedicine***<sup>71</sup> (art.1), which states that “Parties to this Convention shall protect the dignity and identity of all human

<sup>68</sup> Haggerty KD, Ericson RV (2000), The Surveillance Assemblage, *British Journal of Sociology*, 51, 4, 605–622

<sup>69</sup> Slattery DP, (1994), Of corpses and kings: Antigone and the body politic, *Lit: Literature Interpretation Theory*, 5, 2: 155 – 167

<sup>70</sup> Inter-American Court of Human Rights, *Loayza Tamayo Case*, Judgment of Sept. 17, 1997 (Ser. C) No. 33, para. 57, <http://www1.umn.edu/humanrts/iachr/C/42-ing.html>

<sup>71</sup> The concept of body integrity has important applications in the biomedical sphere, where inter alia it requires that invasive actions cannot be lifted without the informed consent of the patient.

beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine". The principle of body integrity does not concern only violations of the body resulting in suffering or in adverse health conditions, but it also deals with intrusions without harmful effects. This leads to an additional issue, which is particularly relevant to the body scanner debate. Does a bodily or psychological intrusion constitute a violation of integrity only if it is perceived as such? Or, on the contrary, are there objective criteria to establish when a violation infringes the right to integrity? Indeed the principle of the "inviolability of the body" includes two cognate, but different,<sup>72</sup> concepts: 1) the view "that the body is a 'sacredness' in the biological order"<sup>73</sup>; and 2) the view of the body as personal property, whose borders cannot be trespassed without the owner's consent. There are then two diverse perspectives about body integrity, the former contends that the right to be free from bodily (and mental) intrusion is inherently part of the notion of human dignity<sup>74</sup>, the latter maintains that bodily integrity is the right of "every human being ... to determine what shall be done with his own body"<sup>75</sup> and to protect his physical privacy. While the dignitarian approach usually contends that body integrity is – at least in part – an objective concept, the privacy approach emphasises the subjective aspect of body integrity, which always implies the notion of consent (or lack of) to the intrusion.

41. The tension between dignitarian and privacy interpretations of body integrity is well illustrated by the Dutch Constitution (art.11) which states "everyone has a right to untouchability of his body, except for restrictions provided by or valid because of the law". Then, according to Dutch criminal law (art.56), arrested people can be "examined on body and clothes" but only if the examination limits itself to the surface of the body (including natural orifices), while "cutting or pulling hair, drawing blood and obtaining sperm, and taking x-rays are not

---

<sup>72</sup> Actually, together with Giorgio Agamben, one could argue that these two concepts are anything but the two sides of the same coin, being the notion of sacred body only the other side of the notion of body as a property. In his analysis of the *habeas corpus*, Agamben argues that "the root of modern democracy's secret biopolitical calling lies here: he who will appear later as the bearer of rights and, according to a curious oxymoron, as the new sovereign subject (*subiectus superaneus*, in other words, what is below and, at the same time, most elevated) can only be constituted as such through the repetition of the sovereign exception and the isolation of *corpus*, bare life, in himself. If it is true that law needs a body in order to be in force, and if one can speak, in this sense, of "law's desire to have a body," democracy responds to this desire by compelling law to assume the care of this body. This ambiguous (or polar) character of democracy appears even more clearly in the *habeas corpus* if one considers the fact that the same legal procedure that was originally intended to assure the presence of the accused at the trial and, therefore, to keep the accused from avoiding judgment, turns -- in its new and definitive form -- into grounds for the sheriff to detain and exhibit the body of the accused. *Corpus is a two-faced being, the bearer both of subjection to sovereign power and of individual liberties*" (Agamben G, 1988, *Homo Sacer: Sovereign Power and Bare Life*. Stanford UP, Stanford, CA. P 124-125)

<sup>73</sup> Murray TH, (1987), On the Human Body as Property: the Meaning of Embodiment, Markets, and The Need of Strangers, *Journal of Law Reform* 20, 4:1055-1089

<sup>74</sup> See for instance, Maschke KJ, (2003), Proxy Research Consent and the Decisionally Impaired: Science, the Common Good, and Bodily Integrity, *Journal of Disability Policy Studies* 13, 4

<sup>75</sup> Schloendorff v. Society of New York Hospital, 1914, quoted by Maschke KJ, (2003).

warranted”.<sup>76</sup> The law then prohibits the use of any instrument which can penetrate the body surface, conceptualised as a moral and legal border not to be trespassed. It is evident that here there is a tension related to the word “untouchability”, which could refer either to the dignity, the sacredness, of the whole body, or to the notion of ‘body’ as a private property, which is touchable only to the extent that its owner consents.<sup>77</sup>

**42.** A dignitarian interpretation of the notion of body integrity is endorsed by the *Charter of Fundamental Rights of the European Union*, which has an article (art.3), specifically focusing on the *Right to the integrity of the person*, in the first Chapter devoted to Dignity:

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

The context in which art.3 is collocated points out that “the dignity principle should be regarded as a tool to identify the cases in which the body should be absolutely *inviolable*”<sup>78</sup> and that consequently “the principle of inviolability of the body and physical and psychological integrity set out in Article 3 of the Charter of Fundamental Rights rules out any activity that may jeopardise integrity in whole or in part - even with the data subject’s consent.”<sup>79</sup> The respect for body integrity demands that body inviolability is considered – at least in part – a non-negotiable principle. Body integrity is violated any time that an undue and unsolicited intrusion “penetrates” the individual’s personal sphere, independently from whether such an intrusion is tactile, visual, acoustic, psychological, etc. or whether it produces injuries.

**43.** In the US bodily integrity is protected by the Fourth Amendment of the Constitution, which protects physical privacy:

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.

In order to be reasonable a search should meet people’s rational expectations about their right to privacy.<sup>80</sup> Intrusive searches demand specific reasons, might need a warrant, and cannot be a routine procedure. In 2008 the New York State

---

<sup>76</sup> Ten Have HA, Welie JW, (1998) *Ownership of the Human Body Philosophical Considerations*, Springer, p.102

<sup>77</sup> The notion of sacredness implies etymologically that something is untouchable because it belongs to the god. The two notions of dignity and privacy eventually differ only in defining who is the owner of the body, whether the god or the man.

<sup>78</sup> European Group on Ethics in Science and New Technologies (EGE), Op. N° 20, *Ethical aspects of ICT implants in the human body*, Adopted on 16/03/2005

<sup>79</sup> Ibid.

<sup>80</sup> *Katz v. United States*, 389 U.S. 347, 351 (1967)

Court of Appeals (New York State's highest court) discussed the case of Azim Hall, a drug dealer who was stripped and searched by the police and was found to have a string hanging from his anus. The police pulled the string and found a baggie of cocaine inside his rectum. Azim Hall complained that his Fourth Amendment right was violated. The Court ruled that

There are three distinct and increasingly intrusive types of bodily examinations undertaken by law enforcement after certain arrests and it is critical to differentiate between these categories of searches. A "strip search" requires the arrestee to disrobe so that a police officer can visually inspect the person's body. The second type of examination — a "visual body cavity inspection" — occurs when a police officer looks at the arrestee's anal or genital cavities, usually by asking the arrestee to bend over; however, the officer does not touch the arrestee's body cavity. In contrast, a "manual body cavity search" includes some degree of touching or probing of a body cavity that causes a physical intrusion beyond the body's surface [...] Summarizing the relevant constitutional precedent, it is clear that a strip search must be founded on a reasonable suspicion that the arrestee is concealing evidence underneath clothing and the search must be conducted in a reasonable manner. To advance to the next level required for a visual cavity inspection, the police must have a specific, articulable factual basis supporting a reasonable suspicion to believe the arrestee secreted evidence inside a body cavity and the visual inspection must be conducted reasonably. If an object is visually detected or other information provides probable cause that an object is hidden inside the arrestee's body, Schmerber dictates that a warrant be obtained before conducting a body cavity search unless an emergency situation exists.<sup>81</sup>

Then according to *People v. Azim Hall* it would be difficult to justify a body scanner examination on a routine-basis without "*a reasonable suspicion*" that the person is "*concealing evidence underneath clothing*". On the other hand, a specific warrant is not necessary, given that WBI cannot inspect body cavities.

44. There is an apparent a tension between the **EU Charter** and the **US Constitution** perspectives on body scanners. In the European perspective the potential offence of WBI to body integrity does not seem to depend chiefly on the way in which the subject perceives the intrusion, nor on whether personal data are properly handled. In other words the offence to human dignity can be hardly mitigated by only respecting rules of decency and by adopting privacy and modesty filters. The potential offence is related to the fact that the human body is not respected, because it is exposed as though it were a commodity. As Murphy and Wilds argue, the body scanner "reduces the traveler's body to the same legal status as a piece of luggage on a conveyor belt."<sup>82</sup> This casts doubts about whether routine search though WBI might ever be consistent with respect for EU fundamental rights, notably art.3, unless the technology would not show the body at all, but merely the objects the person is holding.

---

<sup>81</sup> *People v. Azim Hall*, 2008 NY Slip Op 2676 (2008)

<sup>82</sup> Murphy MC, Wilds MR (2001). X-rated x-ray invades privacy rights. *Criminal Justice Policy Review*, 12(4), 333–343.

45. Also in the light of the **US Constitution**, it would be difficult to justify routine air traveler screening through body scanners. As Klitou<sup>83</sup> argues “under the current conditions, whereby the employment of a privacy algorithm or the deletion of the images is not mechanically ensured and other safeguards are not legally binding, the use of backscatter body scanners is disproportionate and constitutes an unjustified violation of privacy in a democratic society [...]the law, as it stands now, is unable to adequately uphold the integrity of the Fourth Amendment or protect the right to privacy.” It is notable, however, that, according to this perspective, effective and legally binding privacy algorithms could protect the right to privacy and then make WBI systems consistent with the Fourth Amendment.
46. Finally, an ethical framework which would include both dignitarian and privacy perspectives, could be based on the notion of body as a “gift”<sup>84</sup>. The body is never completely “ours”, for the very reason that it has a symbolic dimension, say, each body is “embodied” in a given human community. We “receive” ourselves as a gift from the human community and we are in debt with our fellow human beings. In fact, persons are not simply co-extensive with their bodies: people are made up also by their human relations, by the social networks to which they belong across space and time. “We are bound together by our often needy bodies (and by our other, non physiological needs) into a community of needs. In this community-really multiple communities, sometimes overlapping, some like ripples extending wider and wider around a core we can recognize the needs of others through our shared embodiment”.<sup>85</sup> Our shared embodiment is also the source of our fragility, and the moral justification for cooperation when safety and collective security are at stake. This would be the case of WBI for aviation security, provided that its effectiveness and proportionality are convincingly demonstrated.

#### KEY MESSAGE TO POLICY MAKER

In order to make WBI technology consistent with respect for human dignity, integrity and physical privacy WBI should not show the “naked” body but merely the objects the person is holding. This general tenet implies two converging strategies. First the officer viewing the image should not see the scanned person. The use of modesty filters is also advisable. Second, WBI systems should be selected according to their capacity to detect prohibited items without providing anatomic and medical details. In any case the adoption of WBI technology for routine screening is ethically tenable only if its effectiveness and proportionality are convincingly demonstrated.

<sup>83</sup> Klitou D, (2008), Backscatter body scanners – A strip search by other means, *Computer Law & Security Report* 24, 316 – 325

<sup>84</sup> Murray T, Gifts of the Body and the Needs of strangers, *Hastings Center Report*, April 1987, 30-38

<sup>85</sup> Murray T, (1987), *ibid.*

## Physical Integrity

47. Direct effects on the body of current WBI technologies are very limited<sup>86</sup> and the health impact of all existing WBI is negligible. Apart from x-ray transmission systems, no WBI, including x-ray backscatter, is expected to have any relevant health impact on people. To be sure, pacemakers and implantable cardioverter-defibrillators (ICDs) may be susceptible to electromagnetic interference from a number of devices (e.g., cellular telephones, electronic surveillance systems, metal detectors). People with such medical implants should also avoid electromagnetic pulse generating body scanners (but they could be examined through passive systems).
48. In the case of backscatter technology, however, the body is going to absorb a very low dose of ionizing radiation, which is likely to produce negligible effects on human cells. Although the dose absorbed is below the threshold of health risks and could be considered as a component of the background radiation in which we all live, there is no rationale to expose anyone to an additional source of ionizing radiations, as low as they are, when the same results could be achieved by using non-ionizing electromagnetic waves. Given that there is no evidence that x-ray backscatters are more reliable and accurate than MM-wave scanners, it is difficult to understand why backscatter technology is still considered as a potential candidate for people screening at airport check-points. On the contrary there are two parallel arguments that suggest excluding backscatters from potential screening technologies would be wise: 1) In the absence of any other benefit, one should give privilege to the least physically intrusive technology, and there is no doubt that MM-wave devices have less effects on the human body than x-ray backscatters; 2) In the absence of any other benefit, one should promote the most acceptable technology, and people are likely to prefer to undergo non-ionizing radiations rather than ionizing radiations.
49. X-ray transmission systems have never been proposed for routinely screening in airports. Yet, sooner or later, it is likely that the possibility to use them for selected checks will be raised. Advances in miniaturisation are making it easier for terrorists to hide small bombs into body cavities, or implant them surgically. These bombs, powerful enough to cause a plane to crash, will not be detected by metal detectors and body scanners. Such a body bomb method was tested for the first time in August 2009, when the Saudi anti-terrorism chief, Prince Mohammed bin Nayef, survived a terrorist attack carried out by a 23-year-old Al Qaeda militant who got through several security checks with military grade plastic explosive in his rectum. The bomb was probably triggered by a signal from a mobile phone text message. Most analysts think that this kind of attack is going to increase and consequently will have a very relevant impact on

---

<sup>86</sup> In the EU health and safety of electrical equipment is governed by the Low Voltage Directive 2006/95/EC, and by the Council Recommendation 1999/519/EC. Millimeter wave technology is instead covered by the Directive 1999/5/EC on radio and telecommunication equipment.



screening tactics and techniques for years to come.<sup>87</sup> To date only X-ray transmission systems could detect explosives hidden inside the body, although very low radiation systems are available.<sup>88</sup>

#### KEY MESSAGE TO POLICY MAKERS

Assuming all other conditions equal, there is no reason to adopt X-ray backscatters, which expose the subject to an additional – although negligible – source of ionizing radiations. Other WBI technologies should be preferred for standard use. The use of X-ray transmission systems for selected checks (i.e., explosives hidden inside the body) should be avoided and alternative technologies using non-ionizing radiations should be investigated.

### Mental Integrity

50. On Jan 11, 2010 German activists from the Pirate Party organised for a “fleshmob” in the Berlin-Tegel airport. Naked protesters marked their bodies with a number of messages such as, “Something to hide?” and “Be a good citizen — drop your pants.”<sup>89</sup> Body scanner images might show intimate body parts, like breasts and genitalia, as well as intimate personal and medical details and many scholars and privacy advocates have argued that WBI should be considered a “virtual strip search”<sup>90</sup>. Menstrual pads, incontinence pads, diapers and suchlike, are all detectable and WBI can also easily detect under-the-skin implants, such as breast and penile implants and a vast array of cosmetic surgeries. Colostomy inserts, various kinds of prosthesis, electronic body implants, and body piercings can also all be revealed by all WBI systems. Although in real life the quality of images is far from those advertised in producers’ web sites and leaflets, it is difficult to deny that the end result of WBI, without any modesty filter, “is similar to that of strip searches and far more intrusive than patdowns”<sup>91</sup>.
51. Imposed “virtual” nakedness is an important threat to bodily and psychological integrity. Nakedness is more than nudity. While *nudity* is the simple state of absence of clothing, *nakedness* is a mental state, which implies being stripped of decency, to lack an element of protection. *Nakedness* involves objectification, the process of symbolically turning a person into an object to be appraised. As Rabbi Bradley Shavit Artson argues “In the Garden, Adam and Eve were nude

<sup>87</sup> <http://www.dailymail.co.uk/news/worldnews/article-1218562/Bombers-hide-devices-inside-bodies-Travellers-Europe-face-body-X-rays.html>

<sup>88</sup> There are also *Body Orifice Screening Systems*, which are designed for security inspection of body cavities. The Body Orifice screening system are non intrusive and eliminates the liability and safety issues associated with manual searches. The systems use a low ionising radiations (<http://www.adani.by/en/products/security-x-ray/personnel>)

<sup>89</sup> German ‘Fleshmob’ Protests Airport Scanners; Wired, Jan 12, 2010 <http://www.wired.com/threatlevel/2010/01/german-leshmob/#ixzz0cVWE4UJX>

<sup>90</sup> American Civil Liberties Union (ACLU) Backgrounder on Body scanners and “Virtual Strip Searches”, available at <http://www.aclu.org/privacy/35540res20080606.html>

<sup>91</sup> Klitou D, (2008), *ibid.*



and complete. Outcast, and with a consciousness of having sinned, they became naked."<sup>92</sup> While *nudity* is an objective, empirical, condition, *nakedness* is a highly symbolic experience, which is culturally determined. In most cultures, physical exposure is a form of pornography, which "would de-sacralize matter, deprive matter of spirit"<sup>93</sup>. *Nakedness* has also to do with power: those who see are usually more powerful than those who are seen. In *Foucauldian* terms the exercise of power involves regulation through visibility.

52. What turns nudity into nakedness is degradation.<sup>94</sup> Degradation means devaluation, dehumanization. Degradation always implies a certain degree of self-degradation, as pointed out by Primo Levi in *The Drowned and the Saved* (1986). Levi shows how physical degradation tends to produce the complicity of the victim, and eventually it destroys the sense of worth and self-esteem, and generates humiliation. Humiliation is the last step in this path through threats to mental integrity. "To be humiliated means to have your personal boundaries violated and your personal space invaded [...] Although the feelings of humiliation are intensely personal, the process itself is located in the relationship between the persons."<sup>95</sup>
53. Worries about the risk that WBI might become an humiliating experience have been raised in particular for women, children, incapacitated persons, and specific ethnic and religious groups. Most PIAs recommend that individuals could opt for being examined by an operator of the same gender or, even, that the procedure routinely provides two machines, one for women, and one for men. The Canadian Privacy Commissioner asked that incapacitated persons might be exempted from WBI examination, on the basis of their incapacity to provide a free and informed consent. One should also take into account that some persons wouldn't even be able to enter the body scanner, e.g. mothers with baby carriages and people in a wheelchair. In the UK the civil rights group *Action on Rights for Children* questioned whether the scanners could breach the Protection of Children Act 1978, under which it is illegal to create an indecent image or a "pseudo-image" of a child.<sup>96</sup> Trevor Phillips, head of the *Equality and Human Rights Commission* (EHRC), a UK non-departmental Government body, also warned "that using profiling techniques to single out Muslims, Asians and black people for scanning at airports could breach race and religious discrimination laws introduced by the government."<sup>97</sup> Some Islamic groups<sup>98</sup>

---

<sup>92</sup> Rabbi Bradley Shavit Artson, *Shabbat Parashat Yitro, 22 Shevat 5764 - The Naked & The Nude* - <http://judaism.ajula.edu/Content/ContentUnit.asp?CID=912&u=4556&t=0>

<sup>93</sup> Griffin S, (1978) *Woman and Nature: The Roaring Inside Her*. New York: Harper

<sup>94</sup> Shapiro DL, (2004), *The Nature of Humiliation* Paper presented at the 2005 Workshop on Humiliation and Violent Conflict, Columbia University, New York, December 15-16, 2005.

<sup>95</sup> Klein DC (2005) *The Humiliation Dynamic: Looking to the Past and Future*, Paper presented at the 2005 Workshop on Humiliation and Violent Conflict, Columbia University, New York, December 15-16, 2005.

<sup>96</sup> *Body scanners threaten children's rights*, The Guardian, Jan 4, 2010

<http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/04/airport-body-scanners>

<sup>97</sup> *Airport full-body scanners 'break laws on privacy'*, The Sunday Times January 17, 2010,

<http://www.timesonline.co.uk/tol/news/politics/article6990990.ece>

have questioned whether body scanners are “particularly offensive to Muslim women, who may choose to dress modestly, as well as being targeted for profiling on the basis of their race, religion or appear”.<sup>99</sup> Indeed Islam guides that, for both men and women, clothing must be as loose as not to outline the shape of the body, this rule is apparently contradicted by body scanners. A Fatwa issued on February 9<sup>th</sup> by the *Fiqh Council of North America* emphasized that “a general and public use of such scanners is against the teaching of Islam, natural law and all religions and cultures that stand for decency and modesty”<sup>100</sup>. The Fatwa recommends to Muslim to avail the pat down search over the “nude body scanners”. Also the *Rabbinical Center of Europe* (RCE) complained that WBI in European airports might compromise Jewish women's modesty, and recommended that “men are scanned by men, and women by women, akin to body frisk.”<sup>101</sup> In June 2009, *Agudath Israel*, which represents traditional American Orthodox communities, sent a letter to the US Senate subcommittee dealing with the body scanner dossier, promoting an amendment that limited the use of the full-body scanners to situations in which passengers had already failed a metal detector test, provided that those passengers be also offered the option of a pat-down search. In this letter *Agudath Israel* judged WBI “offensive, and far short of acceptable norms of modesty (*tzniut*) under the laws and practices of Judaism and many faith communities”.<sup>102</sup>

#### KEY MESSAGE TO POLICY MAKERS

All forms of modesty deserve to be fully respected– no matter how far they are from the western ethos. Some people could perceive WBI screening as an humiliating experience. Their objections should be always be taken into account. No one should be ever be obliged to undergo to any security measure that he feels humiliating and degrading. In particular no one should be offered the option to accept such a measure in exchange for a benefit. This would make it still more humiliating.

## CHAPTER 5: PRIVACY ISSUES

54. Emerging WBI technologies promise to be more and more privacy invasive. Today, there is no clear cut distinction between MM-wave and T-ray technology, which are a continuum along the electromagnetic spectrum. All frequencies in this region can be used both to create an image of an object or to gather information on its chemical makeup. As energy moves from the shorter infrared

<sup>98</sup> EU divided on use of airport body scanners, <http://www.msnbc.msn.com/id/34747772>

<sup>99</sup> Airport Body Scanners Only Offensive to Muslim Women?, *Muslimah Media Watch*, <http://muslimahmediawatch.org/2010/01/naked-ambition-plans-for-airport-body-scanners-only-offensive-to-muslim-women/>

<sup>100</sup> <http://www.fiqhcouncil.org>. See also <http://theklaxon.com/council-issues-fatwa-on-full-body-scanners-at-airports-complicates-u-s-security/4989>

<sup>101</sup> <http://www.ynet.co.il/english/articles/0,7340,L-3831622,00.html>

<sup>102</sup> How Modern Airport Security May Run Afoul of Jewish Law, *The Jewish Daily Forward*, <http://www.forward.com/articles/123364/>

to the longer microwave region of the electromagnetic band, it becomes able to do different things. As frequencies increase, the radiation acquires spectroscopic capacities (e.g., it can be used to identify different kinds of chemicals and materials). Also it penetrates the human body surface through half a centimeter, becoming able to distinguish normal skin tissue from tumours, and some superficial breast cancers; T-radiation can also get an image of the dental arcade, which could be used for personal identification.

55. Technologies rapidly evolves: screening systems in the near future probably will be based on “a fusion of multiple technologies, on the ability to detect multiple threats simultaneously, and most important, on the ability to perform the screening on people not as a dedicated function, but while people are engaged in other activities, such as standing in line for passport control, waiting at the ticket counter or walking from one area of a facility to another”<sup>103</sup>. Emerging WBI systems include “covert systems capable of scanning a vehicle traveling at five to 30 mph [...] smart programs may be written to recognize shapes, optimize machine settings for selected purposes, or identify certain materials, [...] Present technology may also assume different forms. For example, systems may be disguised within decorative portals for the covert screening of individuals passing through the portals. Smaller transmission systems may be produced for the sole purpose of imaging stomach contents in order to search people suspected of having swallowed contraband”<sup>104</sup>. It also thinkable that future WBI could become part of wider systems for hostile intention detection, which is one of the main trends in aviation security.<sup>105</sup>
56. Once WBI systems are legally justified and their use is standard in airports, there is the menace that nothing might prevent the slippery slope towards the adoption of more advanced, and privacy intrusive, systems, and the introduction of WBI for more mundane applications, like in sporting stadiums, public malls, schools, etc. In brief, WBI technology risks to become a building block of the wider apparatus called (by Monahan and Wall<sup>106</sup>) *somatic surveillance* in which “bodies are not only informatized but controlled in various ways”.

**KEY MESSAGE TO POLICY MAKERS**

Emerging WBI technologies should be addressed as soon as possible. In this field technology evolves very rapidly and once the use of WBI systems becomes standard in airports, there is a concrete risk that more advanced and privacy intrusive systems are would further then be introduced, and that they are could also be used for more mundane applications.

<sup>103</sup> Homeland Security Market Research, *People Screening Facing a Challenging, Transition Period*, <http://www.homelandsecurityresearch.net/2009/03/17/people-screening-facing-a-challenging-transition-period> )

<sup>104</sup> NCRP (2004)

<sup>105</sup> See in the US [http://www.dhs.gov/files/programs/gc\\_1218480185439.shtm#12](http://www.dhs.gov/files/programs/gc_1218480185439.shtm#12), and in the EU [http://cordis.europa.eu/fp7/security/fp7-project-leaflets\\_en.html](http://cordis.europa.eu/fp7/security/fp7-project-leaflets_en.html)

<sup>106</sup> Monahan T, Wall T, (2007), *Somatic Surveillance: Corporeal Control through Information Networks*, *Surveillance & Society*, 1, 4(3): 154-173

## Privacy Enhancing Technologies

57. Vis-à-vis such a worrying scenario, there is however a consensus among PIA documents that a proper use of privacy enhancing technologies (PET) can minimize privacy invasion and make WBI systems ethically tenable. The so called “second generation” WBI systems which have been adopted e.g., in The Netherlands and in Italy, feature only a kind of generic, impersonal, graphics<sup>107</sup>. The point is whether these protections are, and will be, actually implemented. For instance *Privacy International* “is sceptical about the privacy safeguards that the US Transportation Safety Administration (TSA) is touting. The TSA say that the technology is capable of obscuring faces, but this claimed protection is just a software fix that can be undone as easily as it is applied [...] The TSA also say it will not retain the images. That protection would certainly be a vital step for such a potentially invasive system, but given the irresistible pull that images created by this system will create on some employees (for example when a celebrity or someone with an unusual or *freakish* body goes through the system), our attitude is one of *trust but verify*”.<sup>108</sup>
58. Two recent cases could support such a skeptical approach. In 2009 the American Electronic Privacy Information Center (EPIC) provided a document to CNN in which the US TSA asked the seller that the body scanners have the ability to store and send images when in test mode. The document also showed that the scanners have 10 variable privacy settings.<sup>109</sup> On February 9, 2010, the movie star Shahrukh Khan revealed on the BBC’s Jonathan Ross<sup>110</sup> show that he passed through a body scanner and later had the image of his naked body printed out and circulated by Heathrow security staff. His claims have resonance because of his latest film, *My Name is Khan*, which is about racial profiling of Muslims at airports. A BAA spokeswoman said the claims were “completely factually incorrect”. She stressed WBI images could not be stored or distributed in any form and said there would be no investigation into his claims because they “simply could not be true”.<sup>111</sup>

### KEY MESSAGE TO POLICY MAKERS

Privacy Enhancing Technologies (PETs) can alleviate privacy concern only if PETs cannot be “switched-off”. The “privacy-by-design” approach is the right approach. In addition, given the highly sensitive policy area, it would be advisable to introduce an independent and legally binding control that PETs are properly implemented. In terms of communication with the public, it is paramount that any privacy complaint – although unrealistic – is seriously considered and overtly discussed.

<sup>107</sup> See e.g., <http://detectorfp7.blogspot.com/2010/01/focus-on-full-body-scanners.html> and <http://www.spiegel.de/fotostrecke/fotostrecke-50292-4.html>

<sup>108</sup> Statement on proposed deployments of body scanners in airports, [www.privacyinternational.org](http://www.privacyinternational.org)

<sup>109</sup> <http://www.cnn.com/2010/TRAVEL/01/11/body.scanners/index.html>

<sup>110</sup> <http://www.bbc.co.uk/programmes/b00qn04k>

<sup>111</sup> <http://www.telegraph.co.uk/news/newstopics/bollywood/7203872/Airport-denies-body-scanner-photo-claim-by-Bollywood-star-Shahrukh-Khan.html>

## Does WBI generate personal data?

59. The US TSA claims that the adoption of privacy enhancing technologies could irrevocably unlink WBI images from recognisable individuals. This would prevent labelling WBI images 'personal data', and considering WBI procedures data processing, "TSA has developed operating processes for the WBI, used for pilot operations, that do not collect, store, or distribute any personally identifiable information."<sup>112</sup> This view is rejected by most EU privacy authorities, notably by the Art.29 WP and the European Data Protection Supervisor on the basis that "a link is established between the data provided by the body scanner and the individual who is being screened. Based on the information provided by the body scanner, an evaluation of the threat will be conducted which will result in an impact on the individual (release or additional check). It has therefore to be considered as a processing of personal data."<sup>113</sup>
60. Whether WBI devices are or are not generating and handling personal data is not a trivial particular, because it has important legal implications. According to known WBI operating procedures, and according to available information about privacy-built-in protections, in most systems body scanner images 1) are not retained, and 2) the WBI operator is located in a remote viewing room, and is not allowed to either see the scanned subject, nor to keep, or transmit outside, any image. Transportation authorities usually argue that these protections should prevent linking WBI images to any person. Yet this does not completely solve the problem.
61. First of all, personal details generated by WBI are not linked to a person, if that person is released, but if she is retained and further investigated, data may be linked. Given that in most trials (and notably in Dutch trials at Amsterdam airport) there have been a high number of false positives - say, people who set off the system alarm and required further examination, without concealing any prohibited item under their clothes - it is hardly tenable that WBI systems are not going to generate personal data. All false positive people are indeed "linked" to their body scanner images and - although images will not be eventually stored in the system, nor in any other medium - sensible bodily information becomes potentially linkable to an identified person.
62. It is often misunderstood that the mere fact that images are not retained does not imply that WBI systems are not generating data. At the very least they are generating aggregated data about themselves and their effectiveness in detecting concealed objects. Thus, although images are not retained, they are generating aggregated data about peoples' bodily modifications (e.g., number of people with body piercings, or with under-skin implants). All these details cannot be considered personal data provided that they are not linked to any specific person. Yet there is moment in which there is such a link, although temporary and volatile: when the person is "in" the scanner and the image is in

---

<sup>112</sup> US DHS, Privacy Impact Assessment for TSA Whole Body Imaging October 17, 2008

<sup>113</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009-others\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm)

the process of being generated. In that moment data is in the system and is aligned to an identifiable person (the actual person who is in progress to be scanned). This is indeed the most delicate moment of the whole process. If the system is hacked, this is the moment in which one could either produce fake images or steal images from the system. Likewise, this is the moment in which the system can be (mis)used.

63. The issues of function creep and system misuse have hardly been addressed, yet there is a theoretical possibility that WBI systems can be (mis)used for different purposes rather than for detecting concealed objects. WBI systems can be used for people profiling and for personal identification. Imagine, for instance, that checkpoint operators have been alerted that a person, who is a likely terrorist, is known for having a breast implant. Operators might be instructed to single out all people with a breast implant and submit them to an extra screening. WBI systems could also be used to identify persons. In the previous example, it would be enough that operators are instructed that the suspected terrorist, beyond the breast implant, *has* a Nigerian passport, *and* is aged less than thirty, *and* spent a month in London in the last year (all these elements could be deduced from the Passenger Name Record, PNR, file). By crossing these clues with the information about the breast implant, WBI can easily allow the identification of the alleged terrorist when she passes through the body scanner. As we mentioned, WBI devices could also be misused for hostile intention detection. Microwave dielectrometer portals are already able (at least according to the producer) to monitor and detect increased heart rates and perspiration levels of people<sup>114</sup> and chances are that next WBI generations could do even more.

#### KEY MESSAGE TO POLICY MAKERS

Although images are not retained, WBI systems are generating data. Reaching an international consensus about whether these data are personal and to what extent they are sensitive is certainly important. Yet it is still more important to find a consensus about 1) what data are actually generated; 2) how they should be protected. WBI systems could be hacked and there is a common interest from both security agencies and privacy advocates to improve body scanner security and to build more and more secure systems.

## CHAPTER 6: GOVERNANCE

---

64. In the EU, security screening at airports is “supervised” by the Union, although they remain under member state jurisdictions. According to Regulation (EC) 300/2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, the European Parliament and of the Council “should lay down the basic principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference without going into the technical and procedural details of how they are to be implemented.”

---

<sup>114</sup> <http://www.global-security-solutions.com/PeoplePortal.htm>

National legislations are then responsible for detailed regulations. However in most countries, there is not yet a proper legal framework for the use of body scanners. Air Transportation agencies self-regulations are not binding and could be changed at any moment (and without any obligation to inform citizens) at the discretion of each national agency. Modesty filters, privacy algorithms, built-in restrictions that prevent printing, transmitting and circulating WBI images are not legally mandated in any EU country. There are no agreed international standards concerning WBI and no WBI technology is certified.<sup>115</sup>

#### KEY MESSAGE TO POLICY MAKERS

If we want to implement trusted body scanners, we should **define a legal framework** and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy. This should be substantiated in appropriate standards and certification procedures. If WBI has to be implemented, **European standards and certifications** must be developed as soon as possible.

#### Regular Review

65. A regular review of the rationale which justifies the use of WBI technologies is advisable, also as per Regulation (EC) No 300/2008, which states that “Member States should also be allowed, on the basis of a risk assessment, to apply more stringent measures than those laid down in this Regulation”. This implies a regular review of the proportionality between body scanner screening and airport security needs (i.e., the actual risk for passengers). Yet it is questionable whether a public and reliable risk assessment of the proportionality principle<sup>116</sup> is ever possible in a sensitive field such as aviation security.

#### KEY MESSAGE TO POLICY MAKERS

Reviews of WBI technologies and the rationale which justifies their use, notably as far as the proportionality principle is concerned, must be carried out on regular basis. Citizens input during the system application phase should also be part of the total review system. Although specific contents of these reviews could be partly restricted, review results should always be public.

#### WBI operating procedures

66. Control of people who enter the airport sterile area<sup>117</sup> is the primary task of airport checkpoints. A secondary task is to ensure that people who have been

---

<sup>115</sup> The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Guide 2:2004 defines a standard as “a document, established by consensus that provides rules, guidelines or characteristics for activities or their results.” Standards play a role in everyday life by establishing the size, configuration, or protocol of a product, process, or system. Standards also define terms so that there is no misunderstanding among those using the standards. They enable development of integrated, scalable, system solutions.

<sup>116</sup> Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

<sup>117</sup> The “sterile area” refers to portions of an airport that provides passengers access to boarding aircraft and to which the access is controlled. People who enter sterile area include passengers,



cleared remain cleared before boarding their aircraft. Primary screening methods are those used for controlling all people who want to enter the sterile area. Secondary methods are those used only for some selected groups in addition to primary screening. The issue of whether WBI should be a primary or as secondary screening method is extremely political and ethically sensitive. If WBI is intended as a primary method, it means that we create an intermediate level, between pat-down and strip search, which becomes routine. In other words we “upgrade” the level of intrusiveness of standard security checks. Reading governmental documents, official and unofficial statements, reports and parliamentary hearings, it is unclear what the actual plans are. Yet two points are probably out of discussion, 1) for now WBI is not going to substitute hand search, as it is demonstrated by all operating protocols, which advise further hand search if any anomaly is detected during WBI screening; 2) WBI is not going to make WTMD totally obsolete, given that WBI cannot detect objects hidden in body cavities, which could be instead sensed by metal detectors (if they are made by metal). It is then difficult to escape the impression that in the short term, WBI is destined to become an additional screening tool rather than a substitute for current procedures. This also casts doubts about whether WBI is going to expedite checkpoint procedures. Considering that people have to be offered to opt between WBI and physical search, and some of those who opted for WBI will still undergo a physical search after WBI screening, it is arguable that large scale application of WBI will ever speed up security checks.

67. There is a substantial consensus that establishing rules for body scanner operating procedures is a crucial component of their deployment. Unfortunately these details are not going to become public because of security reasons. “The impact of passenger risk uncertainty can be mitigated by designing sufficient flexibility into security operations, in terms of what procedures are used to screen varying passenger risk profiles. The pursuit of this objective requires a measure of intelligence into how passenger risk is assigned.”<sup>118</sup> Regulation (EC) No 300/2008 states “As a general rule, the Commission should publish measures that have a direct impact on passengers. Implementing acts setting out common measures and procedures for the implementation of the common basic standards on aviation security which contain sensitive security information, together with Commission inspection reports and the answers of the appropriate authorities should be regarded as EU classified information”. Does WBI operating procedures contain sensitive security information? The UK Department for Transportation wrote that “body scanners must be operated in accordance with detailed protocols which contain the security sensitive information on the operation of the body scanner including selection criteria for those to be scanned. The details of the protocol are not published due to the

---

flight crew members, and airport personnel, employed by the airport, air carriers, or by companies, that conduct business in airports.

<sup>118</sup> Nikolaev AG, Jacobson SH, Lee J, (2009) Designing for flexibility in aviation security systems *J Transp Secur* n2:1–8

security sensitive content but will comply with the requirements contained in this interim Code of Practice.”<sup>119</sup>

- 68.** On the other hand, WBI Standard Operating Procedures may determine the overall degree of democratic acceptability of the whole system. On 8 Dec 2009, the Washington Post revealed that the TSA inadvertently posted online its operating manual for screening passengers. The manual, which was immediately obscured by the TSA but which is still readable online,<sup>120</sup> reveals “technical settings used by X-ray machines and explosives detectors. It also includes pictures of credentials used by members of Congress, CIA employees and federal air marshals, and it identifies 12 countries whose passport holders are automatically subjected to added scrutiny”.<sup>121</sup> Some of these details should be considered security sensitive (e.g., body scanner setting) , yet most of them were politically and ethically sensitive. For instance the manual listed criteria to be adopted for selecting people who should undergo to WBI screening. Passengers holding passports from, or taking flights that originated in or passed through, Cuba, Iran, Sudan and Syria, Afghanistan, Algeria, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia, and Yemen, have to pass through body scanners or to be physically searched. Singling out travellers from a few specified countries for enhanced screening is not a technical setting, but it is a, very arguable, political decision.
- 69.** As pointed out by the Art.29 WP and EDPS joint reply to the EC public consultation on body scanners<sup>122</sup>, “excluding some individuals from the screening, whatever the reason (just as giving a choice to the individual), puts into question the real necessity of the system”. Moreover it is highly questionable that it could be ever ethically acceptable that certain categories of travelers (because of their nationality, their ethnicity, or religious beliefs) would have to go routinely through WBI or full physical search. This would be in contrast with Chapter III of the EU Charter, which deals with the prohibition of any discrimination (art. 21), and the respect of cultural, religious and linguistic diversity (art. 22).
- 70.** A similar principle is also affirmed in the Commission’s *Green Paper on detection technologies in the work of law enforcement, customs and other security authorities*<sup>123</sup>, which states that “policies relating to detection and associated technologies have to comply in full with the existing legal framework, including the EU Charter of Fundamental Rights, the European Convention on Human Rights and data protection principles and rules as laid down in Directive 95/46/EC. In this context, the Commission stresses that the design, manufacture and use of detection technologies and associated technologies, together with

---

<sup>119</sup> UK Dept. for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology in an Aviation Security Environment*, [www.dft.gov.uk/pgr/security/aviation/airport/](http://www.dft.gov.uk/pgr/security/aviation/airport/)

<sup>120</sup> <http://boardingarea.com/blogs/thewanderingaramean/2009/12/the-tsa-makes-another-stupid-move/>

<sup>121</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/08/AR2009120803206.html?hpid=topnews>

<sup>122</sup> The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, <http://ec.europa.eu/justicehome/fsj/privacyindexen.htm>

<sup>123</sup> COM(2006) 474 final

legislation or other measures aiming to regulate or promote them, must fully comply with Fundamental Rights as provided for in the EU Charter of Fundamental Rights and the European Convention on Human Rights”<sup>124</sup>

**KEY MESSAGE TO POLICY MAKERS**

Selective screening procedures are hardly consistent with fundamental rights and should be avoided. We welcome the EDPS and Art.29 WP suggestion that the body scanner screening should be universal, say, no specific subgroup of travellers should be targeted or exempted on the basis of considerations about nationality, race, ethnicity, religion, gender, and age. Yet we understand that specific security conditions could oblige to the selection of specific categories of people for body scanner screening. Such a procedure should be always be convincingly justified and should be temporary.

- 71.** Identifying individuals who should undergo to WBI also raises serious questions in relation to civil liberties, also because of the intersection between migration management and aviation security. Selection criteria are very politically sensitive details, which allow to evaluate the consistency of WBI systems with fundamental human rights and democratic rules. As solemnly affirmed by the Berlin Declaration “In the European Union, we are turning our common ideals into reality: for us, the individual is paramount. His dignity is inviolable. His rights are inalienable [...] We will fight terrorism, organised crime and illegal immigration together. We stand up for liberties and civil rights also in the struggle against those who oppose them”.<sup>125</sup>

**The airport as a total institution**

- 72.** A quite neglected aspect of body scanners is their “symbolic” function in the whole security airport apparatus. This is not a minor issue. Airports share several features with the so-called “total institutions”. This is a term used by social scientists to describe an “institution where all parts of life of individuals under the institution are subordinated to and dependent upon the authorities of the organization. Total institutions are social microcosms dictated by hegemony and clear hierarchy [...] A place of residence and work where a large number of like-situated individuals, cut off from the wider society for an appreciable period of time together, lead an enclosed, formally administered round of life”<sup>126</sup> In the standard sociological account total institutions include boarding schools, concentration camps, colleges, cults, prisons, mental institutions, sailing ships, boot camps, monasteries, convents, nursing homes, and orphanages.
- 73.** As some scholars have noticed,<sup>127</sup> airports are very close to total institutions. Airports are self-contained structures, with health clinics, religious sites,

<sup>124</sup> Ibid.

<sup>125</sup> Declaration on the occasion of the fiftieth anniversary of the signature of the Treaties of Rome, [http://www.eu2007.de/en/About\\_the\\_EU/Constitutional\\_Treaty/BerlinerErklaerung.html](http://www.eu2007.de/en/About_the_EU/Constitutional_Treaty/BerlinerErklaerung.html)

<sup>126</sup> Goffman E (1961), *Asylums. Essays on the social situation of mental patients and other inmates* Anchor Books, Doubleday & Company, Inc., New York

<sup>127</sup> Salter MB, Adey P, (2008), *Politics at the Airport*, Minnesota UP

entertainment, hospitality, police power, and so on. People who enter the security area are segregated (at least for the period of time in which they stay in this area). Interestingly enough stripping processes are a peculiar feature of all total institutions (be they colleges, hospitals, prisons, barracks). Personal identity equipment is removed, as well as other possessions with which the inmate may have identified himself. Such a strip is a “rite of passage”, which marks the entrance into the total institution through a mortification of the person (etymologically mortification means to turn someone into a corpse). At symbolic level what happens with body scanners at airport check-points is that “people are stripped of their status as honest citizens and treated like potential criminals. This is more evident in those airports in which operators are a bit rude and the whole screening procedure is carried out in almost-military manner.”<sup>128</sup> Body scanner “virtual strip” could progressively turn into a “symbolic strip” which figuratively deprives the person of his “global citizenship rights”, in other words while we claim to protect universal rights, we run the risk to deny them with our security practices.

## CHAPTER 7: CONCLUSIONS

---

- 74. WE BELIEVE** that the primary aim of security is to safeguard the human person in his or her physical, mental, and social integrity. Respect for human dignity, body integrity and privacy (both physical and informational) are thus essential components of any security policy. Security measures which impair human integrity of those which should be protected are self-contradictory and eventually are also less effective. The primary purpose of WBI technology and systems is only to detect prohibited items concealed on the body. We think that WBI is legitimate as far as it fulfils its original purpose. Any different goal, like people identification or profiling, or detection of anatomic and/or medical details, is not legitimate and is not respectful of personal integrity.
- 75. WE ARE CONCERNED** that body scanners could humiliate people by unravelling anatomic and/or medical details, and by hurting their feelings of modesty. We are concerned by the lack of clarity about WBI operating procedures, and by confusion and inconsistencies about primary and secondary screenings, voluntariness and compulsion. We are also concerned that body scanners can be used to discriminate against certain groups of travellers. In other words we are concerned that WBI technologies and systems can be (mis)used for wider purposes than the detection of concealed objects.
- 76. WE REGARD** the European Charter of Fundamental Rights as the general framework for the introduction in the EU of new technologies for passenger screening and aviation security.
- 77. WE RECOMMEND** that respect for the primacy of the human person and attention to his or her needs are the leading principles followed in the establishment of aviation security. We also recommend that the European Commission should propose a specific framework for detection, profiling, and

---

<sup>128</sup> Salter MB, Adey P, (2008), *ibid*.

identification technologies for aviation security. We recommend that WBI operating procedures should be subject to a public, democratic, scrutiny. Appropriate exemptions can be provided only for those parts of SOP manuals which directly deal with technically sensitive details. We finally recommend that the European Commission should encourage the use of codes of practice and ethical codes at MS level, and promote the establishment of a system of complaints and remedies at EU level.

- 78. WE WELCOME** the regular use of privacy enhancing and “privacy-by-design” technologies in WBI system design. We also recommend that technologies should be selected and systems should be designed in order to make practically impossible to fulfil illegitimate purposes. We recommend that the European Commission, in conjunction with the European Data Protection Supervisor and the Art.29 Working Party, promote independent, publicly available, Privacy Impact Assessments (PIAs) prior to the adoption of any new WBI technology and system.
- 79. WE URGE** the European Commission to commit to a plan of action to promote further research on ethical, legal, and social implications (ELSI) of technologies for aviation security, their likely effect on public trust and their communicational and symbolic dimensions. In particular we recommend that the European Commission and the European Parliament promote the adoption of an ethical framework for trials with new WBI technologies.

## Acknowledgments

*CSSC gratefully acknowledges HIDE and RISE consortia for their contribution to this document, and the following reviewers for their effective assistance in improving the quality of this report:*

**Kamlesh Bajaj**, Data Security Council of India (INDIA)

**Alessandro Caloprisco**, Italian Data Protection Authority (ITALY)

**Nigel Cameron**, Centre for Policy on Emerging Technologies (USA)

**Alastair V. Campbell**, National University of Singapore (SINGAPORE)

**Chi-Shing Chen**, National Cheng-Chi University (TAIWAN)

**Frediano Maria Di Carlo**, Eltag Datamat SPA (ITALY)

**Simon Dobrisek**, University of Ljubljana (SLOVENIA)

**Juliet Lodge**, University of Leeds (UK)

**Ajay Kumar**, The Hong Kong Polytechnic University (HONG KONG)

**Niovi Pavlidou**, Aristotle University of Thessaloniki (GREECE)

**Max Snijder**, European Biometric Forum, (IRELAND)

**Kush Wadhwa**, Global Security Intelligence (USA)

**David Zhang**, The Hong Kong Polytechnic University (HONG KONG)

A special thanks to Prof. **Irma van der Ploeg** (Zuyd University) who participated in the writing of an early version of this report.

Dr **Rene von Schomberg** (European Commission, DG Research, Ethics and Governance) was the DG RTD contact point for this report.

[This page has been left intentionally blank]



