THE TWILIGHT ZONE OF PRIVACY FOR PASSENGERS ON INTERNATIONAL FLIGHTS BETWEEN THE EU & USA

Alenka Kuhelj[*]

ABSTRACT

Terrorism is a serious threat for contemporary democracies. Air traffic represents an area especially exposed to potential terrorist threats. In order to combat terrorism, the governments are ready to use different means, among them collection, mining and storage of personal data of the individuals. Following the US example, a frontrunner in this area, the EU is preparing a new system of data exchange related to passenger name record (PNR). This should come as no surprise, since almost every terrorist plan involves, in one way or another, air travel. With the aim of establishing more security in air travel, the US and the EU signed a series of agreements dealing with exchange of personal data after the US insisted that such an exchange could enhance the possibility of combating terrorism. Here the EU follows a more cautionary approach, insisting that any antiterrorist policy must respect human rights, especially here, the right to passenger privacy. Nevertheless, the EU often goes beyond what is legally permissible and encroaches into the privacy of the individuals.

[*] Associate Professor of Law, Ph.D., LL.M., University of Ljubljana, Slovenia; Vice-Dean for International Relations at the Faculty of Administration. I'd like to dedicate this article to my children, Max and Athena as the passengers of "a new generation" who can not even imagine how easy, unintrusive and uncomplicated air traveling in the past was.

INTRODUCTION

The protection of privacy is an increasingly important issue and, given technological developments, one that demands appropriate legal and practical solutions. In a sophisticated technological and information environment offering new inventions and improvements in the field of surveillance and control on a daily basis, states are increasingly pushing the right to privacy into the background. The state's interest in achieving complete surveillance of the individual has resulted in encroachment on people's intimate space and privacy. Governments justify this encroachment by referring to the need to protect other, conflicting rights. This paper addresses the clash between two values, security and privacy, both legally protected human rights, in the context of intercontinental (EU-US) passenger air transportation.

EU-US travel is becoming increasingly common, in line with the general growth in air traffic. According to Eurostat data, passenger air transportation increased in the first half of 2008 by 4.4% compared to the first half of 2007.[1] Connections between EU and North America increased by 4.3%.[2] Statistical analyses of travel between the US and the EU since 2003 indicate a significant rise in the number of passengers flying between those territories (on approximately 215,000 transatlantic flights a year).[3] Each year over forty-five million passengers cross the Atlantic. Further increases in transatlantic travel can be expected following the new EU-US "Open Skies" agreement, which came into force on March 30, 2008 and liberalized air transportation.[4] This agreement allows European and US airlines to fly between any EU and US airports without restriction.[5]

---

[1] LUID DE LA FUENTA LAYOS, EUROPEAN COMMISSION, EUROSTAT, PASSENGER AIR TRANSPORT – MONTHLY PARTIAL DATA FOR 2008: DATA IN FOCUS, 10/2009 (Apr. 23, 2009), http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-010/EN/KS-QA-09-010-EN.PDF.

[2] EUROPEAN COMMISSION, GERMAN AEROSPACE CENTER, ANALYSES OF THE EUROPEAN AIR TRANSPORT MARKET, ANNUAL REPORT 2008 23-24 (JUNE 2009), http://ec.europa.eu/transport/air/observatory_market/doc/annual_2008.pdf.

[3] Luis De La Fuente Layos, *Air Transport between the EU and the USA, Statistics in Focus – Transport*, EUROSTAT, July 2006, *available at* http://www.eds-destatis.de/en/downloads/sif/nz_06_07.pdf.

[4] Air Transport Agreement, U.S.-E.U., Apr. 30, 2007, *available at* http://www.state.gov/documents/organization/114872.pdf.

[5] *US, EU Ink 'Open Skies' Pact*, EU BUSINESS, May 1, 2007, *available at* http://www.eubusiness.com/Transport/open-skies.32 (The IACA observed that the agreement

Unlike airlines, individual travellers have experienced a significant increase in the restrictions imposed on them. Acts of terrorism and terrorist threats, to which airlines are now understandably extremely sensitive, have led the US and EU to tighten security measures for travel and entry to their territory. The threat of terrorism has been the state's justification for security measures based on the collection and use of information on passengers or potential passengers.[6] For citizens, the resulting exposure to checks, surveillance, and discretionary measures by state agencies represents a major encroachment on their privacy. Passengers have no possibility of viewing the collected and stored data, and therefore have no legal means to protect their privacy. The system exists on a completely 'take it or leave it' basis – the encroachments are absolute requirements for transatlantic air travel. Therefore, a decision to fly not only entails a choice of travel destination, but also an acquiescence to authorities' surveillance mechanisms checking, collating, using, and storing the most intimate personal data of a potential passenger (e.g. infectious diseases, HIV status, eating habits, ethnic identity, and religious allegiance).[7] In addition to accessing personal data, state authorities may also carry out other security and surveillance measures, such as measuring passengers' body temperature to detect those infected with swine flu.[8]

Globalization and people's growing mobility were initially accompanied by the idea of a 'globalization that eliminates borders'. The

---

had not provided equal benefits to each party, since US carriers have full access to the EU internal market, while European carriers still face restrictions in accessing the US internal market); *see EU-US Tentative 'Open Sky' Agreement: One Sided Deal Brings No Real Benefits for European Carriers*, IACA, Mar. 7, 2007, http://www.iaca.be/index.cfm? 4666 555D- BDBE-2776-0C4A-3D59741D8E01.

[6] Even if someone who has reserved a seat on a flight cancels the ticket, the data collected on them and sent from the EU to the US are not deleted from the data registers.

[7] *See* U.S. Department Homeland Security, Frequently Asked Questions Regarding Customs and Border Protection Receipt of Passenger Name Records Related to Flights Between The European Union and The United States, http://www.dhs. gov/xlibrary/assets/ privacy/privacy_faq_pnr_cbp.pdf (last visited June 1, 2010) (In addition to other data such as passenger name, address, telephone number, travel schedule, address in the US, seat number and number of baggage items, detailed information on booking, booking agency, means of payment, frequent flier membership.).

[8] States not only justify passenger surveillance on the grounds of counter-terrorism security, but also health security. The passenger's interest in addition to physical security includes maintaining the same state of health as at the start of the flight. Catching AIDS, bird flu or swine flu or other infectious diseases is not in the interest of the individual or the authorities. Greece is one country (as well as Australia, China, Singapore, South Korea, and Vietnam, *inter alia*), that measure passenger temperature on arrival at the airport without their permission, and on that basis decide whether to admit the passenger to the country; *see also Passenger Screening at the Airports in Crete for Swine Flu*, CRETE GAZETTE, July 27, 2009, *available at* http://www.cretegazette.com/2009-06/crete-airports-swine-flu.php.

world has become 'smaller' and easier to traverse, but passengers have also become subject to much greater surveillance. Surveillance technology has changed borders rather than eliminate them, and Europe and the US have become the most protected zones of travel in the world. Given these changes, maintaining a balance between security, privacy, and the values of a transparent democratic society has become a task that increasingly demands careful consideration from individual states, such as the US and EU.[9]

Information globalization has changed our social environment by facilitating numerous forms of communication, from business to purely private. On the other hand it has deeply impinged on individual privacy, particularly because states all too often poorly supervise the storage and use of private data, leaving such tasks to the data collector. The most pressing legal issue is the transfer or flow of data because states have different means of protecting individual privacy. Just using the Internet involves sending personal information to other users on a daily basis. Even reading news often requires registering as a user, which can provide advertisers with a range of private information. In the case of travelling, passengers provide the personal data voluntarily, and generally remain unaware that states are using their data to build databases that have no time limit for retention and may be used in various ways not necessarily related to the purposes for which they submitted it.

As a result of the September 11th terrorist attacks in the US and a number of acts of terrorism in Europe, the intensity of personal data collection has increased. The collection, editing, comparison, distribution, storage, and use of private data has led to greater state control over individuals' movements, financial standing, behaviour, illnesses, sexual habits, and other personal characteristics important to self-definition. States justify the high levels of data collection as part of the fight against terrorism.[10] Based on information acquired from the surveillance of individuals, the notion of a 'security state' has replaced the previous goal of the welfare state.[11] The US National Security Agency ("NSA") stresses that if its current system had been in place before 9/11 it could have identified at least some of the terrorists involved, and perhaps even prevented the terrorist attack.[12] "It's the largest database ever assembled in the world," said one

---

[9] Natalie La Balme & Edouard de Tinguy, *United in Diversity? in Challenge Europe, Is Big Brother Watching You and Who is Watching Big Brother?* 9 (EUROPEAN POLICY CENTER 2008).

[10] *See* COUNCIL OF EUROPE, GUIDELINES ON HUMAN RIGHTS AND THE FIGHT AGAINST TERRORISM (2002) http://www.coe.int/T/E/Human_rights/h-inf(2002)8eng.pdf.

[11] DAVID LYON, SURVEILLANCE STUDIES (AN OVERVIEW) 119 (Polity Press, Cambridge, 2007).

[12] Jason Leopold, *Bush Ignored 9/11 Warnings*, TRUTHOUT, Jan. 31, 2006, http://www.

person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation.[13] The agency's goal is "to create a database of every call ever made" within the nation's borders, this person added.[14]

Information on Internet communications and plans of attacks US forces found when destroying Al Qaeda terrorist training camps in Afghanistan have reportedly proven useful in taking action against terrorism. State surveillance may further a state's interest in ensuring security, but it remains a sensitive encroachment into the personal sphere of the individual. This is particularly true when security measures result in the categorisation of individuals based on their personal information. The security state uses various methods to ensure the continual surveillance of people and national borders. The fact that the FBI's Terrorist Screening Centre, according to 2008 data, included the names of over 900,000 people, with 20,000 new names added each month, speaks for itself.[15] Furthermore, deletion from the list is very complicated, with no proper set of legal guidelines.[16] Computerisation and online searching for personal data have given counter-terrorism and related security measures a new dimension. According to FBI agent Mike German, this new dimension is harmful because it leads to the neglect of traditional intelligence agents that were the primary, valid, and direct source of information gathering until recently.[17] Terrorist organisations, such as Al Qaeda, are aware of intelligence agency tactics and use extremist websites to order their adherents to take action to avoid suspicion in their actions and internet communications.[18]

States may restrict and prevent, or permit and facilitate our passage

---

truthout.org/article/jason-leopold-bush-ignored-911-warnings ("President Bush and Vice President Cheney have publicly stated that the top-secret domestic spying program Bush authorized in 2002 could have thwarted the 9/11 attacks had the controversial, and possibly illegal, measure been in effect prior to the terrorist strike on the World Trade Center and the Pentagon."). The NSA reports continually to the U.S. Congress on its data collection activities.

[13] Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_ x. htm.

[14] *Id.*

[15] LYON, *supra* note 11, at 118-19 (". . . the security state, which also fosters predominant processes of risk management; the routinizing of 'states of emergency' and of 'exceptional circumstances' – a process that has been accentuated since the events and aftermath of 9/11 . . . ").

[16] *See Know-alls*, ECONOMIST, Sept. 27, 2008, at 68 (data taken from the American Civil Liberties Union report).

[17] *Id.*

[18] *Id.* ("Tricks such as calling phone-sex hotlines can help make a profile less suspicious.").

through its borders on the basis of our personal data.[19] The use of biometrics and the collection of information in databases is central to these determinations.[20] The question is should states' assertions of the goal of detection of terrorism through the collection of personal information and data convince us, as 'unproblematic' citizens, that we should submit any data, without limitation, including the most intimate, to the state? Or, are we willing to set boundaries for the security state's unrestricted and increasingly demanding incursions into our privacy?

I. PRIVACY OR SECURITY – WHY NOT BOTH?

States are introducing increased surveillance of individuals – assuring those individuals that this heightened security is for their benefit, while at the same time using (or abusing) surveillance for actions that society would not normally approve, or would even actively oppose. Mass security and surveillance systems that include biometrics, electronic ID cards, and other methods have become part of our everyday life. We provide information to state, public, or private entities, generally without hesitation, despite the fact that in normal circumstances citizens would at least express considerable dissatisfaction with such systems. We accept these intrusions into private matters because individuals are susceptible to the idea that they must sacrifice part of their privacy in exchange for a 'higher' goal such as security. Individuals generally are not aware how "violent and uncompromising" today's authorities have become.[21]

Surveillance is also controversial because placing suspects under surveillance turns the legal assumption of innocence on its head. Persons defined as suspicious bear the burden of ridding themselves of the suspicion.[22] Using surveillance to categorise people as innocent or guilty, suspicious or not, lawful or unlawful, has transformed society and the state, which now require 'identity management.'[23] Identity management uses

---

[19] LYON, *supra* note 11, at 120.

[20] *See* MICHAEL FOUCAULT, DISCIPLINE& PUNISH: THE BIRTH OF THE PRISON (Vintage, 1995), for more on the idea of 'enforced' order and discipline from a post-modern point-of-view, and how creating order and discipline (through reward and punishment) on one hand creates the same proportion of disorder on the other.

[21] *See* JON L. MILLS, PRIVACY, THE LOST RIGHT 9-11 (Oxford Univ. Press, 2008), for people's erroneous assumptions about state, public, and private protection of their data.

[22] G.T. Marx, *Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information –"Hey Buddy Can You Spare a DNA?",* http://web.mit.edu/gtmarx/www/softsurveillance.html.

[23] Definition of Identity Management, http://www.bitpipe.com/tlist/Identity-Management.html (last visited June 1, 2010) "Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by

biometrics to authenticate identity, approve the right of access (entry), and act as a password. The model, as developed and originally used in business Internet communications, restricts access to specific information to only those who meet a number of preconditions, while also protecting their privacy.[24] Today, states are extending the use of identity management, with biometrics incorporated into state supervisory systems in non-business contexts, including surveillance of air transportation passengers.[25] The first state to introduce an automatic surveillance system was the 'post-terrorist' US. The Patriot Act[26] authorised the state to record telephone conversations, log calls, review emails, monitor computers, monitor health and financial standing, and use other forms of surveillance that previously would have been completely unacceptable. Anti-terrorist legislation has also affected the organization and control of international transportation through the introduction of ATS (Automated Targeting System) computer systems and the US-VISIT (Visitor and Immigrant Status Indicator Technology) system.[27]

The UK developed US-style strategies to combat terrorism and was the first state to introduce them to the EU.[28] Concurrently, individual measures gradually began to spread across the EU. Following the major terrorist acts in Madrid (March 11th, 2004) and London (July 7th, 2005) the security state concept was 'Europeanised' for the fight against terrorism.[29] In 2004, the EU adopted the Declaration on Combating Terrorism, which, declared the fight against terrorism and aimed to have a psychological impact on EU citizens.[30] The Council of the EU responded to a proposal from the EU presidency and counter-terrorism coordinator in November 2005 by adopting a new Counter-Terrorism Strategy[31] and, in June of the same year,

---

associating user rights and restrictions with the established identity."

[24] LYON, *supra* note 11, at 133.

[25] U.S. Department of Homeland Security, US-VISIT Biometric Identification Services, *available at* http://www.dhs.gov/files/programs/gc_1208531081211.shtm#two (last visited June 1, 2010).

[26] USA Patriot Act, H.R. 3162, 107th Cong. (2001).

[27] *See* Marc Rotenberg, *Recent Privacy Developments in the United States, Particularly with Respect to Travelers Using Air Transport*, Mar. 21, 2007, *available at* http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/rotenberg_/rotenberg_en.pdf (reviewing of US Privacy Developments).

[28] Freedom, Security, and Justice, *International Dimension*, http://ec.europa.eu/justice_home/fsj/terrorism/international/fsj_terrorism_international_en.htm (last visited June 1, 2010).

[29] COUNCIL OF THE EUROPEAN UNION, DECLARATION ON COMBATTING TERRORISM (Mar. 25, 2004), http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf [hereafter DECLARATION ON COMBATTING TERRORISM].

[30] *Id.* at 18 ("[T]he Member States and the acceding States shall accordingly act jointly in a spirit of solidarity if one of them is the victim of a terrorist attack.")

[31] COUNCIL OF THE EUROPEAN UNION, THE EUROPEAN UNION COUNTER-TERRORISM

a more detailed Action Plan on Terrorism.[32] The documents commit the EU to counter-terrorism measures on a global level. The European security strategy also promotes solidarity between Member States and with foreign and justice ministries involved in strategy formation.[33] Other important facets are the cohesion effect among EU citizens and, in part, the closing of the democratic deficit faced by the EU.[34]

One of the most important measures at the EU level is the creation of a system to exchange records of air passengers' names. Members of terrorist groups mostly travel by air to meet to plan and train for terrorist actions (regardless of whether aircrafts are the target). If law enforcement agencies in the EU have already acquired and compared data from different passenger records, this will assist in detecting terrorists on the move and discovering their future plans.[35] However, the EU emphasizes that counter-terrorism activity must be respectful of human rights, particularly the passenger's right to privacy (including personal data protection).[36] Therefore, in 2007, the European Commission's proposals to improve the EU's capacity in combating terrorism included a proposal for a "Framework Decision on the use of the Passenger Name Record (PNR) for law enforcement purposes."[37] This is particularly important in terms of protecting individual privacy in relation to the state as "collector and user" of data on individual air passengers.[38] The European Council adopted a resolution for 2007-2013 introducing a special program: Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks.[39] Also in light

---

STRATEGY, 14469/4/05 REV4 (Nov. 30, 2005), *available at* http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf.

[32] *See* European Commission, Action Plan on Terrorism (2004-2005), http://ec.europa.eu/justice_home/fsj/terrorism/strategies/fsj_terrorism_strategies_political_en.htm (The Action Plan offers technical details and possibility to check the progress in the fight against terrorism. The Plan has been updated every six months before the June and December.).

[33] DECLARATION ON COMBATTING TERRORISM, *supra* note 29.

[34] The issue of a democratic deficit arises from the alienation of the EU, as a supranational body, from its citizens, since the EU is organised more as an "institutional organisation" than an organisation that would unite its citizens under the motto "united in diversity".

[35] Press Release, European Union, Fight Against Terrorism: Stepping Up Europe's Capability to Protect Citizens Against the Threat of Terrorism, IP/07/1649, in Brussels (Nov. 6, 2007), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1649.

[36] *Implementation of the Action Plan to Combat Terrorism*, Doc. 15704/05, (Dec. 12 2005), *available at register.consilium.europa.eu/pdf/en/05/st15/st15704.en05.pdf* .

[37] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes, COM (2007) 654 final (June 11, 2007) [hereafter *Council Framework on PNR*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007PC0654:EN:NOT.

[38] *Id.*

[39] Council Decision 2007/124/EC, 2007 O.J. (L 58) (The aim is to support efforts by Member States to protect people and critical infrastructure against risks relating to terrorist

of the EU counter-terrorism strategy, the European Parliament adopted a resolution on the external dimension of the fight against terrorism.[40]

The purpose of this EU legislation is to find a common base to address terrorism because Member States adopt decisions in the third pillar of the EU via intergovernmental co-operation.[41] By adopting the various measures, the EU aims to ensure the best possible protection against terrorism.[42] However, it all too often forgets citizens and their rights, making it appropriate to question the purpose of the EU and whom it is designed to protect. Is it protecting itself, its institutions, and the states as its constituent parts? Or is it actually protecting its citizens? And who is the EU protecting citizens from? Is it really against terrorism as an idea, or terrorists who, as individuals, may even be its citizens? And where is the line drawn between the rights of 'honest citizens' on the one hand and, on the other, the EU's right to ensure the security of its citizens and its own integrity on behalf of society as a whole? These and numerous other counter-terrorism issues remain unresolved in the EU, relating specifically to its *sui generis* supranational authority.

The use of counter-terrorism mesures naturally raises the issue of the propriety of surveillance of the individual. Surveillance is an expression of executive power, but also includes an obligation on those engaged in it to consider and respect the rights of the individual. This is the case whether it involves mass surveillance measures, such as those practiced by the Department of Homeland Security ("DHS") in the US, or small-scale measures such as the surveillance of children via cameras on school buses travelling to small rural schools. As an expression of power and control, it

---

attacks and other security-related risks, and the preparedness for such risks and their prevention.).

[40] Resolution on the External Dimension of the Fight Against International Terrorism, EUR. PARL. DOC. 2006/2032(INI) (2007).

[41] *See* P. CRAIG, G. DE BURCA, E.U. LAW, TEXT, CASES, AND MATERIALS 229-67 (Oxford, 4th ed. 2007) (The EU (since the Maastricht treaty) has comprised three pillars, with each pillar of the division having its own characteristics: The European Community (First Pillar), the Common Foreign and Security Policy (Second Pillar) and Police and Judicial Cooperation in Criminal Matters (Third Pillar). Co-operation on the second and third pillars is intergovernmental, so the European Commission and Parliament play only a minor role in decisions, which is reflected in the conclusion of international treaties. In both areas, the EU is represented by the country holding the rotating presidency and the high representative for the Common Foreign and Security Policy, with the country holding the presidency acting as negotiator. The intergovernmental nature of the co-operation means that unanimous consent must normally be achieved to conclude an agreement, though a qualified majority is sufficient in some cases.).

[42] DECLARATION ON COMBATTING TERRORISM, *supra* note 29, at 9 (Noting that one of the strategic objectives is: "To maximise capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and prevent terrorist attacks.")

demands respect for human rights as a counterweight. The problem is that we are unaware of the most questionable and legally unjustifiable forms of surveillance. One such example in the US is the 'black ops' of the NSA, in which the NSA processes data in detail and stores it for people deemed of interest to the US, and who the authorities want placed under scrutiny.[43] In all likelihood, similar programmes are kept secret from the public in EU states. In the past these states have followed US or Russian 'innovations' in this field. One example of clandestine surveillance is closed circuit camera systems, first widely installed in the United Kingdom among EU Member States.[44] In London, the government installed over 1.5 million cameras during the past decade in part to detect terrorist bombing threats.[45] These cameras record a typical Londoner an average of around 300 times a day,[46] though to date this method has not detected a single terrorist. Despite the ineffectiveness of this practice, the United States has followed the UK model of using surveillance cameras, installed not only on public highways, schools, parks, and government buildings, but also in other public buildings and spaces.[47] We might ask which is more important: that our government know what we are all doing in order to make us feel safe, or to retain our privacy, which is increasingly being lost. "*There's no place to hide*" is becoming a motto for our daily lives.[48]

II. RANGE OF COUNTER-TERRORISM SURVEILLANCE MEASURES – JUST NAME IT!

Counter-terrorist security measures that encroach to varying degrees on individual privacy are causing a clash between two sets of values: the right to security and the right to privacy. In both the EU and the US these measures have taken a variety of forms.

Travellers who want to travel by air from an EU state to the US must successfully pass a number of US preliminary control phases before officials permit them to board a plane and land on US soil. However, even after

---

[43] GlobalSecurity.Org, NSA Activities, http://www.globalsecurity.org/intell/ops/nsa-activities.htm (last visited June 1, 2010).

[44] William R. Webster, *The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK*, SURVEILLANCE AND SOCIETY, http://www.surveillance-and-society.org/articles2(2)/diffusion.pdf (last visited June 1, 2010).

[45] Angie C. Marek, *Trying To Keep New York Safe After The London Bombings, Transit Vulnerabilities Loom Larger Than Ever*, U.S. NEWS AND WORLD REPORT, Jul. 31, 2005, *available at* http://www.usnews.com/usnews/news/articles/050808/8transit.htm.

[46] Elecronic Privacy Information Center (EPIC), Video Surveillance Information Page, http://epic.org/privacy/surveillance/ (last visited June 1, 2010).

[47] *Id.*

[48] Taken from the title of the Robert O'Harrow book, THERE'S NO PLACE TO HIDE (Free Press, 2005).

meeting the preconditions and obtaining permission to travel to the US, passengers cannot be certain they will actually be allowed to enter the US. After landing, they must undergo biometric and border controls.[49] Passengers must show Customs and Border Protection staff that they are entitled to enter and that no reasons exist for denying entry on the basis of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.[50]

President George W. Bush tightened counter-terrorism measures in 2002 with the introduction of the Smart Border[51]program, intended to strengthen security on the US-Canadian border.[52] He allocated 10.7 billion dollars to the fight against terrorism, illegal immigration, and drugs, an increase of 2 billion dollars from the previous year.[53] The US Government partially justified the Smart Border by stating that it would allow "non-suspicious" (and therefore legal) passengers to cross the border more quickly, while making illegal entry more difficult or prevent it in full.[54] The new measures include the introduction of the Entry-Exit Tracking System.[55]

---

[49] U.S. Department of Homeland Security, US-VISIT What to Expect When Visiting the United States, http://www.dhs.gov/files/programs/editorial_0525.shtm (last visited June 1, 2010).

[50] Federal Financial Management Improvement Act of 1996 (IIRIRA), Pub. L. No. 104–208, 110 Stat. 3009 (1996),

[51] Foreign Affairs and International Trade Canada, The Canada-U.S. Smart Border Declaration Action Plan for Creating a Secure and Smart Border, The Secure Flow of People, http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.as.

[52] U.S. Department of Homeland Security, Office of the Press Secretary, Securing America's Borders Fact Sheet: Border Security, (Jan. 25, 2002), http://www.dhs. gov/xnews/releases/press_release_0052.shtm ("According to a White House statement: The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits . . . [a]greements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles.").

[53] *Id.* ("In the 2003 Budget, the President will propose approximately $11 billion for border security, including $380 million for the Immigration and Naturalization Service to construct a state of the art Entry-Exit visa system. In total, this will represent an increase of $2.2 billion from the 2002 Budget for border security.").

[54] 11 MIGRATION DIALOGUE: RESEARCH & SEMINARS, SMART BORDER ACTION PLAN: STATUS REPORT, No. 4 (2005), http://migration.ucdavis.edu/rs/more.php?id=170_0_2_0.

[55] Federation for American Immigration Reform, Automated Entry-Exit System: Key to National Security, http://www.fairus.org/site/PageServer?pagename=iic_immigrationissue centers19fa (last visited June 1, 2010) ("Every year, millions of foreigners enter the US as 'nonimmigrants' (visitors or workers) for a limited period. Although they are expected to return home at the end of their visit, there is no effective means for detecting those who do not . . . . Registration of visitors is commonplace in virtually every comparable country. In the

This system increases the traceability of passengers that do not hold US citizenship. It makes it possible to trace people who cross US borders and verify whether they remain in the state legally or exceed their visas and remain in the country illegally.[56]

The EU followed the US measures by making its own conditions for travel between the EU and outside countries more stringent, with numerous security measures emulating US examples (e.g. PNR and ETA/ESTA).[57] However, enshrining these new measures in EU law was a considerably more complex and lengthy procedure than in the US. According to EU legislation, conditions must be equal for all Member States.[58] This extends and complicates the process because each Member State has a veto.[59] At the same time, the system of consent enhances the democratic nature of decisions adopted, and positions expressed, by the EU. The EU therefore faces much more inefficiency in this field because adopting measures proposed by the European Commission can take an entire year or more.[60] After the European Commission announces a new measure, it must put it forward for adoption by the European Council and Parliament (it does not merely give its opinion: it shares legislative power equally with the Council). If Council and Parliament cannot agree on a piece of proposed legislation, it is put before a conciliation committee, composed of equal numbers of Council and Parliament representatives.[61] By contrast, the US

US, requirements that foreign visitors register with the government are not new; some form of registration has been required since 1940. Sections 261 through 266 of the immigration and Nationality act already require that aliens staying longer than 30 days register and be fingerprinted.").

[56] UNITED STATES GENERAL ACCOUNTING OFFICE, HOMELAND SECURITY: OVERSTAY TRACKING IS A KEY COMPONENT OF A LAYERED DEFENSE 12 (2003), http://www.gao.gov/new.items/d04170t.pdf.

[57] ESTA (Electronic System of Travel Authorization).

[58] Europa, EU Policies: Common Foreign and Security Policy (CFSP), http://europa.eu/scadplus/constitution/foreignpolicy_en.htm (last visited June 1, 2010).

[59] The EU decides on matters in the second and third pillars (common foreign and security policy and police and judicial co-operation in criminal matters) using the intergovernmental method. This means that the European Commission shares the right to put forward an initiative with the Member States, with the unanimous consent of the European Council usually required for a decision to be passed. The working process in these two pillars is driven by the need to achieve unanimity among all Member States on the specific issue.

[60] *See Q&A: How UK adopts EU laws*, BBC NEWS, July 21, 2009, http://news.bbc.co.uk/2/hi/europe/8160808.stm (Because "the negotiations between 27 different countries, each with its own priorities, policies and domestic legal systems, can be long and drawn out.").

[61] A Lisbon Treaty extended the co-decision procedure to govern forty new fields. Between them is a field of freedom, security and justice- border checks, immigration, police cooperation and judicial cooperation in criminal matters. More about the co-decision procedure *at* http://europa.eu/institutions/decision-making/index_en.htm.

government can put measures in place rapidly[62] without any need for prior announcements or warnings to outside states. As a leading country in counter-terrorism, US positions and policies dictate the conditions and measures used in this field.[63] The EU's subordinance to the US is also due to US foreign policy strength and the US's exploitation of the EU's weakness, including its inability to make rapid decisions due to its *sui generis* structure and the diversity of its twenty-seven Member States.

One example of EU inefficiency is the adoption of the European PNR and Electronic System for Travel Authorization ("ESTA") system. After pressure from Member States, the European Council abandoned a Commission proposal on the introduction of PNR and after seven months of deliberation, from November 2007 to July 2008, suggested a different system of surveillance of people travelling from third states.[64] In the future, if states decide that specific counter-terrorism measures are suitable, the process should be made quicker and more efficient by considering both the justification and lawfulness of the act.

Following the US pattern, the EU will introduce an entry-exit system for passengers travelling to the EU from third states for up to three months.[65] The system mirrors the US model, and will record both entry data (time and location) and length of permitted 'visit' to the EU. In this manner, authorities will immediately be able to determine whether an individual has acted legally or otherwise at the time of exit or on expiry of a permit to stay. However, even on this measure, the EU is only now reaching agreement on the application of the system that is planned for introduction in 2015, an

---

[62] *See* Press Release, Dept. of Homeland Sec., Electronic System for Travel Authorization (ESTA) 282 (June 3, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1212498415724.shtm ("The Department of Homeland Security (DHS) has announced the ESTA Interim Final Rule (IFR), which establishes a new online system that is part of the Visa Waiver Program (VWP) and is required by the Implementing Recommendations of the 9/11 Commission Act of 2007 . . . . The ESTA web-based system will be available for voluntary applications after 1 Aug 2008 . . . . DHS anticipates that the Secretary of Homeland Security will issue that notice in November 2008, for implementation of the mandatory ESTA requirements on 12 Jan 2009.").

[63] See Kenneth Roth, *Neglecting human rights: Not the way to fight terrorism*, NY TIMES, Jan. 15, 2003, http://www.nytimes.com/2003/01/15/opinion/15iht-edroth_ed3_.html, *and* Ferruccio Pastore, Jörg Friedrichs, and Alessandro Politi, *Is There a European Strategy Against Terrorism? A Brief Assessment of Supra-National and National Responses*, CENTRO STUDI DI POLITICA INTERNAZIONALE, Feb. 2005, at 16, http://www.cespi.it/WP/wp12-terrorismo.pdf, for a discussion about the United States' role at fighting terrorism.

[64] The EU cannot decide whether to adopt its own ESTA or PNR system or both together. At the EU-US summit in Slovenia on March 13, 2008, representatives of the EU asked the US to provide with additional information on the ESTA to facilitate decision-making. By the first half of 2009, the EU had still not adopted the PNR or ESTA system.

[65] Europa, Press Release Rapid, EU policy to fight illegal immigration, July 19, 2006, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/296.

unreasonably lengthy 'preparatory' period.[66]

A. Passenger Name Record (PNR) and Advance Passenger Information (APIS)

In its "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions" of February 13th, 2008,[67] the European Commission proposed the introduction or preparation of a number of border-management measures, including the VIS (Visa Information System),[68] APIS (Advance Passenger Information System), PNR, and ESTA. These measures already exist in some states, such as the US. Australia, Canada, Denmark, France and the UK have also introduced PNR data collection.[69] States primarily use PNR and ESTA for surveillance of transatlantic passengers, while API(S) is linked to the airlines, which acquire data on the permission (or prohibition) for passengers to board or travel.[70]

In order to regulate civil aviation security and protect against terrorism and in the spirit of the "21st Century Smart Border,"[71] the US passed the Aviation and Transportation Security Act.[72] The act made it compulsory, before a flight "into, from or via" the US, for airlines to enable electronic access by DHS to the personal data of all travellers on these routes as found

---

[66] Renata Goldirova, *Brussels to tighten EU external borders*, EU OBSERVER, Feb. 6, 2008, http://euobserver.com/9/25606.

[67] *Commission from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Examining the Creation of a European Border Surveillance System*, COM (2008) 68 final (Feb. 13, 2008).

[68] The VIS only applies to third-country nationals requesting a short-term visa. From the 2012 introduction of VIS, the EU will verify the authenticity of visas and the identity of the bearer. The system envisages the inclusion of biometric data, such as facial image and fingerprints.

[69] European Parliament, Parliamentary Questions, Oct. 8, 2008, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+OQ+O-2008-0100+0+DOC+XML+V0//EN (". . . data originally collected for commercial purposes, while now serving an increasing number of security purposes (such as aviation security, immigration control, fiscal fraud, money laundering, preventing terrorism and crimes and prevention of communicable diseases, etc.) . . . . These purposes and the related conditions for data treatment differ from country to country and evolve constantly . . .").

[70] U.S. Embassy Tallin, Estonia, Visa Waiver Program, ESTA Frequently Asked Questions, http://estonia.usembassy.gov/esta_questions3.html (last visited June 1, 2010) ("While U.S.-bound carriers will not receive the ESTA application information that travelers provide to DHS, they will receive confirmation of a passenger's ESTA status via the Advance Passenger Information System (APIS)/APIS Quick Query system indicating whether an ESTA is required and whether authorization has been granted.").

[71] Maria Veronica Perez Asinari & Yves Poullet, *The Airline Passenger Data Disclosure Case and the EU-US Debate*, 20 COMPUTER LAW & SECURITY REPORT 2, 98 (2004).

[72] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71 (2001).

in the PNR.[73] This is a passenger database that the US uses for surveillance of domestic and international air transportation passengers.[74] US federal authorities compare the data to other databases held by the Transportation Security Agency ("TSA"), DHS Customs and Border Protection departments, and data from ATS.[75] They use the PNR to decide whether a passenger may or may not be permitted to enter US territory.[76] However, most air passengers are unaware that their government PNR record exists because the travel agency or airline collects the data and must subsequently transfer the data to the US seventy-two hours before the flight.[77] The first check on a potential passenger starts when the traveller books an airline ticket, at which point the travel agency or airline requests a range of personal information from the passenger, creates a passenger profile, and stores this data in a dedicated file. There are nineteen compulsory data items (the previous agreements between the US and EU specified thirty-four) on the passenger, such as email address, flight number, data on fellow passengers,

---

[73] This Aviation and Transportation Security Act has been followed by secondary legislation, notably the document "Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States", Department of the Treasury Customs Service, 66 Fed. Reg. 67, 482-67, 485 (Dec. 31, 2001) (to be codified at 19 C.F.R. pt. 122 and 178), and the document "Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States", Department of the Treasury Customs Service, 67 Fed. Reg. 42, 710-42, 713 (June 25, 2002) (to be codified at 19 C.F.R. pt. 122).

[74] U.S. Department of Homeland Security, Frequently Asked Questions Regarding Customs and Border Protection Receipt of Passenger Name Records Related to Flights between the European Union and the United States, http://www.dhs.gov/xlibrary/assets/ privacy/ privacy_faq_pnr_cbp.pdf.

[75] Statewatch News Online, *EU-US PNR Agreement, US changes the privacy rules to exemption access to personal data*, STATEWATCH, http://www.statewatch.org/news/2007/ sep/04eu-usa-pnr-exemptions.htm ("ATS-Passenger (ATS-P), one of six modules contained within ATS, maintains Passenger Name Record (PNR) data (data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel) that has been collected by CBP as part of its border enforcement mission. ATS-P's screening relies upon information from the following databases: Treasury Enforcement Communications System (TECS), Advanced Passenger Information System (APIS), Non Immigrant Information System (NIIS), Suspect and Violator Indices (SAVI), and the Visa databases (maintained by the Department of State) with the PNR information that it maintains."); U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM 4 (2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf.

[76] D.J. SOLOVE, M. ROTENBERG, & P.M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 60 (Aspen, 2006) ("In 2005, pursuant to a request by Marcia Hofmann of the Electronic Privacy Information Center, it was revealed that the FBI was keeping 257.5 million PNR records on the people who flew between June and September 2001.").

[77] Department of Honmeland Security, Remarks by Secretary Chertoff at a Press Conference on Secure Flight and the Advance Passenger Information System, Aug. 9, 2007, http://www.dhs.gov/xnews/releases/pr_1186693761881.shtm.

number and type of credit card used for purchase, purpose of travel, travel frequency, travel agency, seat number, and even data on services requested by the passenger (e.g. vegetarian or kosher meal, requesting a seat near an exit, request for seat next to infant cots).[78] The reduced number of data items requested (from thirty-four to nineteen) does not actually mean a reduction in database size, but merely the 'merging' of data categories.[79] More specific categories are now included in general categories, so there is no major difference from the previous system with a higher number of data items. US agencies do not delete data sent by airlines as part of 'passenger profiles' that is not necessary for compilation of the PNR, but rather stores such information it in databases.[80] Agencies also save to the PNR data on the date of ticket issuance (or internet e-ticket), the weight of luggage on check-in, and the check-in number.[81] If a purchaser does not use a ticket, this is also recorded in the PNR.[82] For passengers who are frequent customers of a travel agency or members of a frequent flyer programme there is far more data in their profile.[83] If US officials checking the data want further or supplementary information on bank accounts or email addresses, they may request them via the courts.[84] Officially, agencies delete the PNR, but in a manner that allows the data to remain 'traceable.'[85]

---

[78] *See* EDWARD HASBROUCK, *What's in a Passenger Name Record (PNR)?*, *in* THE PRACTICAL NOMAD: HOW TO TRAVEL AROUND THE WORLD (Avalon Travel Publishing, 4th ed. 2007), *available at* http://www.hasbrouck.org/articles/PNR.html (In 2003, DHS responded to an EU question on which data should be included in the PNR by listing 39 data items (in addition to name, address, home telephone number and date of birth), which were required to comply with the US CAPPS-II system.).

[79] Statewatch News Online, *EU: European Commission to Propose EU PNR Travel Surveillance System*, STATEWATCH, http://www.statewatch.org/news/2007/jul/03eu-pnr.htm.

[80] HASBROUCK, *supra* note 78.

[81] *Id.*

[82] *Id.*

[83] *Id.* ("That profile might include all the credit cards you regularly use (even if you aren't using them for this purpose); alternate addresses, phone numbers, and emergency contacts; names and other information on your family members or business associates who sometimes travel with you (even if they aren't on this trip); notes about your tastes and preferences ("prefers king bed", "prefers room on low floor in hotels", "always requests halal meal", "won't fly on the Jewish sabbath", "uses wheelchair, can control bowels and bladder"; "prefers not to fly Delta Airlines"); personal notes intended for the internal use of the travel agency ("difficult customer - always changing his mind"); department and project billing and approval codes for corporate travel; all your frequent flyer numbers (even ones you aren't using on this trip) and a wide variety of other information.").

[84] *See* STATEWATCH, UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP), http://www.statewatch.org/news/2006/jun/eu-usa-pnr-undertakings-may-2004.pdf.

[85] *Id.* ("A PNR can be cancelled, but the audit trail or "history" of the PNR, showing when and by whom each entry in the PNR was made, is always retained at least until the last

The DHR is supposed to store PNR data from flights between the EU and the US in an active analytical database for seven years, and in a dormant, non-operational database for eight years following that.[86] US obligations only permit access to data in dormant databases for separately defined cases or in the case of an identifiable threat.[87] Responsibility for defining separately defined cases and serious threats lies with DHS, as does acquisition of the permission to review these dormant databases.[88] The rules on storing PNR seemingly mandate the destruction of data after fifteen years, yet even here DHS has identified specific situations in which it may continue to use this data, such as cases in which an investigation is ongoing.[89] The US has also avoided publicly committing to destruction in other cases, and has deferred these issues until subsequent agreements with the EU.[90] This means that the US currently stores PNR data it receives from the EU in its databases without a time limit, or for a time it decides itself. The rules for active and dormant databases are therefore meaningless. Without the agreed and actual destruction of data, these rules do not ensure that the US will ever delete the personal data of EU citizens from its databases.

The US has also stipulated that European PNRs (which the EU would collect reciprocally from third country nationals, including the US, for entry into its territory) cannot require more information disclosure than the American PNR, or the US will withdraw from the agreement.[91] In addition

---

date of the reservations, active or cancelled, in the PNR.").

[86] Agreement between the European Union and the United States of America on the processing and transfer of

Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) [hereafter 2007 PNR Agreement], O.J. L 204/18, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf.

[87] *Council Framework on PNR*, *supra* note 37, art. 9 § 2 (". . . the PNR data may be accessed, processed and used only with the approval of the competent authority and only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime. Access to such data shall be limited to personnel of the competent authorities which will be specifically authorised for this purpose.").

[88] Council of the European Union, Agreement Between the European Union and the United States of America on Processing the Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), U.S.-E.U., No. 11304/07, June 28, 2007, *available at* http://www.statewatch.org/news/2007/jul/eu-usa-pnr-agreement-2007.pdf.

[89] 2007 PNR Agreement, *supra* note 86.

[90] *Id.*

[91] *Id.* ("DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory

to biometric passports, the EU is introducing biometric visas, and gradually, but consistently, progressing along the US path towards databases and the checking of individuals by means of PNR and ETA/ESTA systems.[92]

The first agreement providing US federal authorities with access to PNR data on travellers from the EU was the Agreement between the European Community and the United States of America on the processing and transfer of PNR data ("PNR Agreement).[93] The European Commission found that in regards to this agreement, the United States' Bureau of Customs and Border Protection provided adequate protections of PNR data ("Commission Decision").[94] However, the agreement did not remain valid for long. On May 30th, 2006, in response to petitions from the European Parliament, the European Court of Justice ("ECJ") ruled on the PNR Agreement[95] and the Commission's determination of the adequacy of the protection of this data[96]. The court annulled the Council Decision and the Commission Decision on grounds of an incorrect legal basis.[97] This opened up the potential for the annulled agreement to be replaced by numerous bilateral agreements reached independently between the US and EU Member States.

The ECJ decision failed in that it did not address the substantive issues of the agreement. The ECJ did not take an explicit position on whether the PNR Agreement disproportionately encroached on the rights of EU citizens, but instead took an easier course and annulled the Council Decision and Commission Decision on formal legal grounds.[98] In its judgment, the ECJ stated only that "neither the Commission decision on the adequacy of data

---

resolution. In the event that an airline passenger information system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight between the U.S. and the European Union, DHS intends, strictly on the basis of reciprocity, to actively promote the cooperation of the airlines within its jurisdiction.").

92 Tony Bunyan, *Statewatch EU: The Surveillance of Travel Where Everyone is a Suspect*, STATEWATCH, http://www.statewatch.org/news/2008/aug/eu-travel-surveillance.pdf.

93 Council Decision 2004/496/EC of 17 May 2004, 2004 O.J. (L 183) [hereafter Council Decision] (Council approval of the PNR Agreement) *available at* http://eur-lex. europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32004D0496:EN:HTML.

94 Commission Decision 2004/535/EC of 14 May 2004, (discussing the protection of personal data contained in the Passenger Name Record of air passengers transferred to the U.S. Bureau of Customs and Border Protection), *available at* http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=OJ:L:2004:235:0011:0022:EN:PDF.

95 Case C-317/04, Parliament v. Council, 2006 E.C.R. I-04721.

96 Case C-318/04, Parliament v. Commission, 2006 E.C.R. I-04721.

97 Joined Cases C-317/04 & C-318/04, Parliament v. Commission & Council, 2006 E.C.R. I-04721. In accordance with the ECJ judgment, the agreement remained in force for a further 90 days until September 30th, 2006 on the basis of legal certainty and to protect affected parties.

98 *Id.*

protection by the United States nor the Council decision approving the agreement on their transfer to that country had an appropriate legal basis".[99] The ECJ therefore did not test the substantive issues and avoided commenting on the questionable agreement and its compliance with Directive 95/46/EC[100] on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive").

In Case C-318/04, the ECJ was set to rule on whether the Commission Decision ensures adequate protection for data transferred from the EU. In fact, the ECJ ruled that the Commission Decision was incorrectly based on the Directive, which in Article 3(2) excludes its application to personal data processing operations "concerning public security, defence, state security . . . and the activities of the state in areas of criminal law."[101] The ECJ focused on the fact that airlines collected the data as part of their activities, including the sale of airline tickets, and therefore did not fall within the scope of Article 3(2) exclusions.[102] However, it stressed that in the specific case, the transfer of PNR exceeded the stated commercial purpose.[103] The transfer of data to a third country constitutes processing concerning public security and activities of the state in areas of criminal law, which Article 3(2) of the Directive excludes from the scope of that directive.[104] On these grounds, the ECJ annulled the Commission's decision on adequacy.

In Case C-317/04, the ECJ studied whether the Council Decision had a proper legal basis. As in the case involving the Commission Decision, the ECJ found that EU legislation (specifically Article 95 EC[105] in conjunction with Article 25 of the Directive[106]) does not provide a legal basis for the

---

[99] *Id.*

[100] Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (EC).

[101] Joined Cases C-317/04 & C-318/04, *supra* note 97.

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] Art. 95 [ex Art. 100 a] EC Treaty ("It's the main gate through which this massive influx of European standards and regulations is flowing is increasingly becoming the responsibility of the Community to ensure the approximation of the legal and regulatory provisions of the Member States, with the aim of creating and guaranteeing the smooth functioning of the internal market."); *see also* Hans-Peter Schneider, *"Ultra vires" – Limitations to judicial approximation in Europe – Why the ECJ put the Community institutions in their place*, *available at* http://www.law.harvard.edu/programs/iglp/events/2003-2004/Translation%20Prof.%20Schneider%20article%20171000.pdf.

[106] Council Directive 95/46/EC, *supra* note 100, art. 25 ("Transfer of Personal Data to Third Countries – Principles:1) The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures

Community's authority to conclude the agreement with the US. On this basis, the ECJ annulled the Council Decision approving the agreement.[107] The ECJ stated that as a result of the annulment of the decision on adequacy, and hence the subsequent Council Decision, it was unecessary to consider the other substantive grounds to which the European Parliament made reference (the principle of proportionality and breach of fundamental rights).[108] In the event that the ECJ had analyzed the application of Article 13 of the Directive,[109] it would have had to annul the Council Decision on formal and substantive grounds. The ECJ clearly wanted to avoid a substantive judgment on whether the plea was well founded.

An ECJ judgment on the substantive grounds of human rights protection would be a welcome clarification of the open substantive law issues regarding human rights requirements in the collection and transfer of PNR data to the US. Despite a new agreement that came into force in 2007, there remain unresolved and disputed issues.[110]

The ECJ judgment created a legal lacuna that EU Member States began to exploit by concluding bilateral contracts with the US.[111] For many EU Member States, the decision to operate independently in this area proved

---

an adequate level of protection; 2) The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country . . . .").

[107] Joined Cases C-317/04 & C-318/04, *supra* note 97.

[108] *Id.*

[109] Council Directive 95/46/EC, *supra* note 100, art. 13, ("Exceptions and Restrictions: 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security; (d) prevention, investigation, detection and prosecution of criminal offences . . .").

[110] *See* Michele Nino, *The Protection of Personal Date in the Fight Against Terrorism: New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon*, 6 Utrecht L. Rev. 62, 85 (2010), *available at* http://www.utrechtlawreview.org/publish/articles/000119/article.pdf ("The changes introduced by the Treaty of Lisbon will have significant effects on EU antiterrorism activities and policies, and, in particular, on PNR Agreements adopted by the European Union, as well as on the proposal for a Council Framework Decision. The recognition of an important value such as the protection of personal data in the EU legal system and the attribution of strong decisional powers to the European Parliament will facilitate significant legal changes to these tools, especially in the light of the fact that the European Parliament has often criticized PNR Agreements as exclusive and important tools in the fight against terrorism. The protection of personal data in the fight against terrorism.").

[111] Renata Goldirova, *EU Calls on US to Respect Bloc's Powers in Travel Security Issues,* EU OBSERVER, Mar. 7, 2008, http://euobserver.com/9/25795.

beneficial. They gained entry to the Visa Waiver Program ("VWP"), something the EU had been unable to successfully negotiate with the US via a joint approach.[112]

The annulment of the PNR agreement led to a practical dilemma for airlines. Without the agreement or any legal basis, transferring PNR data would no longer be in accordance with the EU's *acquis communautaire*.[113] On the other side of the Atlantic, the US threatened to prohibit inbound flights from the EU to land if the airlines would not permit PNR transfer. The US also threatened airlines with a monetary fine for each passenger without a PNR.[114] The EU therefore had little option but to fill this legal vacuum with the new temporary international agreement on PNR with the US on October 19, 2006, which was only valid until July 31st, 2007.[115] The EU then permanently replaced it with a supplemented agreement with the US on the transfer and processing of PNR data ("2007 PNR Agreement").[116] Under the 2007 PNR Agreement airlines must submit PNR data to DHS from air passenger records. This agreement will be valid for a maximum of seven years after signing, and will apply to airlines operating flights "into" and "from" the US.[117] It is not clear whether the agreement also includes airlines operating flights from third countries with transit via the EU, which is a jurisdiction issue. It is also unclear where the data processing will take place, and whether the data controller will have its registered office in the EU or the US.

The agreement includes 'assurances' (the 2004 agreement referred to 'undertakings') that are set out in the "US Letter to the EU," an annex to the 2007 PNR Agreement.[118] In the letter the US unilaterally states that it will

---

[112] The VWP was joined on November 17, 2008 by the Czech Republic, Estonia, Hungary, Latvia, Lithuania and Slovakia.

[113] The entire body of European laws is known as the acquis communautaire.

[114] Renata Goldirova, *Brussels to fight for EU passenger privacy on US flights*, EU OBSERVER, Feb. 1, 2007, http://euobserver.com/9/23394 ("[A]irlines being threatened with fines of $6,000 per passenger or withdrawal of landing rights if they fly to the US without providing required information.").

[115] European Commission, Justice and Home Affairs, http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm (last visited June 1, 2010).

[116] 2007 PNR Agreement, *supra* note 86.

[117] Valentina Pop, *MEPs look to new data protection battle with US*, EU OBSERVER, July 7, 2010, http://euobserver.com/22/30428 ("A new deal was put in place in 2007 for seven years, but after the coming into force of the Lisbon Treaty, the legislature's consent is needed afresh... instead of striking down PNR shortly after the entry into force of Lisbon last December, members of the European Parliament have given the EU commission the chance to first draw up a general mandate on PNR agreements and civil liberties safeguards which cane be used to amend the US pact. The commission proposals are due in autumn.").

[118] 2007 PNR Agreement, *supra* note 86; Letter from Michael Chertoff, U.S. Secretary of Homeland Security, to Luis Armado, President of the Council of the European Union, at II

provide an adequate level of protection for private data in the use of the PNR and will restrict the use of the data by its administration.[119] The US will ensure the protection of the right to privacy in accordance with its own laws (the US Privacy Act is extended administratively to EU citizens),[120] and together with the EU, will review the state of the PNR periodically to determine whether the level of protection is adequate.[121] The contractual parties can annul the agreement in the event of a breach.[122]

Pursuant to agreements with the EU, the US has stated that it will apply a number of special safeguards: the US will only use data to fight terrorism, it will regularly delete such data if it is not relevant to a counter-terrorism investigation, it will store data considered irrelevant up to a permitted maximum of five years, and an appointed officer in Europe will ensure that these commitments are kept.[123] Legally, of course, it is significant that the processing, collection, use, and storage of personal data are not regulated by a bilateral agreement (or on international law), but only on the transient 'assurances' in the US Letter, which may change at any time.

Although the negotiations that led to the definition of the assurances were extensive, the EU did not achieve a clear response from the US on data protection for passengers from the EU. The EU reached an agreement that if PNR data included sensitive information (e.g. personal data on race or ethnic origin, political views, religious or philosophical convictions, trades union membership, and data relating to an individual's health or sex life), DHS would use an automatic system to clean the record and delete data of this kind.[124] However, the deletion of sensitive data only applies in principle,

---

[hereafter U.S. Letter to E.U.] (Sharing of PNR), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf.

[119] U.S. Letter to E.U., *supra* note 118

[120] *Id.* at V. Enforcement; *see also* European Parliament, *Motion to Resolution to wind up the debate on statements by the Commission pursuant to Rule 103(2) of the Rules of Procedure by Sylvia-Yvonne Kaufmann and Giusto Catania on Behalf of the GUE/NGL Group on the PNR agreement with the United*, July 9, 2007, B6-0285/2007.

[121] PRIVACY OFFICE, U.S. U.S. DEPARTMENT OF HOMELAND SECURITY, A REPORT CONCERNING PASSENGER NAME RECORD INFORMATION DERIVED FROM FLIGHTS BETWEEN THE U.S. AND THE EUROPEAN UNION (Dec. 18, 2008) [hereafter DHS PRIVACY OFFICE], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf ("With the 2007 Agreement, the parties agreed to conduct periodic reviews. Compared with the earlier arrangement, this agreement did not specify that any one component of DHS or the European Union was responsible for conducting the review. Instead the agreement deemed the Secretary of Homeland Security and the Commissioner for Justice, Freedom and Security would be responsible for review.").

[122] *Id.*

[123] 2007 PNR Agreement, *supra* note 86.

[124] DHS PRIVACY OFFICE, *supra* note 121, at pt. III.19. ("DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information . . . . DHS promptly deletes the sensitive EU PNR data.").

and in pracice the US itself will decide what constitutes grounds for deletion.[125] US-EU agreements do not require DHS to carry out the filtering if it would threaten US security interests or fall within a number of "exceptional" cases.[126] Additionally, an agreement has been reached with the EU that data relating to an individual open case or investigation could be retained in an active database until the investigation is concluded.[127]

Furthermore, while US authorities have stated that PNR data will be deleted once the fifteen year retention period expires, EU citizens have no assurance that they will actually do this. The US has certainly given itself considerable room to determine its use of the data. The US will study the effect of the retention rules relating to operations and investigations over the coming seven years.[128] The EU only plays the role of observer in this process because the US has only committed itself to notifying the EU of the study results without committing to a formal legal system for deletion and storage in PNR databases.[129]

Despite the 2007 PNR Agreement, a "wave" of separate bilateral agreements between Eastern European EU Member States and the US took place again at the start of 2008.[130] The US found that it could acquire more PNR data from new EU Member States by offering them the same VWP privileges for their citizens (a visa-free tourist entry to the US for up to 90 days) as was previously available to most of the older EU Member States.[131] Some Eastern European states felt that the Commission's negotiations with the US administration were not progressing quickly enough. These new EU Member States had to make their own arrangements with the US because the EU did nothing to ensure quicker access to the VWP system.[132] The

---

[125] Art. 29, Data Protection Working Party, *Opinion 2/2007 on Information to Passengers about the Transfer of PNR Data to US Authorities* (Adopted on Feb. 15, 2007 and revised and updated on June 24, 2008), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp151_en.pdf (". . . such as where the life of an individual could be imperiled or is in serious danger.").

[126] DHS PRIVACY OFFICE, *supra* note 121, at pt. III.19 (". . . where the life of a data subject or of others could be imperilled or seriously impaired . . .").

[127] *Id.* at pt. VII.

[128] U.S. Letter to E.U., *supra* note 118.

[129] *Id.*

[130] *See* U.S. Department of Homeland Security, DHS Signs VISA Waiver Program Agreements with Estonia and Latvia, Mar. 12, 2008, http://www.dhs.gov/xnews/releases/pr_1205358177498.shtm.

[131] Previously all the older EU-15 Member States were on the visa waiver programme except for Greece, and only Slovenia of the newer Member States. The EU objective is to include all its Member States in the visa-waiver programme, but the US is demanding more data on transatlantic air passengers in return.

[132] BBC News, *EU-US Agree on Visa Waiver Talks*, BBC NEWS, Mar. 13, 2008, http://news.bbc.co.uk/2/hi/europe/7294831.stm.

European Commission warned these Member States not to enter such agreements despite the benefits offered by the US.[133] These warnings did not deter the US, which eliminated visas for entry to its territory for states that had reached special separate agreements, known as bilateral memoranda of understanding ("MoU"). The Czech Republic was the first to sign a bilateral agreement, in February 2008, followed by Estonia, Hungary, Latvia, Lithuania, Malta and Slovakia.[134] The security requirements of the MoUs are problematic from the EU's point of view because the exchange of data on air passengers affects areas under the EU's competence.[135] Due to pressure from the MoU signatories, the EU partially conceded and permitted a "twin-track approach" to visa negotiations with the US.[136] This approach allows Member States to negotiate with the US on matters that come under national jurisdiction, while only the European Commission can negotiate on matters within the EU's competence.[137]

The US is well aware that 'fragmenting' the EU and negotiating with Member States directly, rather than the EU as a whole, weakens the EU and Member States' negotiating positions. As a result, it offers each Member State exactly what meets its specific requirements, e.g. entry to the visa-waiver program, in exchange for benefits to itself. For example, by using the MoU as leverage, the US gained permission from the Czech Republic to install radar systems to provide missile protection for Europe,[138] with 10

---

[133] Zoltán Dujisin, *Europe: U.S. Visa Puts Allies at Odds*, IPS News, Sept. 21, 2007, *available at* http://www.ipsnews.net/news.asp?idnews=39347.

[134] DHS signed VWP MOUs with Slovakia, Hungary, Lithuania, Estonia, Latvia, Czech Republic government representatives. These countries were added to the U.S. Visa Waiver Program on November 13, 2008. The program allows their citizens to travel to the United States for stays up to 90 days without first obtaining a visa. But if a national of the mentioned countries does not have an electronic passport with an integrated chip a visa must be requested. *See* U.S. Department of State, Visa Waiver Program (VWP), http://travel.state.gov/visa/temp/without/without_1990.html#countries, for more about the latest developments.

[135] Renata Goldirova, *EU Unity at Stake Over US Visa-Regime Issue, Brussels warns*, EU OBSERVER, Mar. 11, 2008, http://euobserver.com/?aid=25809.

[136] *Id.*

[137] European Parliament Session Document, Motion for a Resolution on the debate of the 23rd of April: "Negotiations between the European Union and the United States with regard to visa exemptions (Visa Waiver)" by Gérard Deprez, RE\722266EN, May 8, 2008, http://www.statewatch.org/news/2008/may/ep-usa-visa-draft-libe-report-may-2008.pdf ("[I]t is clear from the MoUs that some of the new "security enhancements" fall under the Community's competence (such as the one on visa delivery or the European Security Transport Association (ESTA) complementary future obligations), some under the EU's competence (such as on stolen passport, PNR data, or Schengen crime related data), and the remaining reinforcement falls within the exclusive competence of each Member State (such as the ones linked to the criminal records of its own nationals or the ones providing for the presence of air marshals on transatlantic flights).").

[138] Associated Press, *Bush, Czech Prime Minister Close to Reaching Missile Defense Deal*,

interceptor missiles also planned for installation in Poland.[139]

In addition to PNR data, since 2004 the EU has required airlines to send completed Advanced Passenger Information ("APIS")[140] data to the US before take-off.[141] This includes the basic identification information encoded in biometric passports.[142] The US authorities compare passenger information acquired in this manner with other databases containing data on terrorists, potential terrorists, and other people identified as a threat and either sought by the US or considered undesirable.[143] Data from passports and other information including baggage weight, seat number, check-in number at the airport, and address in the US are a supplement to existing data acquired from the PNR and ESTA. Unlike these prior collections, data

---

FOX NEWS, Feb. 27, 2008, http://www.foxnews.com/story/0,2933,333030,00.html (After meeting with President G.W. Bush, the Czech PM Mirek Topolánek told journalists that before the agreement on US radar stations in the Czech Republic was finally signed, there were a few minor details or "*three words*" in the agreement to be clarified relating to environmental protection and respect for Czech environmental standards.) (emphasis added).

139 *Poland wants US security response in missile shield talks*, SPACE WAR, Jan. 17, 2008, http://www.spacewar.com/reports/Poland_wants_US_security_response_in_missile_shield_talks_999.html ("Washington wants to install 10 interceptor missiles in Poland by 2012, as well as associated radar stations in the Czech Republic, to ward off possible missile attacks by so-called rogue states, notably Iran.").

140 APIS means the API system, though both are used [hereafter APIS].

141 APIS Departure Requirements, *Advance Passenger Information System (APIS) Requirements for Non-Immigrant Aliens Departing the U.S. Following Implementation of the Western Hemisphere Travel Initiative (WHTI) for Air Travelers*, CBP.gov, Apr. 16, 2004, http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/apis_departure_req.xm.

142 U.S. DEPQRTMENT OF HOMELAND SECURITY, PRIVATE IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM APIS (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_apisfinalrule.pdf ("The information to be collected from all travelers (passengers and crew members) consists of: complete name, date of birth, gender, country of citizenship, DHS-approved travel document type (e.g., Passport, Merchant Mariner Document, Nexus Air Card, Alien Registration Card, etc.,), travel document number and country of issuance, travel document expiration date, country of residence, status on board the aircraft (whether individual is crew or non-crew), U.S. destination address (except for commercial aviation passengers who are U.S. citizens or lawful permanent residents, commercial aviation crew and persons in transit), place of birth and address of permanent residence (commercial flight crew only), Passenger Name Record (PNR) locator number (commercial passengers and crew only), pilot license/certificate number and country of issuance, (commercial and private flight crew only).").

143 U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS) 6 (2005), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbpapis.pdf [hereafter APIS PRIVACY IMPACT] ("The APIS data is cross- referenced or compared against other law enforcement data maintained in TECS. These cross-references and comparisons occur through IBIS. IBIS resides in TECS and provides access to the National Crime Information Center (NCIC), which allows users to interface with all 50 states via the National Law Enforcement Telecommunications System (NLETS). IBIS also contains the names of individuals on terrorist watch lists.").

from APIS indicates the passenger's 'status' immediately before take-off.[144] The US stores APIS data for only 12 months and then deletes it.[145] The problem with storing APIS data is similar to that with PNR – parties do not collect and use data solely for official state actions. Travel agencies may (according to US rules) retain the information themselves, without any time limit and without the passenger's permission.[146] Agencies may send the data to third parties, and are therefore able to circulate the data among interested users without the passenger's awareness or consent.[147]

B. PNR and Different Approaches to the Protection of Privacy in the US and EU

The problem of ensuring privacy in an era of constantly advancing information technology relates primarily to justified concerns about preserving human dignity, particularly in an alienated, mass society. The sociological and political dimensions of the right to privacy relate to protecting the individual from state intrusion, and from potential abuse of personal data. These are the main concerns of civil society with regard to authorities compiling and using personal data records. Surveillance and sanctions against the individual are part of the nature of authority, so states continually seek new methods of encroaching on an individual's privacy and personal life.

1. Historical Dimensions

European standards on the protection of the right to privacy are significantly different from American standards, as demonstrated by the fact that the creation of the PNR system was met with much greater resistance in the EU than in the US.[148] The difference in protection on the two continents

---

144 APIS Departure Requirements, *supra* note 141.

145 APIS PRIVACY IMPACT, *supra* note 143, at 17.

146 *Id.*

147 *See* Written Testimony of Edward Hasbrouck before the LIBE Committee of the European Parliament and the Article 29 Working Party: Transfers of PNR Data from the EU to the US (2007), *available at* http://hasbrouck.org/IDP/IDP-PNR-26MAR2007.pdf.

148 *Friends of Europe in partnership with EU, Views of Leaders from Europe and the USA on the Future of Transatlantic Security and Various Anti-terrorism Strategies*, GALLUP, http://www.csis.org/media/csis/events/060530_transatlantic_poll.pdf [hereafter *Leaders Poll*] ("Sixty-two percent of the US and European leaders who responded to our survey agree that concerns over the infringement of civil liberties as a result of anti-terrorist measures are greater in European countries than in the United States. However, close to one-third (31%) of the respondents in our survey mostly disagree and another seven percent completely disagree with this statement."). The survey of 116 high-ranking government officials, members of national legislative bodies, heads of major corporations and NGOs was carried out between April 11 and May 15, 2006.

has historical roots.[149] In Europe, during the Second World War, data collections were the subject of mass abuses that reached unimagined dimensions, such as the mass killings committed by Nazis based on records indicating national or ethnic backgrounds (e.g. Jews, Slavs, and Roma) and political affiliation (e.g. socialists and communists).[150] These examples indicate that the collection and storage of records can be very harmful, and despite the "order" that such systems provide, can have horrific consequences.

In addition to the atrocities of the Second World War, Europeans have also faced communist regimes – experienced in Eastern Europe and feared in Western Europe. Data collections again played a major role in the selection of people deemed an obstacle to these regimes. Europeans continue to view mass databases with scepticism and fear the consequences of actions by the authorities.[151] The atrocities that followed the abuse of personal data in Europe, and the fact that the US has not had similar negative experiences with data protection, makes the different conduct and attitude to the collection, storage, and use of PNR understandable.

It is likely that this contributes to the greater satisfaction and lower suspicion of US citizens towards large government personal databases as compared with Europeans.[152] As a result of their heightened scepticism, Europeans adopted the Convention for the Protection of Human Rights and Fundamental Freedoms ("CHR"), Article 8 of which protects the right to privacy.[153] US privacy law emphatically protects freedom, including privacy, or the 'right to be let alone,' while European privacy law focuses on dignity.[154] There are two different cultural values in play here: the freedom of the individual is protected in the US (particularly protection of the right to

---

[149] Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609 (2007).

[150] *Id.* at 56.

[151] *Id.*

[152] *Id.*

[153] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11 with Protocol Nos. 1, 4, 6, 7, 12 and 13*, Nov. 1, 1998, at art. 8, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf [hereafter CHR]. (1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

[154] James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J., 1151-1221 (2004) (describing the difference between the U.S. and European approach to privacy protection).

privacy in the home) against state intrusion, while in Europe regulations primarily protect the individual's reputation against the intrusion of the media and market.[155] The different attitudes towards privacy have been expressed as follows: "Why is it that French people won't talk about their salaries but will take off their bikini tops? . . . Why is it that Americans comply with court discovery orders that open essentially all of their documents for inspection, but refuse to carry national identity cards?"[156] In the context of the collection, storage, and use of personal data for the purpose of preventing terrorism, the European conception of the protection of privacy goes significantly beyond the American conception. Francesca Bignami reinforces this point by noting that an intelligence agency would inform European subjects that it is gathering data on them, analysing it, and sending it to the police for possible future use – far more than one could expect from a similar US agency.[157]

In Bignami's opinion, the collection, storage and use of private data by the US for anti-terrorism purposes would be more effective if it were not spread between various bodies and agencies, such as the Chief Privacy Office in the Department of Homeland Security, the Privacy and Civil Liberties Board in the Executive Office of the President, and the Civil Liberties Protection Officer in the Office of the National Intelligence Director.[158] Given the relative inefficiency of the US system, Bignami contends that a centralised EU system would not only be more effective, but also more acceptable because control of data would be easier and more transparent.[159] This would be a solution at the systematic level. However, the EU is only at the phase of selecting surveillance systems, and the system's application and storage of data are two issues that will require lengthy negotiations. The European Commission, as part of the negotiations, discussed the supervision of passengers' personal data in the form of PNR and ESTA,[160] but to date there has been no detailed agreement

---

155 *Id.* at 1161.

156 *Id.* at 1151-60.

157 Bignami, *supra* note 149.

158 *Id.* at 63.

159 *Id.*

160 For PNR, see Commission of the European Communities, *Commission Staff Working Document Accompanying Document to the Proposal for a Council Framework Decision on the Use of Passenger Name Record (Pnr) for Law Enforcement Purposes (Summary of the Impact Assessment)*, Brussels, SEC(2007) 1422, *avaliable at* http://www.statewatch.org/news/2007/nov/eu-com-pnr-ia-summary-sec-1422.pdf. For ESTA, *see* Press Release, European Union, Vice President Franco Frattini, European Commissioner Responsible for Justice, Freedom and Security, *Providing Europe with the tools to bring its border management into the 21st century (Ministerial Conference on the Challenges of the EU External Border Management)* in Brdo, Slovenia (Mar. 12, 2008), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/142&format=HTML&aged=0&lang

on the measures it submitted for approval to the Council of the EU. A considerable number of proposals were advanced for a potential EU system, from the US PNR system to the Australian ETA[161] (Electronic Travel Authority) system. Given negotiations to date, the most likely agreement will be a solution using both the ESTA and PNR systems.[162] The parties will reach a final agreement on the EU databases only after extended discussions with the US.[163]

2. EU Privacy Requirements

States must justify each restriction placed on the right to privacy and must establish an appropriate balance between protecting public security and safeguarding public and private interests in the individual's right to privacy. Any unjustified or disproportionate control of data records by a non-EU country is incompatible with the right to privacy and the protection of the individual. Data transmitted by the EU to non-EU countries (including the US) must comply with European standards on the protection of privacy. The EU and its Member States must respect the principle of personal data protection as stipulated in the Directive. While Article 26(1)(a) of the Directive only permits the transfer of data with the consent of the individual to whom the data relates, state policies require airlines to transfer PNR even in the absence of passenger consent.[164] Even in the case of informed consent, passengers have no access to their data or knowledge of what will happen to it in the US, in contravention of Articles 10 and 12 of the Directive.[165]

Article 26(1)(d) relates to Article 13(1) of the Directive, which states that exceptions and restrictions on the scope of the rights are permissible "when such a restriction constitutes a necessary measure to safeguard: state security, defence, public security . . . ."[166] These provisions do not form an

---

uage=EN&guiLanguage=en.

[161] The abbreviation "ETA" is used for the Australian Electronic Travel Authority automatic registration system, http://www.eta.immi.gov.au/.

[162] Renata Goldirova, *EU to Launch Travel Security Talks with Washington*, EU OBSERVER, Apr. 21, 2008, http://euobserver.com/22/26014/?print=1.

[163] Patryk Pawlak, *Made in the USA? The Influence of the US on the EU's Data Protection Regime*, *CEPS 'Liberty and Security in Europe'*, CENTER FOR EUROPEAN POLICY STUDIES, Nov. 20, 2009, at 6-8, *available at* http://www.ceps.eu/ceps/download/2680.

[164] European Digital Rights, *USA Gets Direct Access to European Passenger Data,* Feb. 26, 2003, http://www.edri.org/edrigram/number3/pnr.

[165] Edward Hasbrouck, *Can You Really See What Records Are Kept About Your Travel?*, THE PRACTICAL NOMAD, Dec. 30, 2008, http://hasbrouck.org/blog/archives/001595.html.

[166] Council Directive 95/46/EC, *supra* note 100, art. 26(1): (". . . a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that: (a) the data

appropriate legal basis for the transfer of data to a third country. While Article 26(1)(d) makes possible a transfer if necessary or if required by law on the basis of a significant public interest, Article 13(1) states that Member States may adopt regulations to restrict the scope of rights only when necessary to protect the security of the EU and not that of a third country. If the Directive anticipated protection of third countries, such a goal would justify the encroachment on the right of privacy. However, this is currently something the Directive does not permit.[167]

Among possible legal bases, the CHR and the Charter of Fundamental Rights of the European Union ("CFR")[168] provide clearer guidelines for justifying encroachment on personal privacy by the transfer of PNR. Articles 8 of the EHCR[169] and Article 7 of the CFR[170] protect the rights of individuals to have their private life, home, and correspondence respected. Article 8, Section 2 of the CHR defines conditions under which privacy can be restricted. States cumulatively must fulfill the conditions that restrictions be "in accordance with the law" and "necessary in a democratic society."[171] Additionally, restrictions must be: grounded on "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[172] The application of this provision as a legal basis for the transfer of PNR therefore requires legally appropriate legislation at the EU level. Even if one presumes that the principles of *nullum crimen, nulla poena sine lege* ("No crime, no punishment without a previous law")[173], and certainty apply in a democratic society to protect the public interest, states or the EU must prove that it was impossible to protect

---

subject has given his consent unambiguously to the proposed transfer; or . . . (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims . . . .").

[167] *Id.*

[168] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364/1) [hereafter CFR].

[169] CHR, *supra* note 153, art. 8 § 1.

[170] CFR, *supra* note 168, art. 7 ("Everyone has the right to respect for his or her private and family life, home and communications.").

[171] *See* CHR, *supra* note 153, art. 8, § 2.

[172] *Id.*

[173] Case T-99/04, AC-Treuhand AG v Commission of the European Communities, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0099:EN:HTML ("[T]hat principle requires . . . that any Community legislation, in particular where it imposes or permits the imposition of penalties, must be clear and precise so that the persons concerned may know without ambiguity what rights and obligations flow from it and may take steps accordingly. By the same token, that principle must be observed in regard both to provisions of a criminal-law nature and to specific administrative instruments imposing or permitting the imposition of administrative penalties.").

the public interest with measures that would be less invasive of the right to privacy than PNR.[174] The EU and individual Member States have not demonstrated this.

Like Article 7 of the CFR, Article 8[175] of the same document does not provide a legal basis for PNR.[176] In accordance with Article 8, individuals must have the right to access data collected about them and be able to correct inaccurate data – something not possible for data transferred to the US. Article 5 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108"),[177] requires that automatically processed personal data be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."[178] PNR storage in active and dormant databases exceeds all the time limits imposed by Convention No. 108 because states retain such data even after an individual leaves the state.[179] At this point, the "purposes for which [the data was] stored" no longer exists.[180]

The problem posed for EU citizens therefore lies in the lack of protection in the US of their right to personal data protection. The US Privacy Act[181] only protects its own citizens against abuse and the incorrect

---

[174] See Asinari & Poullet, *supra* note 71, at 104–06, for similar positions on the application of CHR Article 8 to the transfer of PNR. *See* Ioannis Ntouvas, *Air Passenger Data Transfer to the USA: The Decision of the ECJ and Latest Developments*, 16 INT'L J.L. & INFO. TECH. 73, 95-96 (2007).

[175] CFR, *supra* note 168, art. 8 ("Protection of personal data:

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

[176] CFR, *supra* note 168, Article 8 refers to Article 286 EC (after adoption of the Lisbon Treaty – Art. 16 of the Treaty on the Functioning of the European Union), which assures every individual of the right to the protection of personal data relating to them.

[177] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm [hereafter Convention 108].

[178] *Id.*

[179] It does not matter if you stay in the country or leave it. The rules about an active and a dormant phase are the same in all cases.

[180] Convention 108, *supra* note 177.

[181] The Privacy Act of 1974, 5 U.S.C. § 552a (1974) (establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal

use of personal data, while EU citizens in the US are left to the arbitrary will of its state authorities.[182] Thus, the protection offered by the existing PNR agreement is unlawful according to EU data-protection standards. From this point of view, the US Government's July 2007 requirement that all negotiation documents relating to the PNR were confidential for at least 10 years from the agreements' entry into force is understandable.[183]

3. Use of PNR Data in the US

The collection, processing, and use of personal data results in the categorisation of passengers in terms of the threat they represent. However, the database (PNR) itself means very little if agencies do not use the data in conjunction with US government databases. Therefore, the PNR is only useful in combination with CAPPS II (the Computer Assisted Passenger Prescreening System II).[184] CAPPS II intended to authenticate the identity of commercial airline passengers by checking each traveler's PNR, including full name, home address, telephone number and date of birth, against governmental databases for security assessment. CAPPS II, would have notified law-enforcement officials whenever the screening process turned up passengers with outstanding warrants against them, even for non-travel-related incidents." As important, it would use commercial databases for counterterrorism purposes.[185] Is this really a search for potential terrorists

agencies."), *available at* http://www.usdoj.gov/opcl/privacyact1974.htm.

[182] Letter from Jacob Kohnstamm, Chairman, Data Protection Working Party, to Juan Fernando López Aguilar, Chairman of the Committee on Civil Liberties, Justice and Home Affairs, European Parliament, in Brussels (Apr. 6, 2010), *available at* http://www.statewatch.org/news/2010/apr/eu-art-29-wp-letter-us-pnr-agreements.pdf ("Although DHS as a matter of policy has voluntarily extended the rights of the Privacy Act to non-US citizens not covered by this legal instrument, it remains to be seen whether the Privacy Act will be applied in cases of violations. To date the Article 29 WP is not aware of any case where violations of US privacy rules have been challenged in US courts. The US has no independent data protection supervisory authority and that the question of judicial redress has repeatedly been addressed by the High Level Contact Group. The question of judicial redress remains an outstanding issue to which a final answer still has to be found. For that reason it continues to be a concern and needs to be tackled in future discussions.").

[183] Anyway, these documents are no secret. Statewatch.org disclosed them on its website. In ten years, as the US proposed, the public's interest for their disclosure would probably be less intense than today. *See US Demands 10-Year Ban on Access to PNR Documents*, STATEWATCH, Sept. 2007, http://www.statewatch.org/news/2007/sep/02eu-usa-pnr-secret.htm.

[184] Timothy M. Ravich, *Is Airline Passenger Profiling Necessary?*, 62 U. MIAMI L. REV. 1, 16 (2007) ("The aim of CAPPS II was to bridge law enforcement and intelligence databases.").

[185] Timothy M. Ravich, *Airline Passenger Profiling Systems After 9/11: Personal Privacy Versus National Security*, Journal of the TRF, Vol. 44, Number 2, Summer 2005, http://www.trforum.org/journal/2005sum/article9.php.

or other organised criminals, or a general search for anyone who has committed a crime? Even the stated purpose of PNR as a tool in the fight against international terrorism[186] and international organised crime covers two different categories that could be seen as distinct. Terrorism stands out as one of the modern world's major threats.[187] Despite this, US and European authorities have added combating "serious" crime to the PNR's role, in addition to the fight against terrorism.[188] This expansion of the remit for personal data collection is impermissible because it allows authorities to use passenger data to prosecute perpetrators of 'minor' commercial theft or similar, relatively unimportant crimes.

Despite lengthy negotiations and various agreements on the transfer of data between the US and Europe, EU citizens are still without adequate protection for their private data in the US. The EU has no control over what happens in the US to the data on its citizens because authorities transfer the data from the PNR and APIS databases when they compare it with data from other databases from various information systems at the federal, state, and local levels.[189] Furthermore, the EU has no assurances that the data will remain fully under federal or state protection. The Delegation of the European Commission to the USA, assisted by Gallup, Friends of Europe, CSIS and the SDA (Security and Defence Agenda), conducted a survey of

---

[186] Edwin Bakker, *Jihadi terrorists in Europe – their characteristics and the circumstances in which they joined the jihad: an exploratory study*, NETH. INST. OF INT'L RELATIONS CLINGENDAEL (2006), at 15-16, *available at* http://www.clingendael.nl/cscp/publications/?id=6480&&type=summary (". . . We speak of a 'terrorist' or 'terrorists' if it relates to intentional acts which were committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation, as formulated by the Council of the EU. Based on the above, jihadi terrorist acts include both violent attacks and activities in support of these acts, such as financing, recruiting, and purchasing arms and explosives.").

[187] ANDREW HEYWOOD, POLITICS 382 (Palgrave Foundation, 2d ed. 2002) ("Terrorism, in its broadest sense, refers to the use of terror for furthering of political ends; it seeks to create a climate of fear, apprehension and uncertainty... as the term is highly pejorative, it tends to be used selectively and often subjectively (one person's "terrorist" is another person's freedom fighter).").

[188] Nino, *supra* note 110, at 72 ("As far as the purposes for processing data are concerned, PNR data could be used by CBP in order to 'prevent and combat: 1. terrorism and related crimes; 2. other serious crimes, including organised crime; 3. and flight from warrants or custody for those crimes'. The wording of category no. 2, which was so vague as to encompass criminal activities not properly related with terrorist acts, allowed data transmission not in compliance with the purpose limitation principle. It is fundamental that the fight against international terrorism be limited and defined, and not so wide as to admit unjustified limitations to the right to privacy and fundamental freedoms not provided for by international and Community law.").

[189] DHS PRIVACY OFFICE, *supra* note 121, at 14.

EU and US leaders on counter-terrorism strategy in the EU and US that reflected the attitudes of these officials to rights violations in these territories.[190] A total of 73% of those surveyed agreed with the statement that US counter-terrorism measures risk infringing civil liberties, while 58% agreed with the statement that EU counter-terrorism measures did not risk infringing civil liberties.[191]

A passenger surveillance system that treats all passengers as possible suspects is questionable in terms of its effectiveness, as well as its acceptability of such an authorized encroachment on individual privacy. US and EU authorities have attempted to assuage doubts about the purpose and effectiveness of PNR by stressing that it is the only possible means of balancing two values – security and privacy.[192] The choice offered to the individual is effectively a 'non-choice' because security is a pre-condition for enjoying all other fundamental rights, including the right to privacy. What are the US and EU actually offering?

The question has become even more relevant since the start of 2008, when the EU decided to introduce a passenger-data collection system similar to the American PNR system.[193] The EU stated that the system was not a response to the United States mandating most (if not all) of the conditions for transferring PNR to the US federal agency in bilateral treaties.[194] These

---

[190] *Leaders Poll*, *supra* note 148.

[191] *Id.*

[192] European Parliament, Press Release, *US Secretary Of Homeland Security Michael Chertoff Debates Data Protection With MEPs Fundamental Rights*, May 14, 2007, http://www.europarl.europa.eu/sides/getDoc.do?language=EN&type=IM-PRESS&reference=20070514IPR06625 ("No-one wishes to forsake civil liberties for security, and both the US and the European states cherish these rights as democratic nations, Michael Cheertoff said. Nevertheless, "life is the liberty on which all others depend" he added, pointing out that PNR have already been used to keep some dangerous individuals out of the US and claiming that eleven of the 19 hijackers of the 9/11 planes could have been identified using similar data, "at minimal cost to civil liberties").

[193] On February 14, 2008, Manfred Weber (CDU), from the EPP parliamentary group in the European Parliament, welcomed a proposal by Franco Frattini relating to the European collection of data, while just two months later in an interview with *Frankfurter Algemaine Zeitung* on April 15, 2008 (after considerable debate in the European Parliament) he significantly distanced himself from the proposal. He questioned whether it offered a 'European solution' or if this form of collection offered real benefits, since sensitive databanks collected and stored nationally by each of the 27 Member States could be subject to abuse. *See EU to tighten border controls, critics fear 'Fortress Europe*, EURACTIV, Feb. 14, 2008, http://www.euractiv.com/en/justice/eu-tighten-border-controls-critics-fear-fortress-europe/article-170292?; *see also* Nikolas Busse, *Widerstand gegen Speicherung von Fluggastdaten*, FAZ.NET, April 15, 2008, http://www.faz.net/s/Rub99C3EECA60D84C08AD6B3E60C4EA807F/Doc~ECD4191F8A6754686BB82474C1744C7D4~ATpl~Ecommon~Scontent.html.

[194] *EU-USA PNR agreement renegotiated to meet US demands*, STATEWATCH, http://www.statewatch.org/news/2006/oct/05eu-us-pnr-oct-06.htm (last visited June 1, 2010).

treaties are in substance unilateral in nature because the authority of the EU had no real influence over them.[195] In effect, these agreements reflected US power and dominance, with the EU well aware that the US was negotiating from a position of strength. The US threatened to blockade US-bound flights from the EU if the EU was not prepared to reach an agreement on transferring PNR.[196] This risk was unthinkable, so the EU agreed to a treaty based on questionable legal premises.[197]

The US always approaches counter-terrorism issues from a position of strength, even when the resolution of issues requires two equal partners. Undoubtedly, this is because that the US has achieved considerable results in this area. However, this is insufficient reason for the EU to continually subordinate itself to the US in the resolution of all the international aspects of such matters. This is the 'posture' the EU has assumed towards the US ever since the 9/11 attacks. Since the first 'bilateral' (in reality unilateral) agreement on PNR, the European Commission has simply continued to follow the US as it has set out its conditions. To date, the EU has rather stoically accepted US demands to tighten security and introduce new counter-terrorism measures on transatlantic flights. However, the EU's patience with the US finally wore out when the US sent new demands, more of a 'wish list' in effect, to the European Commission in early 2008.[198] The new demands included the placement of US security agents on transatlantic flights by US carriers, the introduction of the ESTA, the obligation to report lost or stolen passports, and demands for transfer of data on air passengers only flying over US territory but not landing.[199] This led the EU to issue a clear response that it did not support the demands.[200] The EU also expressed dissatisfaction with US bilateral agreements with its eastern European Member States.[201] Jonathan Faull, Director General of Justice, Freedom and Security at the Commission, justified this response by noting that the EU does not "negotiate matters which are dealt with in Washington with the

---

[195] *EU/US security "channel"- a one-way street?*, STATEWATCH, http://www.statewatch.org/news/2008/aug/03eu-usa-sw-art.htm (last visited June 1, 2010) ("It has been apparent for years to observers able to get access to unreleased EU documents that EU-US meetings are one-sided affairs with the US side making all the running.").

[196] Goldirova, *supra* note 114.

[197] The problems are posed in relation to the right to privacy and protection of (the transfer of) personal data. *See* Council Directive 95/46/EC, *supra* note 100, arts. 26(1), 26(2) & 4(1)(c).

[198] Renata Goldirova, *Brussels Attacks New US Security Demands*, EU OBSERVER, Feb. 14, 2008, http://euobserver.com/9/25657?print=1.

[199] *Id.*

[200] *Id.*

[201] European Parliament Resolution of 12 July 2007 on the PNR Agreement with the United States of America, P6_TA-PROV(2007)0347, http://www.statewatch.org/news/2007/jul/ep-pnr-resolution-jul-07.pdf.

state of California or other federal states".[202] However, EU objections will again fall on deaf ears because the US has already emphasised that the future of the VWP depends on Europe accepting its demands.[203] Among its reasons for the escalation of security measures, the Bush administration raised the hypothetical danger of a terrorist on a flight not due to land in US territory (e.g. heading to a Mexican destination) exploding that aircraft during a flight over US territory.[204] In its potential terrorist scenarios, the US also posited the danger posed by people accompanying certain air passengers (e.g. wheelchair users) via security controls until their embarkation, but not actually embarking themselves.[205] The US already requires PNR data for such people.[206]

In its November 20th, 2008, resolution on the Commission proposal on the use of PNR, the European Parliament noted that the Commission's statement that *"the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes*" was disputable because no evidence had yet been provided to substantiate the claim.[207] There had been just one joint review of the 2007 PNR Agreement,[208] which only assessed implementation and not results. Furthermore, the US has not proven that regular, large-scale use of data from PNR records is essential to the fight against terrorism and organised crime.[209] The European Commission and Parliament have opposing positions on the creation and implementation of the legally questionable counter-terrorism border measures. An important future development will be whether the Lisbon Treaty eventually enters into force. It would give the Parliament greater powers, making it equal to the Council of the EU in legislative decision-

---

[202] *Id.*

[203] Ian Traynor, Bush *Orders Clampdown on Flights to US*, GUARDIAN (London), Feb. 11, 2008, *available at* http://www.guardian.co.uk/world/2008/feb/11/usa.theairlineindustry/print.

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *Council Framework on PNR, supra* note 37, at 2.

[208] EUROPEAN COMMISSION, REPORT ON THE JOINT REVIEW OF THE IMPLEMENTATION OF THE AGREEMENT BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF PASSENGER NAME RECORD (PNR) DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS), Feb. 8-9, 2010,
http://ec.europa.eu/justice_home/news/intro/doc/100406_pnr_report_joint_review_implementation_agreement_eu_us.pdf.

[209] European Parliament Resolution of 20 November 2008 On The Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, (2010/C 16 E/08), O.J. C /16 E/44, Jan.22, 2010, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:016E:0044:0049:EN:PDF .

making.[210] The strengthening of its legislative function would make the Parliament's positions, when combined with the Council of the EU in the Lisbon Treaty system, more important and give it greater weight when opposing other institutions, particularly the Commission. In this regard, it is important to note that in the second half of 2008 the EU seemed to finally 'awake from its slumber.' In a December 2008 document (EU doc no: 17136/08), the Council Working Party, JHA-RELEX Ad Hoc Support Group (JAIEX), pointed out the long-term inequality in the EU's negotiating position with the US.[211]

Calls for a change in the US negotiating approach to the EU may finally find more fruitful ground with the election of the new US President, Barack Obama. That is the expectation of some of the EU's highest officials, including Ignasi Guardans, a member of the European Parliament and substitute member of the Committee on Civil Liberties, Justice, and Home Affairs.[212] This expectation is partially grounded in a claim that changes will first come from developments within the US because the growing demands of the fight against terrorism will require regulation on the protection of personal data. Changes in the protection of personal data and the right to privacy in the US could lead to a reduction in the gap between EU and US legal and political positions.

It is not only the EU institutions, but also the Member States themselves, that are broadly dissatisfied with the PNR agreements. Only three countries – Denmark, France, and the UK – have passed legal acts permitting the application of PNR at the national level.[213] The European Commission supports the coordinated application of PNR because an alternative scenario in which Member States reach independent decisions on the matter could lead to irreconcilable differences.[214] Despite this, the UK's position is that its decision on the national application of PNR is lawful because it is in line with EU data-protection legislation.[215] It expresses no

---

[210] Nino, *supra* note 110.

[211] Tony Bunyan, *Statewatch Analysis: EU Agrees US Demands to Re-write Data Protection Agreement*, STATEWATCH, http://www.statewatch.org/analyses/no-78-eu-us-dp.pdf ("[the] broad feeling among many in the past years that it was essentially left to the United States to determine what was on the agenda of EU-US relations and that the EU has been insufficiently strong to set its own objectives, its own requests and where appropriate, also its own 'red lines'.").

[212] Winter Casey, *Parliamentarian Provides Privacy Update*, TECH DAILY DOSE (CONGRESS DAILY – NATIONAL JOURNAL ONLINE), Mar. 3, 2009, http://techdailydose.nationaljournal.com/2009/03/parliament-member-offers-priva.php?print=true.

[213] *Id.*

[214] Nino, *supra* note 110.

[215] Casey, *supra* note 212.

interest in the related issues of intra-EU consistency.[216] Who will dare to criticise the US if the EU Member States are themselves prone to attitudes of superiority and arrogance?

C. The VWP (Visa Waiver Program) and ESTA (Electronic System of Travel Authorisation)

Despite the reservations of the European Parliament, the Council of the EU, and some independent civil liberties groups regarding the protection of personal data within the US PNR system, by 2010 the EU plans to establish a data collection system for non-EU passengers on flights to and from the EU.[217] The Council of the EU has already lent its support to a project to introduce an Electronic System of Travel Authorisation (ESTA), which is apparently based on the Australian Electronic Travel Authority system ("Australian ETA").[218] The amount of data involved[219] is said to be less than the amount currently transferred to US authorities under the PNR system regarding European passengers, but the EU has yet to reach final agreement on that.

In 2007, the European Commission, a year before the ESTA proposal, proposed the use of PNR data for air passengers entering EU territory.[220] This data would be similar to the information stored when a flight reservation is made. All Member States would use the PNR system, but it would not be connected to the Schengen cooperation,[221] which fascilitates

---

[216] *Id.*

[217] Nino, *supra* note 110.

[218] The EU reached an agreement with Australia – after introducing a system based on its traveller information system – on air passenger records that allow both parties to exchange data on air passengers. EU reached consensus on the agreement on 5 June 2008, which is its third intercontinental PNR agreement (following those with the US and with Canada). See Council Of the European Union, Agreement Between the European Union and Australia on the Processing and Transfer of European Union-sourced Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs Service, Brussels, No. 9946/08, June 10, 2008, *available at* http://www.statewatch.org/news/2008/jun/eu-australia-pnr-agreement-2008.pdf.

[219] The Australian ETA requires non-Australian citizens to provide data on credit cards, passport, citizenship, date and place of birth, sex, and passenger name.

[220] Press Release Concerning the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes, MEMO/07/449, Nov. 6, 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en.

[221] Council Decision 1999/435/EC, Council Decision of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis [The Schengen Acquis], 1999 O.J. (L 176) (referencing the provisions from "Free movement of persons, asylum, and immigration", *available at* http://europa.eu/legislation_

the customs clearance of goods.[222] The European Commission intended the system to prevent terrorism and organized crime rather than assist with border control.[223] In March 2009, Privacy International described EU deliberations on ESTA as purely hypothetical, characterizing it as *"merely kite-flying at the moment, as Europeans have no idea how to implement it."*[224]

On August 1st, 2008, the US introduced a system for passengers permitted to travel without a visa (via VWP), which the EU is still debating.[225] Before travelling to the US (or even on transit through the US) the applicant must complete an electronic form for ESTA travel approval, which is valid for two years (if approved) and for an unlimited number of journeys.[226] The retention time limit for this data is seventy-five years, the same as the I-94W form that ESTA replaces.[227] In doing so, the US outflanked the EU again, now demanding not only PNR data from Europeans but also ESTA registration. The US denies that the US ESTA is a form of visa.[228] The US ESTA is identical to the Australian ETA system that the Australian government recognises on its website as equivalent to a visa.[229] This is the case even though the Australian ETA involves no stamps or other marks in passports and no need to visit an Australian diplomatic office to submit an application, as it can be completed via travel agents, airlines, or online.[230] It is arguable that, despite its denials, the US has informally and without any announcement cancelled the benefit of visa-free

---

summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/index_en.htm).

[222] *Id.* art 25 ("The Parties shall develop their cooperation with a view to facilitating customs clearance of goods crossing a common border, through a systematic, automatic exchange of the necessary data collected by means of the single document.").

[223] *See Council Framework on PNR*, *supra* note 37.

[224] *EU to Announce Fingerprinting for All Visitors*, PRIVACY INT'l (Mar. 17, 2009), *available at*
http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-560378&als[theme.

[225] Civil Liberties, Justice, and Home Affairs, Directorate General Internal Policies of the Union, *The Tools Called to Support the 'Delivery' of Freedom, Security and Justice: A Comparison of Border Security Systems in the EU and in the US* 23 (Briefing Paper) (Feb. 2009) (". . . the US Visa Waiver Program (VWP) began as a pilot program with the UK and Japan in 1988 (and became permanent in 2000)").

[226] U.S. Department of Homeland Security, Frequently Asked Questions: Electronic System for Travel Authorization (ESTA), June 3, 2008, http://www.dhs.gov/xnews/releases/pr_1212501117599.shtm [hereafter ESTA Frequently Asked Questions].

[227] *Id.*

[228] *Id.*

[229] Australian Electronic Travel Authority, What is an ETA?, http://www.eta.immi.gov.au/ETAAus2En.html (last visited June 1, 2010).

[230] *Id.*

(VWP) entry to its territory.[231]

Even when responding to the potential introduction of a European ESTA system, the US proceeded with its own ideas. By contrast, when developing the European ESTA system, European leaders have again followed the US's lead.[232] The EU system, like the US system, will mirror the Australian ETA model. The difference between the US PNR and ESTA systems lies in the fact that in PNR the US checks passenger data before and during the flight, whereas authorities use ESTA to check passengers before travel and permit or refuse entry to the US on that basis.[233] Border-protection services retain discretionary powers to decide, on the basis of additional APIS data (acquired just before take-off from an EU airport) and assessments during the border-control process (including biometrics and psychometrics), whether to permit passengers to enter the US.[234] If rejected, authorities return passengers to the EU, or even arrest and detain them if information links them to terrorist or criminal activities.[235]

The Australian ETA is more transparent than the US ESTA because passengers must submit personal data to the Australian authorities at least two weeks before their proposed date of travel.[236] Despite the discretionary powers retained by Australian border-control personnel, the acquisition of an ETA is a greater guarantee that the passenger will gain entry to the intended destination country.

The problem with the application of the US ESTA system is that, together with the PNR, it provides a dual passenger control system – before and during the flight. The US emphasizes that the ESTA is only a

---

[231] Travellers not eligible for ESTA registration (even in VWP member states) are: people who have been arrested; those with criminal records; those with certain serious communicable illnesses; those who have been refused admission into, or have been deported from, the United States; and those who have previously overstayed on the VWP (even by only one day). Such travelers must apply for special restricted visas. If they attempt to travel without a visa, then they may be refused entry into the United States. U.S. Embassy Ljubljana, Slovenia, Visa Waiver Program, http://slovenia.usembassy.gov/visa_waiver_program.html (last visited June 1, 2010).

[232] Madhu Unnikrishnan, *EU to Consider Electronic Travel Authorization,* AVIATION DAILY, Aug. 9, 2007, http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aviationdaily&id=news/ETA08097.xml.

[233] U.S. Depqrtment of Homeland Security, Electronic System for Travel Authorization (ESTA), http://www.dhs.gov/files/programs/gc_1217365595781.shtm.

[234] U.S. Department of Homeland Security, Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Records, DHS-2007-0041, http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_cbp_apis_final_rule.pdf.

[235] *See, e.g.*, Associated Press, *U.S. Officials Detain Venezuelan Foreign Minister at New York Airport*, Sept. 24, 2006, FOXNEWS.COM, http://www.foxnews.com/story/0,2933,215373,00.html.

[236] Australian Government, Department of Immigration and Visas; Visas, Immigration and Refugees, http://www.immi.gov.au/visitors/tourist/976/how-to-apply.htm

replacement for the previous I-94W form that passengers had to complete onboard their flight and hand over to the authorities upon landing.[237] The US implemented ESTA to give itself more time to review and compare data from its own databases than was previously provided using I-94W forms that could only be checked from a completed form on the border-crossing point.[238] The US explains this as a 'courtesy' to innocent travellers, who will pass the border security check more quickly thanks to the ESTA.[239]

In the ESTA electronic application form, passengers must give their passport details and personal data (which duplicates the PNR data). In addition, they must respond to 'security' questions, such as queries about links to the Nazi regime in Germany between 1933 and 1945, and questions about health status, including HIV infection or AIDS.[240] Jacques Barrot, the current European Commissioner for Justice, Freedom, and Security, warned that placing HIV and AIDS status on the form was incompatible with EU standards, particularly the right to privacy provided for by Article 8 of the CHR.[241] Despite this warning and an assurance from the US Secretary of Home Security, Michael Chertoff,[242] that this section of the form would be withdrawn, it was still included.[243] These questions encroach on the right to privacy, yet passengers must answer them if they are to register using ESTA. The passenger information section of the official DHS website regarding ESTA registration requirements makes no mention of questions on health or connections to Nazism.[244] These questions only appear after a potential passenger using the system has submitted personal data and passport details. It is not clear what data the system retains when a passenger starts the registration process and then abandons it upon encountering questions that unduly impinge on his or her privacy.[245]

---

[237] USAGreenCardCenter.com, US Shifts Visa Waiver Program Authorization to Internet, Jan. 2009, http://www.usagreencardcenter.com/esta.htm.

[238] *Id.*

[239] *Id*.

[240] U.S. Embassy Tallin, *supra* note 70 (". . . the traveler will also be required to answer VWP eligibility questions regarding communicable diseases, arrests, and convictions for certain crimes, and past history of visa revocation or deportation, among others... communicable diseases: chancroid, gonorrhea, granuloma inguinale, HIV, leprosy (infectious), lymphogranuloma venereum, syphilis (infectious stage), tuberculosis (active) . . . .").

[241] *Americans Interested in Aids* (Američane zanima tudi aids), 24UR.COM (Brussels), Jan. 13, 2009, http://24ur.com/novice/svet/americane-zanima-tudi-aids.html; ESTA Frequently Asked Questions, *supra* note 226 ("The traveler will also be required to answer VWP eligibility questions regarding communicable diseases, arrests and convictions for certain crimes, and past history of visa revocation or deportation, among others.").

[242] *Americans Interested in Aids*, *supra* note 241.

[243] *Id.*

[244] *See* ESTA Frequently Asked Questions, *supra* note 226.

[245] U.S. Department of Homeland Security, Customs and Border Protection, Electronic

As with the PNR, the US has not committed itself to using ESTA data solely for investigating and detecting terrorism. Information acquired via ESTA is accessible to federal, state, local, and foreign government agencies, and multinational government organizations. DHS allows these entities to use the data in civil and criminal cases.[246] Civil cases, and to a lesser degree 'ordinary' criminal cases, are far removed from the original ESTA objective: the fight against terrorism. The US justifies the ESTA by calling it a passenger-friendly "partial assurance" that they will be able to enter the United States.[247]

In the near future, the Council of the EU intends to adopt a Framework Decision on the protection of data exchanged between Member States in the fight against terrorism and organized crime.[248] As a Slovenian minister, representing the EU presidency, stated in the first half of 2008, this should "create the possibility of the safe exchange of such data between states."[249] The EU continually emphasizes the need to provide a high level of protection of personal data and references the Directive.[250] At the same time, its decisions to install a European ESTA will encroach on the privacy of passengers from outside countries who travel to or from the EU. On this point, some EU institutions – Council and Parliament, though not the Commission – have severely criticized the US's highly similar version of the system.[251] Authorities state that they will only permit access to the collected

---

System for Travel Authorization – Modernizing the Visa Waiver Program, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/fact_sheets/fact_sheet_esta.ctt/fact_sheet_esta.pdf ("Q: What information does a traveler need in order to complete the travel authorization form? A: The traveler must provide biographical data including name, birth date, and passport information, *as well as answers to questions regarding eligibility to travel under the VWP*.") (emphasis added).

[246] U.S. Embassy Tallin, *supra* note 70 (". . . investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or licence, or where DHS believes information would assist enforcement of civil or criminal laws").

[247] *Electronic System of Travel Authorization (ESTA)*, LEADERSHIP JOURNAL, Jan. 9, 2009, *available at* http://www.dhs.gov/journal/leadership/2009/01/electronic-system-of-travel.html (". . . it *saves* travelers the time, expense, and hassle of flying to the United States only to find out that they are inadmissible under the Visa Waiver Program.") (emphasis added).

[248] Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, O.J. L 350, 30/12/2008, p. 0060 – 0071.

[249] Slovenia held the EU Presidency during the first half of 2008, which means it led all meetings of heads of state and government and the Council of the EU. In accordance with the division of duties between the cabinet of the presiding EU Member State, the prime minister chairs meetings of the Council of the EU, while the relevant ministers chair the Council of Ministers meetings within their brief.

[250] Council Directive 95/46, O.J.1995 (L 281) 31-50.

[251] European Parliament, Draft Motion for a Resolution, further to the Commission statement pursuant to Rule 37(2) of the Rules of Procedure by Johanna L.A. Boogerd-Quaak

data for checks on a suspect's point of origin for travel into the EU. The Council of Ministers stated that this data could make a significant contribution to solving crimes, which means that anti-terrorism measures are now being extended or are no longer distinguished from the field of criminal prosecution of 'traditional' crime.[252] The EU's rationale for collecting personal data is therefore the same as that of the US: fighting not only terrorism, but also crime generally. Franco Frattini[253] has also cited the fight against undesired immigration as another goal, which Italy – together with other European states – has clearly added to counter-terrorism projects.[254] The expansion of the anti-terrorism rationale to include the prevention of crime and illegal immigration is expanding the security cordon and creating a 'Fortress Europe'.

In addition to the concerns set out above, viewing the ESTA and PNR systems separately is inappropriate because they are pursuing the same objective – collecting, storing and using the maximum amount of personal data. The US combination of PNR, ESTA and APIS is even more comprehensive, and, given the length of data retention (seventy-five years for ESTA, fifteen total years for PNR), is extremely questionable in terms of personal data protection.[255] It must also be emphasized that the European

---

on behalf of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA, Sept. 24, 2003, http://www.poptel.org.uk/statewatch/news/2003/sep/eppnr.pdf.

[252] Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes - State of Play, 2007/0237 (CNS), May 23, 2008, p.3, http://www.statewatch.org/news/2008/may/eu-pnr-9514-08.pdf.

[253] Franco Frattini is an Italian politician, currently serving as Italy's Foreign Minister in the new Berlusconi cabinet. Before May 8, 2008, he served as European Commissioner for Justice, Freedom and Security and one of five vice-presidents of the 27-member Barroso Commission (as of May 8, 2008). For more on F. Frattini, see his profile (European Comm'n, Franco Frattini, http://ec.europa.eu/commission_barroso/frattini/welcome/default_en.htm)(last visited June 1, 2010).

[254] The discriminatory gathering of fingerprints from members of the Roma community (including children) – a kind of "ethnic cataloguing" speaks eloquently of the Italian government's positions on the protection of human rights. *See* Renata Goldirova, *Italian Plans to Fingerprint Roma Criticised as 'Ethnic Cataloguing',* EU OBSERVER, Apr. 27, 2008, http://euobserver.com/9/26408. Italy has joined the Europol "Special Task Force", in the "Police Wo rking Group on Terrorism" project to exchange information and counter-terrorism preventive measures, and actively co-operates with Interpol and the Eurojust group (information exchange and co-operation between justice systems to prevent terrorism). For more on Italy's inclusion in the international fight against terrorism, see DEPAUL UNIVERSITY COLLEGE OF LAW, INTERNATIONAL HUMAN RIGHTS INSTITUTE, ITALY, http://www.law.depaul.edu/centers_institutes/ihrli/downloads/publications/Italy.pdf (last visited June 1, 2010).

[255] ESTA Frequently Asked Questions, *supra* note 226 ("The ESTA application data will over time replace the paper I-94W form. In those instances where an ESTA is then used in lieu of a paper I-94W, the ESTA will be maintained in accordance with the retention schedule for

ESTA will apply to Americans, as well as Australians, Africans, Asians, and anyone travelling into the EU from "outside." Separate negotiations with Washington alone are therefore irrational and unjustifiable. But what gives greatest cause for concern is that the measures being taken by the EU are not subject to sufficient reflection and consideration by society at large, which appears to unquestioningly accept the policies as essential to security and the fight against terrorism.

D. Biometrics and Border Controls (VIS and US-VISIT)

One of the EU counter-terrorist measures involving personal data collection used in border control – a measure very similar to those used in the US – is the European Visa Information System (VIS). As an instrument of visa policy, the European VIS is similar in content to the US-VISIT system, which is specifically aimed at the 'fight against terrorism.'[256] According to Americans for Better Immigration, the US-VISIT system is based on the principle of "keeping out those who should not be let in."[257] US authorities use the system to check all foreigners (except Canadian and Mexican citizens crossing their respective land borders) entering the US.[258] The border-security program uses technology to verify biometrics alongside lists of undesirable persons.[259] The efficacy of the system is based on the effectiveness of three processes: 1) verifying the identity of people presenting passports for identification at the border to prevent document or identity theft; 2) checking visitors against lists of persons recorded for security purposes (terrorists, criminals, and illegal immigrants); and 3) verifying that people who enter US territory depart on time (expired visas or VWP status).[260]

Biometric testing is intended to verify passengers' identity against their passport. The system involves biometric checking – currently the digital capture of fingerprints and photography.[261] Authorities crosscheck the

---

I-94W, which is 75 years.").

[256] *See* Peter Hobbing, *A Comparison of the Now Agreed VIS Package and the US-VISIT System*, EUR. PARL., DIRECTORATE GENERAL INTERNAL POLICIES (2007), http://www.europarl.europa.eu/activities/committees/studies/download.do?file=17239.

[257] *Full Implementation of US-VISIT*, AMERICANS FOR BETTER IMMIGRATION, http://www.betterimmigration.com/candidates/2006/entryexit.html [hereafter BETTER IMMIGRATION] (last visited June 1, 2010).

[258] Jessica M. Vaughan, *Modernizing America's Welcome Mat, The Implementation of US-VISIT*, CENTER FOR IMMIGRATION STUDIES, Aug. 2005, http://www.cis.org/articles/2005/back905.pdf.

[259] *Id.*

[260] BETTER IMMIGRATION, *supra* note 257.

[261] Elitsa Vucheva, *EU to Launch Biometric Passports by Summer*, EU OBSERVER, Jan. 14, 2009, http://euobserver.com/9/27407.

information gathered with data obtained at the time of US visa acquisition.[262] The differences between visa and non-visa passengers is that visa passengers must undergo biometric checks twice, while visa-free passengers only undergo this process with immigration officials upon arrival in the US.[263] Under the VWP, the 'other' check was effectively carried out as part of the acquisition of the biometric passport where relevant.[264] Therefore, in yet another context, one could assert that there are no longer essential differences between visa and visa-free passengers.

In addition to the data transfer via APIS, PNR and ESTA, EU citizens are also checked at the first airport of entry to the US from the EU.[265] The only consolation for Europeans is that the system only subjects them to biometric testing once. The US only permits this system because countries covered by the scheme before the introduction of the VWP required the introduction of biometric passports.[266] As with PNR or ESTA, authorities store the data acquired from biometrics in databases and as Hasbrouck says "these lifetime travel dossiers make no sense as a security system, but a lot of sense as a surveillance system".[267]

A serious problem with US-VISIT is that the system does not function as intended. Sec. 110 of the Illegal Immigration Reform and Immigrant Responsibility Act[268] states that authorities must collect entry and exit data (arrival and departure from the US) for each foreigner.[269] Despite this provision, the system currently only includes data on approximately 22% of foreign visitors.[270] Travelers from Mexico and Canada are exempt, and they

---

[262] Homeland Security Europe, *Biometric Passports*, http://homelandsecurityeu.com/ currentissue/ article.asp?art=271261&issue=219.

[263] U.S. Department of State, Visa Waiver Program (VWP), Entering the United States under the Visa Waiver Program (VWP) – What happens at the port of entry?, http://travel.state.gov/visa/temp/without/without_1990.html#vwpport.

[264] Homeland Security Europe, *supra* note 262.

[265] Even if a passenger's final destination is elsewhere, the border control must be carried out at the first airport at which a flight from the EU lands. Subsequent flights are deemed as internal flights.

[266] U.S. Deptartment of State, Biometric and MRP Requirements for VWP Travelers, http://travel.state.gov/visa/laws/telegrams/telegrams_1393.html.

[267] STATEWATCH NEWS ONLINE, *Commission did agree that PNR data can be used for CAPPS II testing, but the question is why?*, http://www.statewatch.org/news/2004/jan/09eu-usa-pnr-databases.htm.

[268] *See* Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110, 110 Stat. 3009 (1996) (describing the Automated Entry-Exit Control System).

[269] *Id*. at § 110. AUTOMATED ENTRY-EXIT CONTROL SYSTEM. (a) SYSTEM.-Not later than 2 years after the date of the enactment of this Act, the Attorney General shall develop an automated entry and exit control system that will- 1) collect a record of departure for every alien departing the United States and match the records of departure with the record of the alien's arrival in the United States.

[270] Hobbing, *supra* note 256.

represent the vast majority (about 70%) of unrecorded foreigners,[271] despite the fact that in terms of illegal immigration, Mexicans rank first and Canadians fourth.[272] The concerns of the Government Accountability Office regarding the logic of introducing and maintaining a system of this kind are more than justified in terms of both the effectiveness in reducing illegal immigration and in terms of pursuing terrorists.[273] In 2007, the United States welcomed nearly 56 million foreign visitors.[274] Given such numbers and the deficiencies of the US-VISIT system, it is impossible for DHS to monitor whether every foreigner – including illegal immigrants, terrorists and other criminals – departs 'on time'.[275]

Biometrics include the most noticeable and measureable physical characteristics such as fingerprints, retina patterns, face shape, and some externally discernable mental and physical conditions (e.g. sweating, rapid heart rate, and increasing breathing). This data is supplemented through the use of psychometrics and sociometrics. Psychometrics include externally discernable signs of human perception, emotion, motivation, and behavioural tendencies, including style of talking and walking. Sociometrics involve anticipating behaviour in interpersonal relations – within groups, between organisations, etc. – and how individuals react in such circumstances, whether biologically, psychologically and socially.[276] Among these approaches, only biometrics involve physical measurements, and thus requires a legal basis to justify it. A legal basis is not required for psychometrics and sociometrics because individuals are unaware they are even subject to such examination. As individuals cross a border,

---

[271] *See* Jessica M. Vaughan, *Modernizing the Welcome Mat – A Look at the Goals and Challenges of the US-VISIT Program*, SMART BORDERS CONFERENCE: CENTER FOR IMMIGRATION STUDIES (2004) *avaliable at* http://www.cis.org/articles/2004/usvisittranscript.html.

[272] Mark Krikorian, *The Link: Legal and Illegal Immigration*, NEW YORK POST, Feb. 16, 1997, *available at* http://www.cis.org/articles/1997/msk2-16-97.html ("[I]llegal immigrants . . . more than one-third of all people in the U.S. born in Mexico, almost half of Salvadorans and Guatemalans, nearly a third of Haitians, 15 percent of Canadians, and 8 percent of Filipinos.").

[273] *See* U.S. GAO, INFORMATION SECURITY, HOMELAND SECURITY NEEDS TO IMMEDIATELY ADDRESS SIGNIFICANT WEAKNESSES IN SYSTEMS SUPPORTING THE US-VISIT PROGRAM 10 (2007), http://www.gao.gov/new.items/d07870.pdf.

[274] Victoria Colette Reynolds, *Record Number of Overseas Visitors Coming to United States*, AMERICA.GOV, July 25, 2008, http://www.america.gov/st/econ-english/2008/July/20080725142833berehellek0.5649835.html.

[275] BETTER IMMIGRATION, *supra* note 257 ("DHS estimates that at least 40% of the illegal aliens in the United States are overstayers. Consequently, US-VISIT would be a vital tool in 'interior enforcement' [i.e. detecting, detaining and deporting illegal aliens from communities in all regions, not just along the borders].").

[276] *Biometric, Psychometric, and Sociometric Profiling*, INT'L BULLETIN OF POL. PSYCH, Oct. 24, 2003, *available at* http://security.pr.erau.edu (select "Archives", then scroll to "Article 41").

immigration officials are attentive to these related factors, on the basis of which they can refuse an individual entry or detain them in some manner.

The development of ID-security technology has led to new techniques such as scanning brainwaves, heartbeat and gait.[277] A group of scientists developed these techniques in a three-year project called Humabio which the European Commission partially financed.[278] The brain scanning produces models of individuals' brains that are unique and authorities can therefore use for identification purposes. Combining this with information on heartbeat and individual gait and posture means that scientists can produce an extremely successful identification model. Switzerland is currently testing this system for the transfer of pilots and flight attendants from the airport to aircraft.[279] Some scientists have welcomed this system enthusiastically, while there has been far less enthusiasm among people aware of the violations of human rights that this surveillance model could lead to.[280] The European Union is committed to convincing its citizens that it will respect the right to privacy, yet its involvement in projects such as Humabio is nothing other than a new form of surveillance on the individual.[281]

The EU has followed the US in making biometric passports obligatory in order to enhance surveillance and prevent the growing phenomenon of identity theft.[282] The European Parliament passed a legislation with a large majority that required all EU Member States to prepare second-generation biometric passports that will include fingerprints.[283] States will store EU

---

[277] *See* A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, G. Ruffini, *Unobtrusive Biometric System Based on Electroencephalogram Analysis*, EURASIP JOURNAL ON ADVANCES IN SIGNAL PROCESSING (2008), http://www.hindawi.com/journals/asp/2008/143728.abs.html *and* A. Riera, A. Soria-Frisch, M. Caparrini, I. Cester, G. Ruffini, *Multimodal Physiological Biometrics Authentication*, http://www.humabio-eu.org/docs/papers/riera_multimodal_physiological_biometrics.pdf.

[278] Humabio, Organization Definition, http://www.humabio-eu.org/ ("HUMABIO is a EC co-funded "Specific Targeted Research Project" (STREP) where new types of biometrics are combined with state of the art sensorial technologies in order to enhance security in a wide spectrum of applications like transportation safety and continuous authentication in safety critical environments like laboratories, airports or other buildings.").

[279] Humabio, Pilot tests, http://www.humabio-eu.org/pilot_tests.html.

[280] *Brain Waves Reveal Your ID*, BBC FOCUS - SCIENCE, TECHNOLOGY, FUTURE, Apr. 2009, at 16.

[281] Owen Bowcott, *Brain Scanning May be Used in Security Checks*, THE GUARDIAN, May 10, 2009, http://www.guardian.co.uk/technology/2009/may/10/biometric-scanning-brain-security-checks/print.

[282] Jim Brunsden , *Biometric Passports to Become Mandatory*, EUROPEAN VOICE, Jan. 15, 2009, http://www.europeanvoice.com/article/2009/01/biometric-passports-to-become-mandatory/63653.aspx.

[283] Council Regulation (EC) NO 2252/2004 OF 13 December 2004 on Standards For Security Features and Biometrics in Passports and Travel Documents Issued by Member

citizens' fingerprints in Radio Frequency Identification chips (RF-Chip) that enable rapid, contact-free identification.[284] The EU has not followed the US regarding the issuance of passports to its citizens, but has adopted measures relating to all third country nationals who need a visa for entry and will require biometric passports.[285] Given the slow rate at which the EU has been putting these measures into practice, it is realistic to assume that the system will not be ready by the planned start date of 2015.[286]

CONCLUSION

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." - Benjamin Franklin, 1759[287]

In the aftermath of 9/11 and other terrorist attacks at the start of the 21st century, democratic 'western' society has had to decide where it should set boundaries on government encroachment on human rights and fundamental freedoms. Advances in Internet technologies increasingly impact air passenger transportation and are vital to countries' efforts to bolster their security. They also enable states to intrude into the most private areas of an individual's life and identity. Identification technologies and processes often do not allow the individual any opportunity to avoid such encroachment.

The spectre of terrorism has tempted governments to consider their population only in terms of strengthening security and, in the euphoria surrounding new technologies, to forget about the individual. For example, the research department at DHS has already informed the public that tests are underway on the use of "psychological scanners" that it will install at airports and use to distinguish terrorists from other passengers.[288] The

---

states, 2004 OJ (L 385/1), 29.12.2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT.

[284] Europa, Biometrics Deployment of EU-Passports: EU – Passport Specification Working Document (EN) – 28/06/2006, http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_en.pdf (last visited June 1, 2010).

[285] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 Establishing a Community Code on Visas (VISA CODE), 2009 O. J. (L 243/1), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:243:0001:0058:EN:PDF.

[286] EUROPEAN UNION, NEW TOOLS FOR AN INTEGRATED EUROPEAN BORDER MANAGEMENT STRATEGY (Feb. 13, 2008), http://europa.eu/index_en.htm (search for "MEMO/08/85" and select first result).

[287] Founding.com, http://founding.com/founders_library/pageID.2129/default.asp.

[288] *See* Pam Benson, *Will airports screen for body signals? Researchers hope so*, CNN, Oct. 7, 2009, http://edition.cnn.com/2009/TECH/10/06/security.screening/index.html?eref=rss_travel.

scanner, called Future Attribute Screening Technology (FAST), is designed to function on polygraph technology and recognise changes in body temperature, blood pressure, and breathing as an individual passes through it.[289] DHS has stated that these indicators can identify potential terrorists or criminals, who security staff will subsequently separate from other passengers and subject to a more detailed enquiry into their identity.[290] This raises the question of whether the government will even inform passengers of such checks or if they will occur clandestinely. There is a further concern that simple discomfort with the idea of air travel may trigger the so-called "signs of a terrorist or criminal." Furthermore, the potential health impact of body scanning is unclear and DHS must provide evidence that direct scanning of this kind is not a health risk.

Without continued investigation into the potential consequences of scanning, this form of encroachment on privacy is excessive even by US standards, and the state should not permit it. Even clear evidence that it might increase security by detecting more potential terrorists should not outweigh the threat to health and privacy. Countries deciding to circumvent the legal, ethical, and medical dilemmas posed by the FAST scanners will be able to do so without difficulty because it remains completely invisible to the public.[291] The introduction of new 3D scanners that offer security personal a detailed view of personal luggage is also troubling. Furthermore, even more invasive technologies are on the horizon, such as the General Electric high-resolution scanner, the CTX 9800 Dsi, which the BBC magazine Focus explicitly praises for its ability to not only reveal the content of luggage, but also the brand of goods within the luggage.[292]

Individuals remain passive and forced to face a decision dictated by the state – a choice between security and privacy – which is unreasonable and unjust. Everybody wants both security and respect for their privacy. The issue is the extent to which the state can encroach on an individual's privacy without unduly infringing on human dignity and privacy. Ensuring security in air transportation is a priority for state intelligence and security services, but states must also restrict their encroachment into individual privacy. State authorities must take both these aspects into account when setting a privacy-based limitation on the use of each new technology intended to

---

[289] DEPARTMANT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf.

[290] *Id.*

[291] *See* Thomas Frank, *Anxiety-detecting Machines Could Spot Terrorists*, USA TODAY, Sept. 28, 2008, *available at* http://www.usatoday.com/news/nation/2008-09-18-bioscanner_N.htm.

[292] *3D Scanner Takes a Closer Look*, BBC FOCUS - SCIENCE, TECHNOLOGY, FUTURE, June 2009, at 16, 17.

increase security in the air and at airports.

There are wide-ranging interpretations of this security and privacy balancing. Proponents of IT innovations in air transportation often completely neglect the privacy issue. They simply pose the question to an individual as a 'black and white decision' on which is the greater priority.[293] Given these choices, individuals are likely to prioritize security if civil liberties mean less to them, and vice versa. Research by political scientists into changes in value indicators after 9/11 revealed an interesting phenomenon – despite the increased sense of threat, most Americans still placed their right to privacy ahead of security.[294] Individuals' personal circumstances are important in balancing these interests, as are their socio-political circumstances, social backgrounds, and other subjective and often unmeasurable factors. As passengers, we do not want to forfeit our privacy rights, nor do we want to travel ill at ease because of the spectre of terrorism.

Another issue that merits careful consideration is whether terrorists can actually be identified. Edwin Bakker from the Netherlands Clingendael Institute of International Relations stated in a study on terrorist profiling that *ex ante* identification of terrorists is an almost impossible task.[295] The study, which analysed convicted terrorists and people accused of terrorism in Europe between 2001 and 2006, indicates that there are very few characteristics shared by the 'average' terrorist.[296] The 'average' terrorist was found to be a man of Arab origin, born and raised in Europe, from a lower or middle-class background. He is between sixteen and fifty-nine years of age (average twenty-seven) and has a one-in-four chance of having a criminal record.[297]

The results of the research are academically useful, but in practice can be misleading and discriminatory. The profile of an average terrorist does not include women, individuals not of Arab origin, persons over fifty-nine years old, etc. Thus, the production of these profiles can be misleading in identifying terrorists in that they create inappropriate and unusable

---

[293] Darren W. Davis & Brian D. Silver, *Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, 48 AM. J. POL. SCI. 28, 29 (2004); Ravich, *supra* note 184.

[294] Davis & Silver, *supra* note 293, at 32 ("In response to a general question of giving up some civil liberties in order to curb terrorism in this country, 55% favored protecting civil liberties . . . . [A]nalysis of public opinion polls conducted after the terrorist attacks, however, this level of support for civil liberties breaks down when applied to specific situations.").

[295] Bakker, *supra* note 186, at 43.

[296] *Id.*

[297] Edwin Bakker, *Jihadi terrorists in Europe – their characteristics and the circumstances in which they joined the jihad: an exploratory study*, NETH. INST. OF INT'L RELATIONS CLINGENDAEL (2006), *available at* http://www.clingendael.nl/cscp/publications/?id=6480&&type=summary.

stereotypes. Terrorism is based on unpredictability and non-stereotyped actions to avoid becoming detected. Profiling individuals through the use of personal data is an unreliable method of finding potential terrorists. Additionally, the use and storage of such information in this time of computer, scientific, and medical advances poses a risk of unintentional exposure of vast amounts of personal data. Outside intruders often illegally access computers – even ones from high-level government agencies.[298] The consequences of a security breach of that kind could be unimaginable.

At present, we expect the state and organisations such as the EU to provide us with maximum security against terrorism while also protecting our civil liberties. What are they actually doing to ensure this? An individual alone is powerless against the state and international organizations, but organized in civil society, individuals acquire power and the possibility of forcing states to act within our expectations, at least as a *vox populi* (voice of the people), if not yet as a more or less equal negotiator. Statewatch is a not-for-profit organisation that criticizes and monitors political and legal decisions by EU institutions that encroach on human rights. Statewatch has repeatedly warned of such violations, including the disputed agreement on the transmission of PNR data to the US.[299]

As groups such as Statewatch have noted, implementing effective anti-terrorist control of airline passengers does not demand a choice of either freedom and privacy (including privacy of personal data) or national security, as though these are mutually exclusive.[300] The European Data Protection Supervisor Peter Hustinx asserts that a state cannot, and must not, force its citizens to choose between security and effective data protection.[301] He emphasizes that effective protection of personal data is completely compatible with the successful prevention of crime, including terrorism.[302] Adequate protection of personal data improves the quality of databases,

---

[298] Even FBI had such an experience. *See* Eric M. Weiss, *Consultant Breached FBI's Computers*, WASH. POST, July 6, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/07/05/AR2006070501489.html.

[299] Statewatch – Monitoring the State and Civil Liberties in Europe, http://www.statewatch.org/ ("Statewatch is a non-profit organization founded in 1991 that monitors the state and civil liberties in the European Union. It is composed of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 14 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe in the fields of the state, justice and home affairs, civil liberties, accountability and openness.").

[300] Ravich, *supra* note 184.

[301] Christine Tréguier, *E.U. Data-Protection Controller: Right to Privacy is Not Absolute*, SILICON.COM, http://www.silicon.com/special-features/protecting-your-id/2004/03/09/eu-data-protection-controller-right-to-privacy-is-not-absolute-39119014/ ("[W]e can come to the conclusion that security is best served when [privacy] is preserved,' Peter Hustinx said.").

[302] *Id*.

which should only be accessible to a restricted circle of authorised people.[303]

DHS data indicates that in autumn 2006, from a total of sixty-three million visitors, the US PNR and US-VISIT systems[304] helped detect 1,200 criminals due to alleged terrorist activity or illegal immigration.[305] DHS makes no distinction between terrorists and illegal immigrants in this analysis. Its placement of these two categories together produces an artificially higher figure, allowing DHS to provide greater justification for surveillance systems regardless of distinctions between different categories of undesirables.

At a time when the EU is reaching agreement on the introduction of a European PNR system, some thought should be given to the method of data collection.[306] The current plan creates a decentralised system where data collection is left to the discretion of Member States.[307] Decentralisation is generally positive, but not in sensitive cases relating to personal data records, where incompatibility and potential system errors not only lead to an ineffective system, but also to the 'leaking' of information and unauthorised use. The information technology for the PNR system is problematic, both in terms of information leakage and identity theft. Consider the case of a security breach of the PNR transfer computer system. Deletion or falsification of data could lead to the creation of new identities or the deletion of old. This, combined with plastic surgery could lead to incorrect identification and potentially catastrophic consequences in international terrorism. Sadly today this is not just a fictional scenario.

Europe is attempting to present the methods of combating terrorism in air transport as a group of proposed measures that generally follow the US pattern. However, the EU is failing to consider the actual effectiveness of technological data processing in preventing terrorism. Authorities present counter-terrorism in air traffic to citizens only as an issue of security versus the protection of privacy. Passengers will thus consider whether they want greater security in exchange for giving up some privacy. As the price for

---

[303] *No excuse for privacy breaches, says EU regulator*, OUT-LAW.COM, Sept. 19, 2006, http://www.theregister.co.uk/2006/09/19/terrorism_privacy_breaches/.

[304] U.S. Department of Homeland Security, US-VISIT Traveler Information, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (Mar. 15, 2010).

[305] *Commission to Propose EU PNR Travel Surveillance System*, STATEWATCH, July 15, 2007, http://www.statewatch.org/news/2007/jul/03eu-pnr.htm.

[306] On November 6, 2007, the European Commission proposed PNR data collection on all air transport passengers into and out of the EU. *See* Commission of the European Communities, Accompanying document to the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Summary of the Impact Assessment, http://www.statewatch.org/news/2007/nov/eu-com-pnr-ia-summary-sec-1422.pdf.

[307] *Id.*

choosing privacy could well be too high in this case, the answer becomes clear: European citizens choose security. It sounds simple, but is there a trick? Can security really be guaranteed by foregoing privacy and relying on profiling personal data each time we leave EU territory?[308] The European Parliament has frequently drawn attention to problems relating to data collection, and has raised the issue of privacy in this regard. The possibility of identity theft and falsification of data in databases is not negligible. Leaving the decision on who can and cannot enter a territory to computer technology could be very dangerous and lead to uncritical decisions based only on technology and databases. Timothy M. Ravich has described two events that demonstrate these problems.[309] In one instance, the computer system did not flag anything unusual when the name Osama Bin Laden was entered into the US system. Conversely federal agents from the TSA, FBI and Secret Service stopped an air passenger travelling from Kentucky twenty-two times because his name was similar to that of a financer of Al Qaeda.

Europol published data for 2008 indicating a 23% reduction in openly planned terrorist acts (compared to 2007). This could be taken in two ways – as an EU success based on a series of counter-terrorist measures that reduced the number of planned terrorist attacks, or as a failure by the EU because it detected at least 23% fewer planned terrorist actions.

States are tightening security measures due to fears of terrorism while the EU and the US are simultaneously removing obstacles to transatlantic flights by concluding the Open Skies Agreement.[310] Millions of passengers cross the Atlantic each year and the agreement is expected to swell those numbers. The Open Skies agreement makes it possible for flights to the US to take off from smaller EU airports that will have to install comprehensive new counter-terrorism security systems that meet the same specifications as at larger airports. Additionally, European airlines can now fly to the US from any EU state, and not just their state of origin as was previously the case.[311] Together with the introduction of a European PNR and ESTA

---

[308] The European Commission specifically emphasises that PNR is at present only planned for air passengers from third countries that land in EU territory. In future, the EU will consider collecting data on air passengers within the Union, again following the US example, which uses a data collection system for all internal flights as well (CAPPS, CAPPS II, Secure Flight and Registered Traveler Program).

[309] Ravich, *supra* note 184.

[310] Council Decision 2007/339, Decision of the Council and the Representatives of the Governments of the Member States of the European Union, meeting within the Council of 25 April 2007 on the signature and provisional application of the Air Transport Agreement between the European Community and its Member States, on the one hand, and the United States of America, on the other hand, 2007 O.J. (L 134) (EC).

[311] One of the main reasons for reaching the agreement is economic: U.S. airlines can buy

system, these circumstances present a major security challenge, and there is uncertainty as to how well the EU will manage it.

up to a 49% stake in European airlines, while European airlines can only buy up to 25% of their US competitors. The EU Commissioner Jacques Barrot said that he supports US and European airlines having equal stakeholding rights, but it is unlikely this will be achieved. At a time of economic slowdown, Americans will not permit foreign takeovers of their leading airlines. *See Open Skies Deal Comes into Effect*, BBC NEWS, Mar. 31, 2008, http://news.bbc.co.uk/2/hi/business/7318455.stm.