Interim Report
on the EU Approach to the Commercial Collection of Personal Data for Security Purposes: The Special Case of Hotel Guest Registration Data

January 16, 2009

LETTER FROM THE CHIEF PRIVACY OFFICER

The beginnings of this report go back to the spring of 2007, at a Brussels meeting of the High Level Contact Group, a joint United States (US)-European Union (EU) effort created to improve transatlantic information sharing in the areas of law enforcement and public security under a common understanding on privacy principles for those exchanges of data. The dialogue convinced the Department of Homeland Security (DHS) Privacy Office participants that, while much is known generally about the US approach to privacy – thanks in large part to transparency requirements enshrined in US law, a robust civil society, and a pluralistic society – we in the US Government know less than we should about the EU's approach. In particular, we lack insight into the application of data protection laws to law enforcement, intelligence, and security agencies, about oversight of law enforcement, intelligence, and security agency-use (collectively, security service use) of personal data, and about the effectiveness of that oversight. As a result of the lack of full information on both sides, discussions on security and privacy have not been as fruitful as they should have been.

To bolster understanding in this area, to be equipped to enforce the provisions of Article 5 of the 2007 Passenger Name Records (PNR) Agreement, and recognizing that over 12 million Americans visit countries in Europe every year, the Department of Homeland Security (DHS) Privacy Office decided to study the application of EU data protection law and practice in the context of the commercial collection of personal data for security service use. Specifically, we looked into the EU practice of mandatory collection of hotel guest registration data for use by security services, a longstanding practice that pre-dates by decades, if not centuries, the various EU data protection laws in place today.

This report is the effort of nearly two years' work. Frankly, I was surprised at how difficult it was, generally, to get information from our colleagues in the various data protection authorities, justice and interior ministries, and the European Commission. Significant gaps remain in our understanding of this practice in the EU and the application of data protection laws to it, but we are more informed now than we have been in the past.

We did not limit our inquiries to organs of the state. We contacted hotels, hotel industry associations, academics, non-governmental organizations, and even hotel registration software manufacturers, to better understand law enforcement and security agencies' collection and use of hotel guest registration data. As was the case when we contacted our Government colleagues, we encountered some resistance to our requests, so we have supplemented the information we did receive with our own research. I want to stress that we are not European lawyers; and we may not fully understand all of the nuances of EU or European national law, facts that explain in part why this is an interim report.

This report is intended to serve three purposes: 1) to contribute to existing international debates over protecting privacy through greater transparency into specific applications outside the US; 2) to better inform current and future US Government officials tasked with responding to European questions and complaints about privacy; and 3) to help Americans who travel abroad to better understand the privacy implications of their travels. To meet these objectives and

ensure the American public is informed of its Government's efforts to protect its privacy abroad, this report is being made available to the general public.

As of the date of this report, it remains unclear whether EU Member State law enforcement, intelligence, and security agencies actually meet the standards for the protection of personal data that European interlocutors have argued various EU laws require. The level of EU transparency in this area does not seem to meet standards imposed by US law as evidenced by the difficulty my office faced in obtaining data from official sources. In addition, numerous questions remain regarding the effectiveness in the oversight of law enforcement and security agency collection and use of hotel guest registration data in the EU.

Our inquiries are not complete, which is another reason for issuing this document as an interim report. We look to our colleagues in the EU and the Member States to provide the Privacy Office with the comprehensive information that we requested on oversight mechanisms covering security service use of commercially-collected information. This report is intended as an aid to providing greater understanding to those who face these issues in the course of their duties and to the traveling public. I am convinced that greater information and understanding on both sides will inevitably lead to increased security and improved privacy protections.

Respectfully,

Hugo Teufel III
Chief Privacy Officer
Chief Freedom of Information Act Officer
United States Department of Homeland Security

Interim Report
on the EU Approach to the Commercial Collection
of Personal Data for Security Purposes:
The Special Case of Hotel Guest Registration Data

I. Executive Summary

The United States (US) and the European Union (EU) have been, and in the future will continue to be, engaged in discussions on transatlantic exchanges of information, including personal information collected commercially but used for security purposes. There is widespread understanding of the US approach to privacy within the Federal government, including oversight of law enforcement, security, and intelligence agency use (collectively, security service use) of personal information, because of the accepted government practice of transparency within government. Far less is understood in the US about the EU approach to data protection and oversight within its security services.

Pursuant to the Department of Homeland Security's 2007 agreement with the Council of the European Union regarding the transfer of Passenger Name Record (PNR) data to the Department of Homeland Security (DHS) by air carriers operating flights between the US and the EU, the DHS Privacy Office recently published a comprehensive report on PNR.[1] Mindful of this responsibility in 2007, the DHS Privacy Office looked for an analogous situation in which commercial entities collected PII for security service use. The DHS Privacy Office chose to investigate and report on the EU practice of collecting hotel guest registration data, as from a functional perspective it most closely mirrored PNR data collection and use. For comparative purposes, the DHS Privacy Office discusses PNR data within the report.

Within the European Union, Article 45 of the Schengen Implementing Convention makes hotel guest registration data a requirement of Member States and specifies the amount of information to be collected. The applicable EU oversight mechanisms for hotel guest registration data collection and use, however, are unclear. Certainly, hotel collection and use of this data falls under the First Pillar[2] of the EU structure set out in the Maastricht Treaty, or Treaty on European Union (TEU), that created the EU in 1992, and the EU Data Protection Directive. However, security service collection and use of hotel guest registration data would likely fall under the Third Pillar of that structure, and no data protection directive or equivalent law exists at the EU

[1] The report, entitled *A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union,* is available on the Privacy Office website at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

[2] The concept of "Pillars" is generally used in connection with the Treaty on European Union (TEU), signed in Maastricht on February 7, 1992. The TEU consists of three Pillars and is reflects the EU's authority over data protection. The First Pillar, the Community pillar, corresponds to the three Communities: the European Community, the European Atomic Energy Community (Euratom), and the former European Coal and Steel Community (ECSC); the Second Pillar is devoted to the common foreign and security policy; and the Third Pillar is the pillar devoted to police and judicial cooperation in criminal matters. Subsequent to the establishment of the EU, the Treaty of Amsterdam, signed in Oct. 1997, transferred some of the fields covered by the Third Pillar to the First Pillar (free movement of persons- specifically, immigration and asylum), leaving only criminal justice in the Third Pillar.

level for the Third Pillar. Importantly, there has been no oversight reporting at the EU level regarding the collection and use of hotel guest registration data, or the implementation of the terms of Article 45.

The DHS Privacy Office faced great difficulty in obtaining relevant information from the responsible EU and Member State data protection, justice, and interior ministry officials. As of the date of this report the DHS Privacy Office had sufficient information to report on only eight Member State countries. There are differences in the way each of the eight countries requires hotels to collect hotel guest registration data and make it available to security services. Significantly, the DHS Privacy Office has observed a trend of electronic capture and transmission of this data to security services.

There are also differences in the way each of the eight countries we studied has established oversight mechanisms for security service collection and use of hotel guest registration data. Data Protection Authorities may not always be fully competent to investigate security services, though other bodies may exist to do so. Importantly, none of the eight countries has actually conducted and made publicly available audits or investigations of security service use of hotel guest registration data. The lack of publicly available oversight reports, whether at the EU level or from the Member States, stands in stark contrast to the publicly available oversight reports on PNR.

The DHS Privacy Office intends to continue to make inquiries and gather information on the laws governing the collection and use of hotel guest registration data by EU Member States and other European nations bound by the pertinent European laws and conventions, as well as these countries' security service oversight mechanisms. There will be more, not fewer, transatlantic exchanges of data in the future, and those exchanges are likely to involve commercially-collected data. The stakes are too great for the EU and the US to not reach a mutual understanding of the protections afforded in law and practice, as continued ignorance on both continents makes it more difficult to implement the essential values of privacy and security in transatlantic data transfers.

II. Introduction

The US and the European Union (EU) share a long history of cooperation and collaboration on issues concerning data protection and privacy. Recent discussions between the US and the EU regarding the protection of personal data have allowed us to identify a number of significant commonalities in our approaches based upon our shared values.[3] The discussions between our governments, through the High Level Contact Group (HLCG),[4] have rested on the understanding that the US and EU have different systems to protect personal data, but that ultimately each system provides the individual with effective and comparable protections when law enforcement

[3] High Level Contact Group (HLCG) Common Principles, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/report_02_07_08_en.pdf; see also http://www.dhs.gov/xlibrary/assets/privacy/privacy_intl_hlcg_usa_statement_data_privacy_protection_eu_12122008.pdf

[4] The HLCG is a joint US-EU effort created to improve transatlantic information sharing in the areas of law enforcement and public security under a common understanding on privacy principles for those exchanges of data.

authorities handle such information. Importantly, the US and EU approaches share essentially the same core principles.

In spite of this commonality, there has been significant criticism from the European data protection community about differences, with particular criticism directed at DHS and its use of passenger name record (PNR) data for security and safety purposes. Similar concern arose from within the EU when the HLCG began discussing a framework for future transatlantic exchanges of data.

To better understand the EU and Member State sensitivities to the US Government's use of commercially-collected personal data, in late spring of 2007, the DHS Chief Privacy Officer and the then-Privacy and Civil Liberties Officer for the US Department of Justice (DOJ) wrote to the European Data Protection Supervisor and the Article 29 Working Party regarding hotel guest registration data and its compulsory collection in Europe. The officials inquired whether the European practices with respect to the commercial collection of personal data for security service[5] uses were as restrictive as those that some within Europe sought to impose on the US in its collection of PNR data.

In a series of follow-up letters, the DHS Privacy Office expanded its inquiry to better understand collection of personal data within the EU from hotel guests and the data protection principles that apply to hotels; security service collection of this data from hotels and the principles that apply to security services; the transparency of the process, both with hotels and security services; and the oversight, from a data protection perspective, of security services. This interim report discusses these practices from the perspectives of eight EU Member State countries. The purpose of the report is to provide US Government officials and the American public with a better understanding of European data protection in the context of EU law enforcement, intelligence, and security agencies that rely upon commercially-collected personal data. It is the hope of the DHS Privacy Office that, armed with this information, the US Government and the travelling public will make informed decisions which, in the aggregate, will benefit the protection of personal privacy at home and abroad.

III. Authority

The DHS Privacy Office was the first statutorily required, comprehensive privacy policy office in any US federal agency. The Chief Privacy Officer serves under the authority of the Secretary and Section 222 of the Homeland Security Act of 2002, as amended.[6] The DHS Privacy Office has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personally identifiable and Departmental information. In 2007, Congress expanded the Chief Privacy Officer's responsibilities under Section 222 to include explicit investigative authority, the ability to

[5] Recognizing that the phrases "security agency" and "security service" may have a different meaning in some European countries than in the United States, for the purposes of this report "security agency" and "security service" are used interchangeably to mean a law enforcement, police, intelligence, justice, home affairs, or security agency or service.

[6] 6 U.S.C. sec.142.

conduct regular reviews of privacy implementation, and greater coordination with the Inspector General.

Of significance to this report is Section 222(b)(1)(B), which authorizes the Chief Privacy Officer to "make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable." In this case, the DHS Privacy Office determined that the EU practice of sharing personal data collected by hotel operators with law enforcement, security, and/or intelligence agencies is necessary in order to enforce the provisions of Article 5 of the 2007 Passenger Name Records (PNR) Agreement.[7] Further it is desirable to deepen US understanding of these practices to inform discussions over future data transfers and to ensure the privacy of the millions of Americans who travel to Europe and stay in European hotels every year.[8]

IV. Methodology

Only a few EU Member States have recently established systems to collect and analyze PNR. The DHS Privacy Office anticipates reviewing these systems sometime in the future, according to the terms of the 2007 PNR Agreement. Until Europe has greater experience with the collection and processing of PNR and the DHS Privacy Office conducts an official review of these systems they present an imperfect model for understanding the EU approach to oversight of commercial collection of personal data for security purposes. For these reasons, the DHS Privacy Office decided to examine the collection and use of hotel guest registration data, and the applicable transparency and oversight mechanisms in place.

The DHS Privacy Office's methodology has evolved over the course of this inquiry. In June 2007, the DHS Chief Privacy Officer and the Privacy and Civil Liberties Officer for the US Department of Justice (DOJ) sent letters to the European Data Protection Supervisor (EDPS) and the German Federal Data Protection Commissioner, in his capacity as the head of the Article 29 Working Party, regarding hotel guest registration data and its compulsory collection in Europe.

The initial responses, while helpful, were incomplete, perhaps because the US letters did not distinguish between the commercial collection of the data from hotel guests and the security service collection of the data from the hotels, and did not focus on transparency and oversight with respect to the security services' use of this personal data. Therefore, the DHS Privacy Office pursued the matter directly with the European Commission and various EU Member States. In meetings with various Member State justice and interior ministry officials, DHS Privacy Office officials began to better understand the range of issues associated with the mandatory collection of hotel guest registration data. It became clear to the DHS Privacy Office that not only were there more questions to be asked, but more persons and entities from whom to seek the answers to those questions. Accordingly, the DHS Privacy Office contacted senior privacy and security officials from EU Member States as well as officials from the European

[7] The 2007 PNR Agreement is available at http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf

[8] According to the U.S. Department of Commerce International Trade Administration report "2007 Profile of U.S. Resident Travelers Visiting Overseas Destinations (Outbound)," 39% of the 31,228,000 travelers went to Europe in 2007. This would mean approximately 12,178,920 hotel registrations in 2007. Report available at http://tinet.ita.doc.gov/outreachpages/download_data_table/2007_Outbound_Profile.pdf

Commission, EUROPOL, and the office of the EDPS. The DHS Privacy Office also contacted members of the privacy advocacy community and academics, various hotel industry associations, hotels, and even hotel registration software manufacturers in Europe and the US.

To distinguish between privacy protections of the hotels' collection of hotel guest registration data and those related to the security agencies' subsequent use of that data, our questions focused on implementation of the Fair Information Practice Principles (FIPPs). Specifically, we asked questions regarding the use, retention, notice provided, access/redress for the data subject, onward transfers (both within the government and beyond their borders), transparency, and oversight/competence of the data protection office. A sample letter can be found in Appendix 1.

Each of the persons and entities contacted by the DHS Privacy Office had a "piece of the puzzle" needed to better understand the European practice of mandatory collection of hotel guest registration data and the European approach to transparency and oversight of security service use of personal data. No one person or authority could provide a comprehensive answer to our questions. In addition, the collective response of our interlocutors fails to paint a complete picture. More comprehensive information on oversight mechanisms covering security service use of commercially-collected information, to include audits or investigations into such use, are necessary before a final report can be completed.

V. EU Member State Use of Hotel Guest Registration Data

The Privacy Office research found that many European nations have a long tradition of requiring commercial accommodation providers to collect personal data for security purposes, possibly stretching as far back as the Middle Ages and certainly pre-dating the EU.[9] The purpose for this collection was and remains today based on safety and security, core responsibilities of the sovereign. Similarly, the US Government use of passenger reservation information and its predecessor manifest lists has been in practice for nearly 200 years as an integral part of US sovereignty and responsibility for immigration and border controls. In Appendix 5 of this interim report, we provide a brief description of the historical antecedents to PNR, along with a discussion of PNR and Advance Passenger Information (API), for comparative purposes.

In Europe, the tradition has been for hotel guests, upon registration, to fill out a card or form providing personal data including surname, nationality, sex, and identity card number. The hotel retains these cards for a set period of time, making them available to the authorities whenever asked. In some locales, the law enforcement authorities visit the hotel and collect the cards on a regular schedule (*e.g.*, daily, weekly, monthly, semi-annually). The local authorities review the cards to find wanted individuals or suspected criminals.[10]

[9] On December 4, 2008, the Belgian Ambassador to the U.S., Dominique Struye de Swielande informed DHS Assistant Secretary for Policy Stewart Baker, that Belgium had been engaged in the collection of hotel guest registration data for over 100 years.

[10] Security service use of hotel registration information has not escaped popular fiction. In Frederick Forsyth's *The Day of the Jackal*, French police seeking to apprehend a hired assassin, make use of hotel registration cards, along with border entry cards to track the individual. Only good luck and proper tradecraft keep the assassin ahead of the police until the day of the attempted assassination.

To better understand the tradition of using hotel guest registration data for security purposes, the DHS Privacy Office spoke with various EU law enforcement officials. Of particular interest were our conversations with German Interior Ministry officials[11] and the Director of EUROPOL.[12] The DHS Privacy Office learned that the German Government used hotel guest registration data in the 1960's and 1970's to great effect in its battle against German terrorist groups, such as Bewegung 2. Juni,[13] Baader-Meinhof-Gruppe/Rote Armee Fraktion,[14] and Revolutionäre Zellen,[15] during the "German Autumn." German security services would use registration cards to construct profiles of likely terrorists, based on various criteria (*e.g.*, age, companions, type and quality of hotel or other lodging, use of cash for transactions, etc.) and then would search to find persons who fit the profiles.[16]

Reviewing individual cards by hand is a time-consuming process, more effectively achieved through information technology, the use of which has triggered increased interest in privacy and data protection. It is the DHS Privacy Office's understanding that information technology is in use in some EU countries to collect and transmit hotel guest registration data to security services.

Most hotels of any size today rely upon property management software (PMS) to keep track of reservations, day-to-day activities, catering, and other hotel functions. The PMS maintains guest name records similar to PNR, which may come directly from a guest or travel agent or via a computer reservation system, such as Sabre, Worldspan, Amadeus, or Galileo. Hotels store the accumulated personal data on servers, which may be owned by the hotel, the company that produced the PMS, or a third party. The servers may be resident in the hotel, elsewhere in the country where the hotel is located, or anywhere in the world. If the hotel chain is a US company or the hotel has opted to use the PMS company's servers and the PMS company is American, a hotel may need to transfer data from the US in order to comply with European requirements.[17]

In some EU countries, PMS systems are set up to provide for a "police interface," allowing the direct, routine transmission of hotel guest registration data to law enforcement agencies. Data fields are unlimited and may include name; address, including city, country, and postal code; gender; date of birth; place and country of birth; identification number (internal pass or

[11] Meeting in Berlin, June 12, 2007.
[12] DHS Privacy Office meeting with Max Peter Ratzel at the DHS Privacy Office, December 11, 2008. Mr. Ratzel is a former Bundeskriminalamt (BKA or "Federal Office for Criminal Investigations") officer.
[13] Movement 2nd of June.
[14] The Red Army Faction was also known as the Baader-Meinhof Group or Gang.
[15] Revolutionary Cells.
[16] The use of "Rasterfahndungen," and other techniques used by the BKA during the German Autumn, likely would not be permitted in Germany today. Nevertheless, German law still requires the collection of hotel registration data and, indeed, requires anyone living in their own home, renting an apartment, staying in a hotel or pension, or staying at a campground or hostel to provide registration information of police use.
[17] The potential for overlapping, or conflicting, data protection or privacy laws is great. Globally, there are two major property management software producers. One company is based in the United States, and the other is based in the Netherlands. Not unsurprisingly, many countries in which these companies' software products are used have unique legal requirements that require modification of the base software to collect guest information for government purposes. For example, many Latin American governments regulate the printing of folios to ensure that hotels are properly remitting to the government taxes charged from guest stays.

passport); and profession. The PMS has been designed specifically for the purpose of electronically transmitting hotel guest registration data directly to the police.

Though many in Europe might view the collection of PNR and the collection of hotel guest registration data as different, our study found significant similarities. For instance, both were legislated within the last 10 years as the result of dramatic shocks to past border management and law enforcement practices. In the US, the voluntary practice of collecting and processing PNR was evaluated as a result of the terrorist attacks on September 11, 2001, and further legislated under the Aviation and Transportation Security Act of 2002.[18] Likewise, as the EU deconstructed its internal border the need for increased harmonization of border control and law enforcement practices was necessary to ensure one Member State could trust the practices of its neighbors. As a result, the collection of hotel guest registration data for use by security services became mandatory under the Schengen Implementing Convention and integrated into EU law in 1999.

Title III (Police Security), Chapter 1 (Police Cooperation), Article 45 of the Schengen Implementing Convention provides for contracting parties to agree to implement the collection of hotel and other personal accommodation registration data. Article 45 states:

> 1. The Contracting Parties undertake to adopt the necessary measures in order to ensure that:
>
> (a) the managers of establishments providing accommodation or their agents see to it that aliens accommodated therein, including nationals of the other Contracting Parties and those of other Member States of the European Communities, with the exception of accompanying spouses or accompanying minors or members of travel groups, personally complete and sign registration forms and confirm their identity by producing a valid identity document;
>
> (b) the completed registration forms will be kept for the competent authorities or forwarded to them where such authorities deem this necessary for the prevention of threats, for criminal investigations or for clarifying the circumstances of missing persons or accident victims, save where national law provides otherwise.
>
> 2. Paragraph 1 shall apply *mutatis mutandis* to persons staying in any commercially rented accommodation, in particular tents, caravans and boats.

Signatory States include most EU Member States (with the exception of the United Kingdom and Ireland), as well as other countries external to the Union (Norway, Switzerland, and Iceland). Any Member State implementing Article 45 must do so in accordance with other European laws, to include the 95 Directive,[19] Article 126 of the Schengen Implementing Convention (requiring member states to adopt national provisions to a level at least as great as found in Convention

[18] 49 U.S.C. sec. 401.

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individual with regard to the processing of personal data and on the free movement of such data; OJ L 281, November 23, 1995, page 31.

108), and Article 129 of the Schengen Implementing Convention (requiring a level of data protection that complies with the principles of Council of Europe R (87) 15).

Article 45 requires the personal completion and signing of "registration forms" and the "presentation of a valid identity document." The Article does not specify data quality standards, the nature of the form, the information to be collected, or specify the type of identification to be shown. Similarly, establishments must keep the "registration forms" or forward the forms to the "competent authorities" for threat prevention, criminal investigations matters involving missing persons and accident victims, or whatever national law requires, but there is no definition of what a "competent authority" is. Further, the sum of acceptable purposes is quite broad, including the national law exception. As Article 45 does not provide for further standards and no further harmonization on this matter has taken place, implementation and enforcement of this provision among the Member States varies greatly.

Although expressly covered in the EU's Schengen Implementing Convention, there is no guidance from the European Commission on the proper implementation of Article 45. Moreover, we are aware of no exercise of oversight by the EDPS or the Article 29 Working Party. The European Commission, however, recently asked the Working Party to deliver an opinion on the "differences and inconsistencies in the application of data protection rules" with regard to hotel registration[20] to promote "the uniform application of the Data Protection Directive 95/46/EC in all Member States."[21] This is an interesting development but the issue here is not the practices of *hotels* in the collection and use of hotel guest registration data; rather, it is the practices of *security services* in the collection and use of hotel guest registration data, and the oversight of those practices.

VI. The EU Pillar Structure and its Application to Commercial Collection of Personal Data for Security Service Use

The collection and use of guest registration data by hotels and security agencies in Schengen signatories must satisfy EU law as expressed in the pillar structure of the Treaty on European Union (TEU) and national law.

As noted above, the TEU consists of three Pillars and is reflects the EU's authority over data protection. The First Pillar, the Community pillar, corresponds to the three Communities: the European Community, the European Atomic Energy Community (Euratom), and the former European Coal and Steel Community (ECSC); the Second Pillar is devoted to the common foreign and security policy; and the Third Pillar is the pillar devoted to police and judicial cooperation in criminal matters. Subsequent to the establishment of the EU, the Treaty of Amsterdam, signed in Oct. 1997, transferred some of the fields covered by the Third Pillar to the First Pillar (free movement of persons- specifically, immigration and asylum),[22] leaving only criminal justice in the Third Pillar.[23]

---

[20] Letter from Alain Brun, Unit D5, Justice, Freedom and Security Directorate-General to Hugo Teufel, Chief Privacy Officer, DHS (December 3, 2008).
[21] December 3, 2008 letter from the European Commission to the Chief Privacy Officer.
[22] http://europa.eu/scadplus/glossary/eu_pillars_en.htm
[23] See discussion in Maria Fletcher & Robin Loof, EU Criminal Law and Justice, Elgar European Law, pages 1-2.

The European Commission enacted *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (the 95 Directive) in order to remove potential obstacles to personal data flows between EU Member States and to ensure a consistent level of protection within the EU.[24] The 95 Directive, however, applies only to the First Pillar. (See Appendix 7 for a summary of the application of the Pillar structure to US collection of PNR data.)

Convention 108, which was signed by the Member States in 1981, is the first binding international instrument that protects the individual against abuses that may accompany the collection and processing of personal data and that seeks to regulate at the same time the transfrontier flow of personal data.[25] The processing of personal data that takes place in the field of law enforcement falls under the scope of application of Convention 108. Convention, however, 108 "is too general to effectively safeguard data protection in the area of law enforcement." [26] Although the EU Council recently passed *Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters* ("Data Protection Framework Decision" or DPFD), it applies only to personal data that is transmitted across borders, and does not apply to use by law enforcement or security agencies within the Member State where the data was collected.

It is notable that the EU has oversight mechanisms for EU law enforcement and security institutions. For example, data protection provisions in the EUROPOL Convention are overseen by an independent joint supervisory body, which reviews the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and utilization of the data held by EUROPOL. In addition, the joint supervisory body also monitors the

[24] http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[25] http://conventions.coe.int/Treaty/en/Summaries/Html/108.htm
[26] Declaration of the Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005, http://www.cnpd.pt/bin/actividade/Outros/krakowdeclarationfinalversion.pdf
The EU's growing authority in the area of "justice, freedom and security" has necessitated data protection rules where information is shared across borders. The growing authority is evident from the Hague Programme, adopted by the European Council in November 2004. The Hague Programme contained two resolutions relevant to data protection in the Third Pillar, to be realized as of January 2008: (1) Biometrics and Interoperability of Information Systems should be pursued to prevent illegal immigration, fight crime, and prevent terrorism. (2) The Principle of Availability should be the governing standard for information flows throughout the European Union. Availability is defined as fast and direct access for any law enforcement officer to necessary information held in any other member state.

Availability, with its implications for decreased state control of law enforcement information, is a politically sensitive concept. The realization of Availability has been mixed at best, while the goal of biometrics and linked information systems has enjoyed greater success. Proposals that would have fully realized Availability have languished, but there is a mechanism that may be considered as achieving partial implementation: the Framework Decision on the Protection of Personal data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters ("Data Protection Framework Decision" or DPFD).

permissibility of the transmission of data originating from EUROPOL.[27] Similar joint supervisory bodies exist for the Customs Information System, the Schengen Information System,[28] and Eurojust.[29] Where an EU database falls within the First Pillar, as with EURODAC,[30] the European Data Protection Supervisor (EDPS) has supervisory authority.[31] (For a discussion of data protection in the Third Pillar, see Appendix 6).

Oversight within Member States for data protection in law enforcement and security agencies varies. In some countries it may be in the hands of Parliamentary Committees, in others internal agency authorities may exercise full supervision. Some countries have Ombudsmen who respond to citizen complaints about government on a range of issues, including data protection violations. In the course of our research, some data protection authorities claimed oversight over all government agency collection of personal information, regardless of the purpose, but they did not provide any references (see country section below for more detail)**.**

VII. Selected European Country Laws Regarding Private Collection and Public Use of Hotel Registration Personal Data

After nearly two years of inquiries to most of the EU Member States, and a few non-EU countries within Europe, the DHS Privacy Office felt it had a sufficient understanding of the approaches to the collection and use of hotel guest registration data in eight Member States: Austria; Belgium; France; Germany; Italy; the Netherlands; Portugal; and Spain. Numerically, these countries represent less than a third of the 27 Member States of the EU. Nevertheless, a significant number of the over 12 million Americans who visit Europe annually visit these eight countries. To aid the Department, other US Government agencies, and American travelers, we list the highlights of our findings for these countries.

A. Austria

Austria's primary data protection law is the Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000). The Austrian Data Protection Commission has competence over both private and public sector data controllers, to include security services. The Austrian Interior Ministry has responsibility for collection of hotel registration data under the country's residence laws.

Hotel Collection – Hotel guest registration data is made available to competent authorities upon request. More precisely, the hotel information is first transmitted by the hotels to the public authorities in charge of population registers that store this data. These authorities then verify and authorize access by the police in specific cases specified by law. Hotels retain the data for seven years. Travelers are not necessarily informed by the hotel of the purpose of this registration.

---

[27] The Europol Convention, Article 24, at http://www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf

[28] SIS maintains and distributes personal information related to border security and law enforcement

[29] Eurojust is an EU agency established to enhance shared judicial cooperation.

[30] EURODAC is a fingerprint database for identifying asylum seekers and irregular border-crossers

[31] http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/65

Security Agency Use – As stated above, the Austrian Interior Ministry has responsibility for collection of hotel registration data under the country's residence laws. In a letter dated October 30, 2008, the Austrian Data Protection Commissioner advised the DHS Privacy Office that she has forwarded the Office's inquiries to the Interior Ministry. To date, the DHS Privacy Office has not received a response from the Austrian Interior Ministry.

B. Belgium

Belgium's data protection law is the Law of December 8, 1992 in relation to the Processing of Personal Data. It was modified by the Law of December 11, 1998, implementing EU Directive 95/46/EC, and the Law of February 26, 2003. Belgium's hotel registration laws are the Law of March 1, 2007 (Articles 141 to 147) and the Royal Decree of April 27, 2007.

Hotel Collection – Hotels collect given and family name, place and date of birth, nationality, ID document number, date of arrival and departure, and name and surname of accompanying children under 18. As recently as 2007, hotels were required to collect the guest's automobile license plate number, but they are no longer required to do so. Information is collected from Belgian and non-Belgian hotel guests. Data registered by hotels must be kept for seven years after a traveler's departure, at which point it must be destroyed. Previously, hotels were required to collect the information on paper. As of May 28, 2007, hotels may collect the data electronically**.**

Security Agency Use – The Law of 30 November 1998 provides the legal basis for intelligence and police services and states that only these "law enforcement authorities" may ask hotels for traveler data. If police request the data, hotels must provide it. The Law of 5 August 1992 defines police duties and permissible uses of this data, including purposes within the scope of their mission "to maintain public order" within the scope of their criminal investigation mission; and the search for persons who are recorded in the national police database.

Police do not have to inform the data subject that their data is being used for law enforcement purposes a data retention schedule is not specified, but the law provides that data should be retained "no longer than necessary" to achieve the purpose. Article 44/1 of the Law of 5 August 1992 on police duties contains an exhaustive list of all the authorities to whom the police may disclose personal data strictly in the context of their duties, *i.e.*, foreign police services, Belgian intelligence services, Interpol, or EUROPOL. The Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee may have oversight authority.

C. France

French data protection is covered under Act no. 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties, as amended by the Act of August 6,

2004, relating to the protection of individuals with regard to the processing of personal data. The French Interior Ministry has responsibility for implementation of the relevant French decrees for the collection of foreign guest hotel registration data.

Hotel Collection - French decree (article R 611-25 of the Code of the entrance and the stay of the foreigners and the right of asylum) requires hotelkeepers to obtain a signed registration form from foreign visitors. Data collected includes family and first names, date and place of birth, nationality, and home address. The information is transmitted daily to the police authorities.

Security Agency Use – The French Interior Ministry is the data controller of information transferred from hotels. There are limits as to the entities with which the police can share this data, and the DPA must be informed. In January 2008, the French Data Protection Authority or the CNIL (La Commission Nationale de l'Informatique et des Libertés) advised the DHS Privacy Office that it had asked the Ministry to respond to DHS regarding practical modalities of operation, retention period, and lack of information, particularly the right of access and modification by data subjects (article 32 of French data protection law dated January 6, 1978 and modified August 6, 2004). To date, the CNIL apparently has not received a response from the French Interior Ministry.

D. Germany

The German Federal Data Protection Act is the primary data protection law. Germany has a federal system and up until 2009, the data protection laws of the various Länder applied to the collection and use of hotel guest registration data and registration data generally. As of 2009, new legislation will establish a central federal register which will contain the all hotel guest registration data. The Federal Ministry of the Interior is preparing new legislation that will establish a Central Federal Registration Register in addition to the existing local ones.

Hotel Collection – Pre-2009, a framework of federal and state laws exists on the compulsory registration of citizens, including foreigners, requiring completion of and signature on a form when checking into a hotel. Section 16 of the Framework Registration Act lays down general rules for the registration of hotel guests; state law identifies specific rules. Foreigners must provide an identity document; data collected includes arrival/departure dates, family and given name, date of birth, permanent address, citizenship, and number of accompanying minors. Hotel guest registration data is not routinely transferred to security services.[32] All state Registration Acts require that the completed registration forms be held for possible law enforcement inspection. The data is generally retained for one year, at which time it is destroyed.

Security Agency Use – Pre-2009, the disclosure of the collected data is regulated

[32] There are a variety of agencies that might request this information: the Federal Intelligence Service; the Military Counter-intelligence Service, the Federal Criminal Police Office, the Federal Police, the Customs Investigation Service, the Attorney General, the constitutional protection office, criminal prosecutors and courts and Länder police agencies, provided that the personal data are required for the fulfillment of their statutory duties.

differently in the various state Registration Acts. Hotel guest registration data may be used in preliminary criminal proceedings, to include the avoidance of danger, apprehension of fugitives and investigation of missing persons and accident victims.

There is no statutory requirement to inform the DPA when dissemination to the police or security authorities takes place. Data subjects are not informed that their data is made accessible to the police. State data protection commissioners have the right to monitor whether police or other security authorities observe the legal prescriptions for data protection requirements. Personal data may be disseminated to foreign public, supranational and international agencies.

E. Italy

The Italian data protection law is the Personal Data Protection Code, enacted by Legislative Decree of June 30, 2003, No. 196. Decree 773/1931 and ministerial decree 11 December 2000 regulate the transfer of personal data from guests to Italian security agencies.

Hotel Collection - Data collected includes passport number and expiration date, first and last name, date and place of birth, and place of residence. The hotel retains the data for billing purposes only and no longer than necessary.

Security Agency Use – Hotel registration personal data is transferred within 24 hours to local police, either manually or electronically. Police authorities may use the data in question only for the purposes provided for in the relevant legislation as related to public security. Security agencies are not required to notify individuals that their hotel registration data is being used for law enforcement purposes. Security agencies can share personal data with other Italian government and third party agencies if so provided for explicitly by law and on a case by case basis. Police authorities may retain it "for no longer than is necessary to comply with [public security/public order] purposes."

The DPA is authorized to oversee hotel collection of the data,[33] and is also in charge of supervising the processing operations performed by the security service. Section 160 of the Data Protection Act regulates the investigations the DPA is empowered to perform in respect of police, law enforcement, and intelligence services.

F. The Netherlands

The Dutch Personal Data Protection Act of 2000 covers data protection generally. The Dutch law covering hotel guest registration data is the National Criminal Code, Article 438. Like Germany, the Netherlands requires individuals living within the country to register with the authorities under Article 2 of the Municipal Basic Administration Personal Data Act. The Interior Ministry is responsible for these registration requirements.

[33] See also Ministry of the Interior Decrees of July 5, 1994 (No. 30457) and December 11, 2000 (no. 1329100) and Legislative Decree June 30, 2003 (no. 196).

Hotel Collection - Article 438 requires hotel owners to ask arriving guests for a valid travel document or ID card and to collect the type of document, name, profession, place of residence, and arrival/departure dates. It is prohibited to copy or scan an ID card. Registration information is then shared with the Mayor or his designee (*e.g.,* the police) upon request. A municipal General Local Bylaw may establish additional requirements with respect to recording information about guests of overnight lodging facilities.

There are no specific regulations concerning data retention for hotel guest registrations, but the Data Protection Act requires that personal data generally be retained for "no longer than necessary." The data is collected on a municipal level, and there is no national central database for hotel registration data. Under the use limitation principle, hotels must inform the DPA each time police or intelligence agencies are given registration information.

Data subjects can exercise the right of access provided by article 35 of the Data Protection Act and right of rectification by article 36, although this is not an absolute right. The Data Protection Act, the Judicial Information Act, and the Police Data Act address data protection and all have some degree of oversight by the DPA.[34]

Security Agency Use – As mentioned above, the police may request the information from the hotel. The authorities may not request copies of hotel guests' passports. "Personal data comprised in hotel registration is not systematically collected by the Dutch authorities";[35] however, it is the DHS Privacy Office's understanding that there is or will be an ongoing pilot project in either Amsterdam or Rotterdam in which hotels will electronically transmit hotel guest registration data to the authorities. Apparently, this will be done with existing hotel PMS systems.

Article 17 of the Intelligence and Security Services Act 2002 authorizes the intelligence and security services to request any controller of personal data to provide them with all the data they may need for any purpose associated with the official duties entrusted to them. The Act has special rules on the right of access of data subjects to data processed by the services concerned, with exceptions. Once the police have the registration information, its handling is supervised by the Ministry of Justice, not the DPA. Police may informally share this information with law enforcement in other EU Member States. The IAVD, an intelligence agency, is under a Parliamentary oversight committee and must also respond to the national Ombudsman, who takes up all complaints against government. The DHS Privacy Office has written to the Dutch Interior Ministry for information on the IAVD's use of personal hotel registration data. To date, the DHS Privacy Office has received no response from the Dutch Ministry of the Interior.

---

[34] See also The Personal Data Protection Act (Wbp), Criminal Code (WvSr), General Local Regulations (AVP), and Intelligence and Security Services Act 2002 (Wiv, Article 6).

[35] Letter from Robert K. Visser, Directorate-General for Legislation, International Affairs and Immigration, Dutch Ministry of Justice, to Hugo Teufel III, Chief Privacy Officer, U.S. Department of Homeland Security, November 7, 2008.

G. Portugal

Act No. 67/98 of October 26, 1998, Act on the Protection of Personal Data, is the Portuguese data protection law. Portaria no. 23/2007 provides that all who offer paid accommodation are required to inform the Borders and Foreigners Service (SEF)[36] (or, when not available, the Public Security Police or the Republican National Guard) whenever foreign guests are present. Portaria no. 287/2007 creates the "Sistem de Informação de Boletins de Alojamento" (SIBA), mandating the electronic transmission of notification of the presence of a foreign guest. Portaria no. 415/2008 imposes a "Boletim de Alojamento" to be used by hotels that submit registration information.

Hotel Collection – The general data protection law applies to hotel collection of personal data for security service use under Decree 23/2007. Hoteliers must inform the SEF, through a specific form, of the whereabouts and personal data regarding guests. Forms must include: given and family name, nationality, data and place of birth, identification document (type, number and country of origin), residence, and date of entry/exit. Portuguese law does not address photocopying of identity documents. In practice, many hotels photocopy these documents. Under Portaria no. 23/2007, registration information must be retained by the hotel for one year.

Hotels and others providing accommodation must forward guest registration information to the Borders and Foreigners Services using SIBA.[37] Most hotels' PMS provides an interface for the electronic transmission of hotel registration data. In the alternative, hotels may upload the text or spreadsheet file to the SEF. Hotels lacking sufficiently capable PMS may upload a file based on the SEF's template.

According to Decree 67/980, data subjects have the right to information, access and objection. Of note: Portuguese Department of Tourism (DOT) and the SEF, signed a partnership that will allow DOT access, starting December 2008, to more than five million registers owned by the SEF regarding accommodation of foreign tourists in hotels.

Security Agency Use – It is the understanding of the DHS Privacy Office that the SEF uses hotel registration personal data for control of foreign citizens' travel within Portugal. Data collected must be kept "no longer than is necessary" for the purpose it was collected or subsequently processed under Decree 67/98. Police have no direct responsibility to inform data subjects that their hotel registration is used for law enforcement or security purposes. Data subjects have the right to access and redress. Transfer of hotel guest registration data within EU is allowed; however, transfer to non-EU countries must be evaluated by the DPA.

[36] Serviço de Estrangeiros e Fronteiras.

[37] It is our understanding that the Portuguese Data Protection Commission has issued an opinion on the requirements of Portaria 415/2008, finding them secure.

H. Spain

The Spanish Data Protection Law (LOPD), enacted in 1999, conforms Spanish data protection law to the EU data protection directive. There are several laws specific to hotel registration personal data collection: Decree 1513/1959, August 18 (Registry for Lodging Establishments); Order Int 1922/2003, July 4 (Registers and Records of Travelers Lodging in Hotels); and the Resolution of July 13, 2003.

Hotel Collection - Article 12 of the LOPD on the protection of public safety and Decree 1513/1959 of 18 August requires hotels to collect and share guest registration information with the police. Under LOPD, guest registration data at a minimum includes an ID card or passport number and expiration date, name, family name, sex, date of birth, nationality, and check-in date.

Hotels are not required to inform data subjects about the transfer of their data to the police, which as a matter of law takes place within 24 hours after check-in. This information is retained by the hotel for three years. Hotels may transmit the hotel registration information in one of four ways: by providing two copies of the registry sheet directly to the police; by faxing the information to the police; by transmitting the information to the police electronically (presumably through PMS);[38] and/or by transmitting the information via the internet to the data processing center of the General Directorate of the Police or the General Directorate of the Civil Guard, as appropriate.

The LOPD specifies that personal data shall be erased by the hotel when no longer necessary or relevant for the purpose for which it was collected. Sharing with third parties is allowed "only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject," with exceptions.

Security Agency Use – Police may use the data for public security purposes only, and the principles of data quality and data subjects' rights "must be respected." According to the LOPD, personal data stored for police purposes must be deleted when the police determine it is no longer necessary for the investigations and the purposes for which it was stored. The DPA has the authority to "inspect" a public agency's use of such data and intervene on behalf of a data subject. Police may share this data with other public entities when a law permits sharing this data, as long as it is consistent with the data collection purpose.

VIII. Oversight of Security Service Use of Hotel Guest Registration Data

A. European Union

A great deal has been written in the EU about the recent US requirement for security service use of commercially-collected PNR, the High Level Contact Group and the future of US-EU exchanges of personal data for security service use. The Privacy Office has found no written discussion, however, of the European practice of security service use of hotel guest registration

[38] The technical specifications for delivery of data are set forth in Appendix C of Resolution of July 13, 2003.

data. This is curious, given the lack of clarity in Article 45 of the Schengen Implementing Convention.

The plain language of Article 45 seems to require the full name of an "alien," whether from another EU Member State or from outside of the EU, and the alien's "valid identity document," presumably including the document number. Personal data from spouses, minor children, and others within a travel group are seemingly exempt. Our review of eight EU Member States found that the following additional pieces of information are being collected by hotels for security services, pursuant to national laws: date and place of birth; date of arrival and departure; identification document expiration date; home address; gender; marital status; profession; and the guest's signature. These countries also appear to differ with regard to the ages below which hotel guests traveling with their parents or guardians are considered minors.

Additionally, the DHS Privacy Office notes that Article 45 specifies "registration forms," which are either kept for the authorities or forwarded to the authorities. Article 45 is silent as to the medium used for these forms. Thus, a plain reading of the phrase "registration form" suggests that Article 45 authorizes the electronic collection of hotel registration personal data, as well as electronic transmission of that data to the authorities.[39]

B. Selected EU Member States

Each of the eight countries that responded to DHS Privacy Office inquiries had oversight regimes in place, whether exclusively within an independent data protection authority, or segmented among different officers and offices. This is a requirement of membership in the EU. Through the European Commission, the DHS Privacy Office report was able to obtain DPA audits of nine countries' data protection authorities, including five of the eight countries on which the DHS Privacy Office has focused: Austria; Belgium; Italy; Netherlands; and Spain.[40] The audits are summarized as follows.

1. Austria

In 2006, the DPA acted on a complaint that a hotel chain in Vienna had collected certain personal data, including the person's credit card number, and then transferred the information to the US.[41] The hotel had taken the hotel registration form prescribed under the Austrian Registration Act of 1991 and modified it to allow guests to opt out of transferring data for certain purposes, rather than requiring them to opt in to the data transfer. The DPA revised the form, bringing it into compliance and obviating the need for a formal recommendation.

[39] The Privacy Office notes the ECJ's recent decision in Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*. To the extent that a Member State does not require collection of its citizens' hotel registration personal data, but does require collection of other Member State's citizens' hotel registration personal data, *Huber* may be implicated. It would appear, however, that under such a reading, assuming it is correct, collection of American citizens' hotel registration personal data would be allowed to continue unimpeded.

[40] The other countries are: Estonia, Latvia, Luxembourg and Slovakia.

[41] Ombudsmanverfahren GZ 211,632.

2. Belgium

In September 2007, the DPA sent out guidance to the various Belgian hotel industry associations requesting that they make hotel managers aware of their obligations under Article 9 of the Belgian Privacy Protection law, "Rights of the Data Subject." One of the associations, HORECA, issued four-language laminated cards on hotel guests' data protection rights for distribution to its member hotels.

3. Italy

The DHS Privacy Office is aware of four documents that the Italian DPA has issued on hotel registration. In 2008, the DPA issued an opinion on the Regina Hotel Baglioni, part of the Baglioni hotels S.p.A chain, and its use of hotel guest personal data to "spy" on hotel guests' tastes.[42]

In 2006, the DPA issued an opinion on the Jolly hotel chain's use of personal data without proper consent from its guests.[43] The DPA forbade the hotel's use of the improperly collected personal data and required the hotel to redraft its information and consent notices to provide guests greater understanding of how the information was used.

In 2005, the DPA issued an opinion on a draft ministerial decree regarding the transfer of hotel guest registration data to Italian law enforcement.[44] The Italian DPA had some concerns about the "excessive" nature of the data collected, and about inconsistencies between the Italian law and Schengen, aspects regarding the electronic transmission to security services and retention.

In 2004, the DPA issued an opinion on l'Hotel Quirinale di Roma.[45] An individual lodged a complaint against the hotel for having failed to respond to the individual's request for PII about him in the hotel's possession. The DPA found the complaint unfounded.

4. The Netherlands

In December 2007, the Dutch DPA wrote to the Dutch hotel industry association to remind hotels of their data protection obligations. Of particular concern was the practice of photocopying or scanning passports. The Dutch DPA advised that this was not permissible under Dutch law.

---

[42] *Privacy in albergo: vietato "spiare" i gusti dei clienti* (January 31, 2008) [1490553].
[43] *Profilazione della clientela di alberghi* (March 9, 2006) [1252220].
[44] *'Schede d'albergo' e modalità di comunicazione all'autorità di pubblica sicurezza. Il parere del Garante* (June 1, 2005) [1138725]. The draft decree is not yet final.
[45] *Titolare, responsabile, incaricato - Trattamento di dati da parte di un albergo* – (June 10, 2004) [1041002].

5. Spain

In June 2004, the Spanish DPA issued *Plan de Inspección de Oficio a Cadenas Hoteleras: Conclusiones y Recomendaciones*,[46] which considered the handling of personal data by hotel chains under the LOPD. Although comprehensive in its coverage of the commercial collection and use of personal data, this document did not address security service collection and use of personal data.

C. Excessive Data Collection?

With the exception of Italy, none of the audits and, indeed, no country's DPA, has addressed the security service aspects of the collection and use of hotel registration personal data. The Dutch DPA's 2007 letter to the hotel industry association is striking. Some Dutch hotels were photocopying or scanning guest passports at the request of the Dutch police, in contravention of Dutch data protection law. While the DPA warned the hotels of the illegality of this practice, the DHS Privacy Office is unaware of any similar communication from the Dutch DPA to the Dutch Police, the Dutch Interior Ministry, or the Dutch Justice Ministry regarding this practice.

The DHS Privacy Office also spoke with representatives of US hotel chains operating in Europe. Several indicated reluctance to speak to officials of the US Government about possible violations of data protection laws. Doubtless, these US companies were worried about disparate treatment within the EU because of their non-European status, should European security services or European agencies become aware of their having raised data protection issues with the US Government. Based on these conversations, the DHS Privacy Office is concerned that the practice of scanning passport photos may extend to countries beyond the Netherlands, and that there are other activities related to hotel guest registration data that have not been revealed in the information provided to us. This is of heightened concern to the DHS Privacy Office in light of the trend in electronically transmitting hotel guest registration data directly to security services. The Privacy Office believes that further effort is necessary to provide a complete picture of the effectiveness of EU data protection laws with respect to security service collection of personal data.

IX. Recommendations

Based on its review of procedures and privacy issues surrounding the mandatory collection of hotel guest registration data in the EU, the DHS Privacy Office offers the following recommendations for the Department and for the American travelling public. It is our hope that these recommendations may be useful to other agencies that are engaged in discussions on trans-Atlantic exchanges of personal information.

1. The DHS Privacy Office and the Department should continue to collaborate with interagency partners to ensure consistency in engaging on privacy issues that relate to the trans-Atlantic sharing of commercially-collected personal data for security service use. To that end, there should be greatly increased understanding across the Executive Branch of the transparency and oversight mechanisms that apply to European security agencies.

[46] Position Inspection Plan to Hotel Chains: Conclusions and Recommendations.

The DHS Privacy Office should continue to help improve understanding of European data protection structures.

2. Americans have an obligation to understand and to assert their rights when travelling to Europe. Americans should become more informed on EU data protection laws and practices. They should ask to see notices and demand clarity whenever a business or government official requests personal data from them. Americans should submit complaints to the appropriate DPA, the Article 29 Working Party, or the European Data Protection Supervisor.[47]

3. The DHS Privacy Office should complete its review of the various European countries' (EU and non-EU, Schengen and non-Schengen) handling of hotel guest registration data and update this report.

X. Conclusion

The DHS Privacy Office intends to continue its research to further a full understanding of the different EU and Member States approaches to security, immigration and border control and privacy and data protection. This research will benefit both security and privacy.

The first step is gaining the necessary facts to understand the EU's approach to security and data protection. Transparency of laws and processes is critical to this fact-finding. Sadly, the difficulties that the DHS Privacy Office faced in its efforts to better understand how Europe approaches data protection in the context of security service use of commercially-collected personal data suggests that there is plenty of work to be done on the European side as well.

All trends indicate there will be even more, not fewer, transatlantic exchanges of data in the future. Due in part to the growth of the Internet, the ever-increasing speed and ease of storage and transmission of data, and increased collection by private entities, those data exchanges are ever more likely to involve commercially-collected data. The stakes are too great for the US and the EU, and for the essential values of privacy and security, not to go forward in finding agreement on a proper and consistent approach to sharing information.

[47] As an aid to Americans travelers, we have included the names and addresses of various European data protection authorities in Appendix 4.

Appendix 1 – Sample letter from DHS Privacy Office to European Data Protection Authority or Ministry of Interior/Justice

[Begin Text]

I am writing to you to seek your assistance to better understand the [country] approach to third-party, commercial collection of personally identifiable information for law enforcement use. Of particular and immediate interest is the dual use of hotel guest registration information.

As you know, Article 45 of the Schengen Convention requires Schengen Member States to adopt measures in order to ensure that hotels collect personal information from guests upon registration and that they retain or forward the information to police for law enforcement and other purposes. For [country], I am interested in domestic legislation apart from applicable EU directives that could shed some light on this example of private – public data sharing.

Previously, I have written separately to the European Data Protection Supervisor, the Article 29 Working Party, and [others], seeking information and views from their perspectives. I seek from you now the [agency's] perspective in this regard and am interested in your interpretation of domestic legislation apart from applicable EU directives that could shed some light on this example of private – public data sharing. My questions are:

Hotel Collection of Personal Data

- Do hotels in [country] collect personal data from guests to provide to [country] security agencies?
  - If yes, is this a requirement under federal or state law? Which law or laws govern this collection?
  - If yes, is such information routinely transferred or made available upon request by the security agency?
  - If done routinely, how often do these transfers occur?
  - If yes, are hotels required to notify guests of routine or case-specific transfers?
- What personal data is collected?
- Is the passport scanned or passport number collected? Are photocopies or images of passports collected?
- How long must the hotel retain the personal data?
- For this collection, what means of access and redress do individuals have?
- In what form is the personal data provided to the police or a security agency (i.e., hardcopy or electronic)?
- If in hardcopy format, are there any pilot programs or plans in [country] for electronic transmission of hotel registration data to police or security agencies?
- What is the competence of the Data Protection Commissioner with respect to hotel collection of registration personal data?
- Must hotels inform the Data Protection Commissioner when transfers are made to security agencies?

Security Agency Collection of Hotel Registration Personal Data

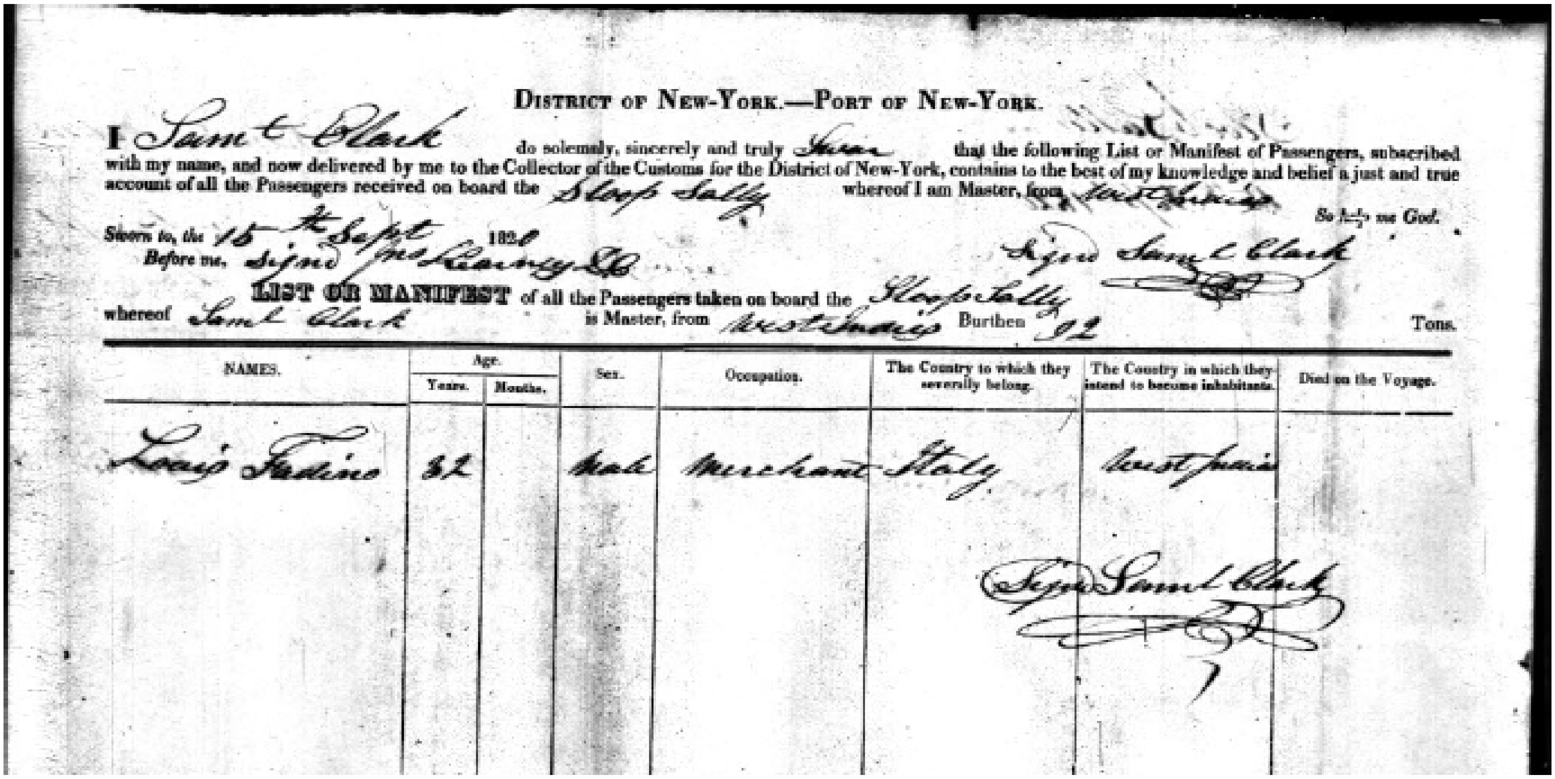
- What use or uses do the police or security agencies make with hotel registration personal data?
- How long is it retained?
- Are security agencies required to notify individuals that their hotel registration is being used for a law enforcement or security purpose?
- What means of redress do individuals have via the police or the security agency?
- Do the police or security agencies in [country] share the personal data with other [country] government agencies, such as the intelligence service? Others?
- Do the police or security agencies in [country] share the personal data with third party countries? If so, which?
- Does the Data Protection Commissioner have competence with respect to oversight of the security agency's use of the personal data? Are there any limits to the Data Protection Commissioner's competence over the police, security, or intelligence agency use of the personal data?
- What other oversight bodies are there in [country] that may have competence to oversee the police, security, or intelligence agency use of this personal data?

Your clarification of these questions will help me better understand the [country] practice of information sharing between the private and public sectors. Please let me know if there is a point of contact to whom I can address follow-up questions.

Warmest regards,

Hugo Teufel III
Chief Privacy Officer

Appendix 2 – Sample 1819 Steerage Act Compliant Sea Line Manifest



DISTRICT OF NEW-YORK.—PORT OF NEW-YORK.

I Saml Clark do solemnly, sincerely and truly Swear that the following List or Manifest of Passengers, subscribed with my name, and now delivered by me to the Collector of the Customs for the District of New-York, contains to the best of my knowledge and belief a just and true account of all the Passengers received on board the Sloop Sally whereof I am Master, from West Indies

So help me God.

Sworn to, the 15th Sept 1820
Before me, Signd Jns Kearney DC

Signd Saml Clark

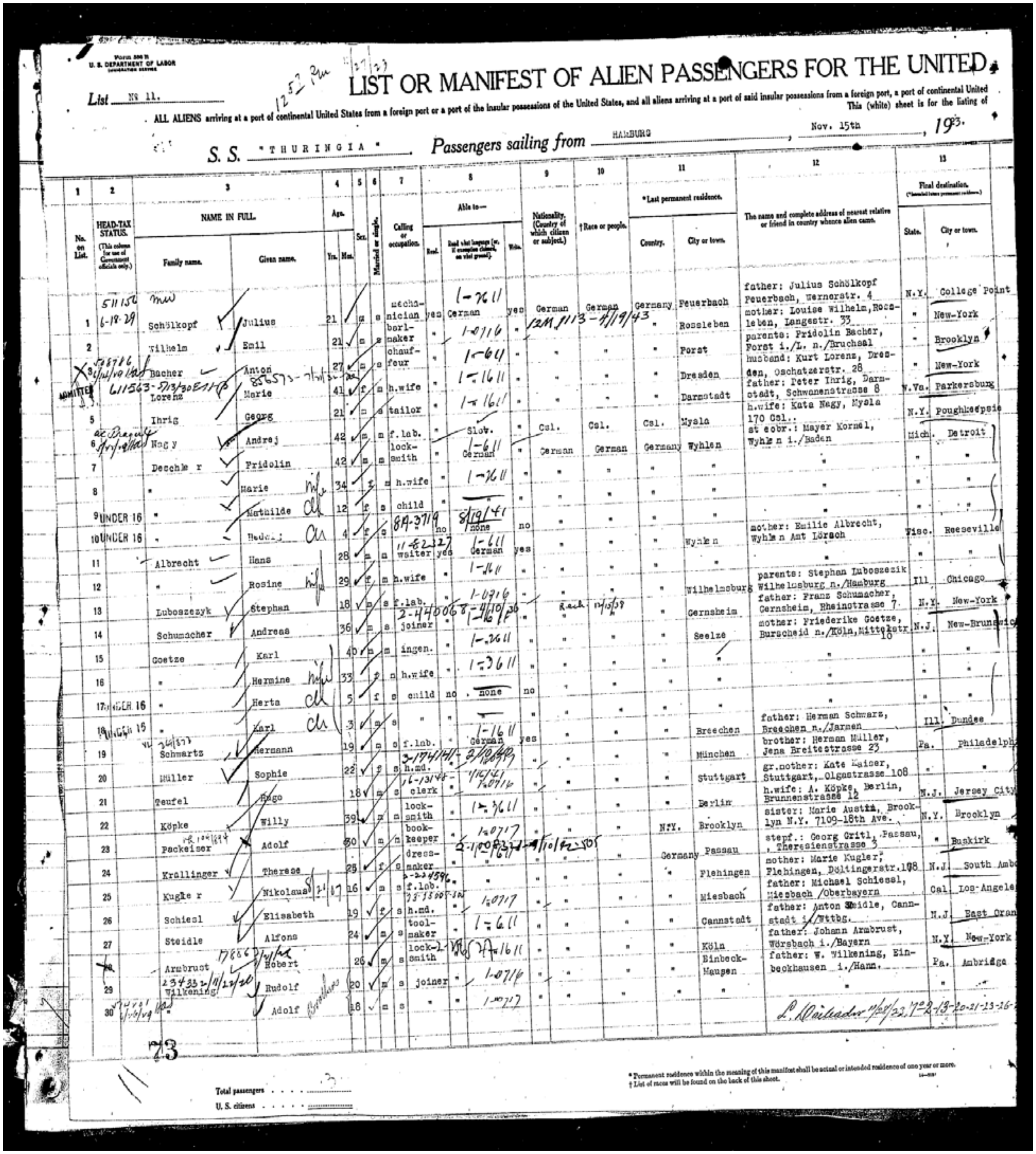
LIST OR MANIFEST of all the Passengers taken on board the Sloop Sally whereof Saml Clark is Master, from West Indies Burthen 92 Tons.

NAMES.	Age. Years.	Age. Months.	Sex.	Occupation.	The Country to which they severally belong.	The Country in which they intend to become inhabitants.	Died on the Voyage.
Louis Fadino	32		Male	Merchant	Italy	West Indies	

Signd Saml Clark

Passenger Manifest for the Sloop Sally, arrived New York Sept 15, 1820

Appendix 3 – Example of a Manifest List from 1923



Form 500 B
U. S. DEPARTMENT OF LABOR
IMMIGRATION SERVICE

List No 11.

LIST OR MANIFEST OF ALIEN PASSENGERS FOR THE UNITED

ALL ALIENS arriving at a port of continental United States from a foreign port or a port of the insular possessions of the United States, and all aliens arriving at a port of said insular possessions from a foreign port, a port of continental United ... This (white) sheet is for the listing of

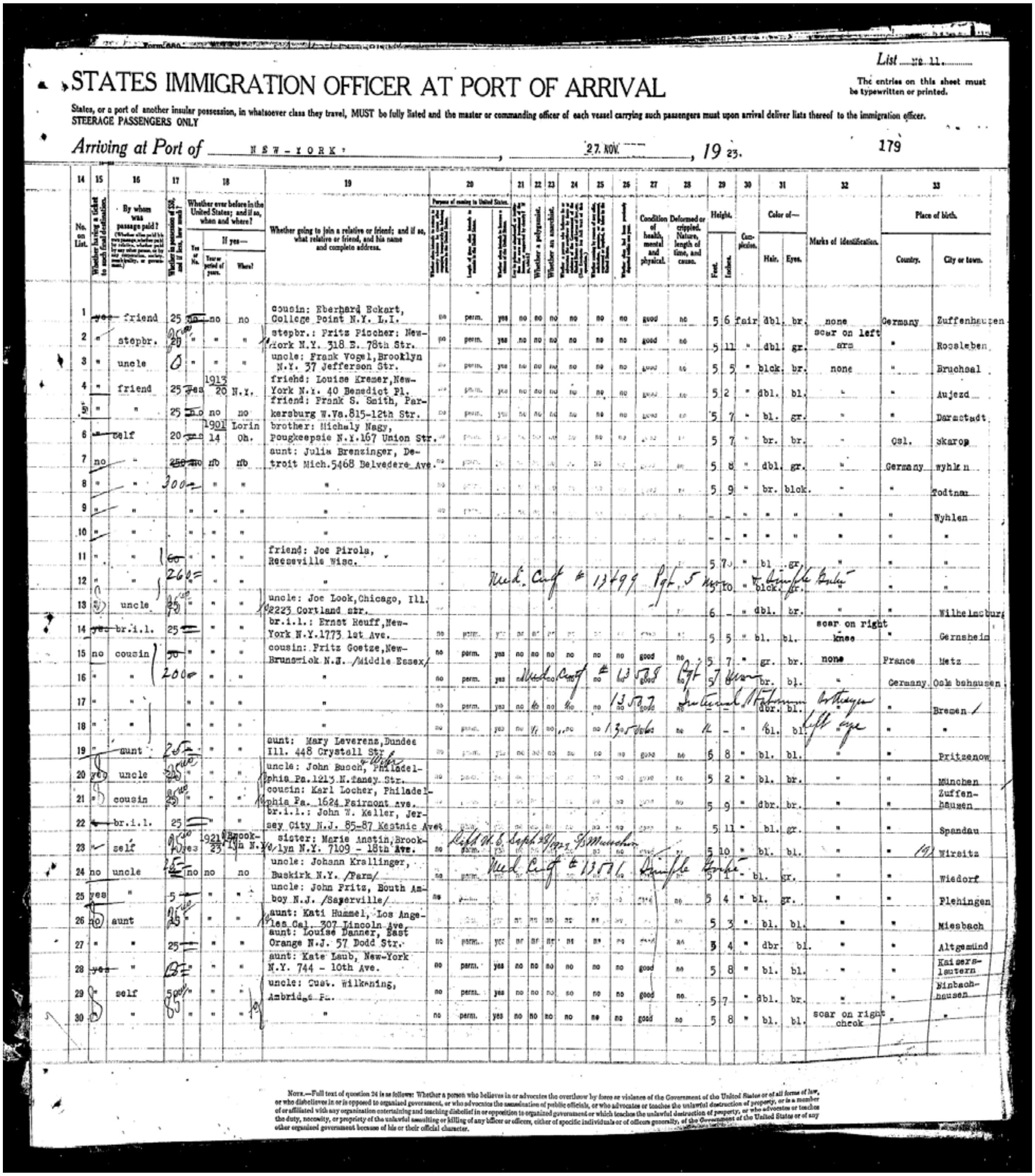
S. S. "THURINGIA", Passengers sailing from HAMBURG, Nov. 15th, 1923.

1 No. on List	2 Head-tax status (This column for use of Government officials only.)	3 Name in full: Family name	Given name	4 Age: Yrs.	5 Sex	6 Married or single	7 Calling or occupation	8 Able to— Read	Read what language	Write	9 Nationality (Country of which citizen or subject)	10 †Race or people	11 *Last permanent residence: Country	City or town	12 The name and complete address of nearest relative or friend in country whence alien came	13 Final destination: State	City or town
1		Schölkopf	Julius	21	m	s	mechanician	yes	German	yes	German	German	Germany	Feuerbach	father: Julius Schölkopf Feuerbach, Wernerstr. 4	N.Y.	College Point
2		Wilhelm	Emil	21	m	s	boilermaker	"		"			"	Rossleben	mother: Louise Wilhelm, Rossleben, Langestr. 33	"	New-York
3		Bacher	Anton	27	m	s	chauffeur	"		"	"	"	"	Forst	parents: Fridolin Bacher, Forst i./L. n./Bruchsal	"	Brooklyn
4		Lorenz	Marie	41	f	m	h.wife	"		"	"	"	"	Dresden	husband: Kurt Lorenz, Dresden, Oschatzerstr. 28	"	New-York
5		Ihrig	Georg	21	m	s	tailor	"		"	"	"	"	Darmstadt	father: Peter Ihrig, Darmstadt, Schwanenstrasse 8	W.Va.	Parkersburg
6		Nagy	Andrej	42	m	m	f.lab.	"	Slov.	"	Csl.	Csl.	Csl.	Mysla	h.wife: Kata Nagy, Mysla 170 Csl.	N.Y.	Poughkeepsie
7		Dechler	Fridolin	42	m	m	locksmith	"	German	"	German	German	Germany	Wyhlen	st eobr.: Mayer Kornel, Wyhlen i./Baden	Mich.	Detroit
8		"	Marie	34	f	m	h.wife	"		"	"	"	"	"	"	"	"
9	UNDER 16	"	Mathilde	12	f	s	child	"		"	"	"	"	"	"	"	"
10	UNDER 16	"	Hedwig	4	f	s		no	none	no	"	"	"	"	"	"	"
11		Albrecht	Hans	28	m	m	waiter	yes	German	yes	"	"	"	Wyhlen	mother: Emilie Albrecht, Wyhlen Amt Lörach	Wisc.	Reeseville
12		"	Rosine	29	f	m	h.wife	"		"	"	"	"	"	"	"	"
13		Luboszczyk	Stephan	18	m	s	f.lab.	"		"	"	"	"	Wilhelmsburg	parents: Stephan Luboszczik Wilhelmsburg n./Hamburg	Ill	Chicago
14		Schumacher	Andreas	36	m	s	joiner	"		"	"	"	"	Gernsheim	father: Franz Schumacher, Gernsheim, Rheinstrasse 7	N.Y.	New-York
15		Goetze	Karl	40	m	m	ingen.	"		"	"	"	"	Seelze	mother: Friederike Goetze, Burscheid n./Köln, Mittelstr. 10	N.J.	New-Brunswick
16		"	Hermine	33	f	m	h.wife	"		"	"	"	"	"	"	"	"
17	UNDER 16	"	Herta	5	f	s	child	no	none	no	"	"	"	"	"	"	"
18	UNDER 16	"	Karl	3	m	s	"	"		"	"	"	"	"	"	"	"
19		Schwartz	Hermann	19	m	s	f.lab.	"	German	yes	"	"	"	Breechen	father: Herman Schwarz, Breechen n./Jarmen	Ill.	Dundee
20		Müller	Sophie	22	f	s	h.md.	"		"	"	"	"	München	brother: Herman Müller, Jena Breitestrasse 23	Pa.	Philadelphia
21		Teufel	Hugo	18	m	s	clerk	"		"	"	"	"	Stuttgart	gr.mother: Kate Kaiser, Stuttgart, Olgastrasse 108	"	"
22		Köpke	Willy	39	m	m	locksmith	"		"	"	"	"	Berlin	h.wife: A. Köpke, Berlin, Brunnenstrasse 12	N.J.	Jersey City
23		Packeiser	Adolf	30	m	m	bookkeeper	"		"	"	"	N.Y.	Brooklyn	sister: Marie Austin, Brooklyn N.Y. 7109-18th Ave.	N.Y.	Brooklyn
24		Krallinger	Therese	25	f	s	dressmaker	"		"	"	"	Germany	Passau	stepf.: Georg Gritl, Passau, Theresienstrasse 3	"	Buskirk
25		Kugler	Nikolaus	16	m	s	f.lab.	"		"	"	"	"	Flehingen	mother: Marie Kugler, Flehingen, Döltingerstr. 108	N.J.	South Amboy
26		Schiesl	Elisabeth	19	f	s	h.md.	"		"	"	"	"	Miesbach	father: Michael Schiessl, Miesbach /Oberbayern	Cal	Los-Angeles
27		Steidle	Alfons	24	m	s	toolmaker	"		"	"	"	"	Cannstadt	father: Anton Steidle, Cannstadt i./Wttbg.	N.J.	East Orange
28		Armbrust	Robert	26	m	s	locksmith	"		"	"	"	"	Köln	father: Johann Armbrust, Wörsbach i./Bayern	N.Y.	New-York
29		Wilkening	Rudolf	20	m	s	joiner	"		"	"	"	"	Einbeck-Hausen	father: W. Wilkening, Einbeckhausen i./Hann.	Pa.	Ambridge
30		"	Adolf	18	m	s	"	"		"	"	"	"	"	"	"	"

Total passengers . . . . .
U. S. citizens . . . . . .

* Permanent residence within the meaning of this manifest shall be actual or intended residence of one year or more.
† List of races will be found on the back of this sheet.

Passenger Manifest for the SS Thuringia, arrived New York, November 27, 1923.



List ... 11
STATES IMMIGRATION OFFICER AT PORT OF ARRIVAL
The entries on this sheet must be typewritten or printed.
States, or a port of another insular possession, in whatsoever class they travel, MUST be fully listed and the master or commanding officer of each vessel carrying such passengers must upon arrival deliver lists thereof to the immigration officer.
STEERAGE PASSENGERS ONLY
Arriving at Port of NEW-YORK, 27. NOV. 1923.
179

No. on List	15	16 By whom was passage paid?	17	18 Yes or No	Year	Where	19 Whether going to join a relative or friend; and if so, what relative or friend, and his name and complete address	Feet	Inches	Complexion	Hair	Eyes	Marks of identification	Country	City or town
1	yes	friend	25	no	no	no	cousin: Eberhard Eckart, College Point N.Y. L.I.	5	6	fair	dbl.	br.	none	Germany	Zuffenhausen
2	"	stepbr.	20	"	"	"	stepbr.: Fritz Fischer: New-York N.Y. 318 E. 78th Str.	5	11	"	dbl.	gr.	scar on left arm	"	Rossleben
3	"	uncle	0	"	"	"	uncle: Frank Vogel, Brooklyn N.Y. 37 Jefferson Str.	5	5	"	blck.	br.	none	"	Bruchsal
4	"	friend	25	yes	1913 20	N.Y.	friend: Louise Kremer, New-York N.Y. 40 Benedict Pl.	5	2	"	dbl.	bl.	"	"	Aujezd
5	"	"	25	no	no	no	friend: Frank S. Smith, Parkersburg W.Va. 815-12th Str.	5	7	"	bl.	gr.	"	"	Darmstadt
6	"	self	20	yes	1901 14	Lorin Oh.	brother: Michaly Nagy, Pougkeepsie N.Y. 167 Union Str.	5	7	"	br.	br.	"	Osl.	Skarop
7	no	"	250	no	no	no	aunt: Julia Brenzinger, Detroit Mich. 5468 Belvedere Ave.	5	8	"	dbl.	gr.	"	Germany	Wyhlen
8	"	"	300	"	"	"	"	5	9	"	br.	blck.	"	"	Todtnau
9	"	"		"	"	"	"	–	–	"	"	"	"	"	Wyhlen
10	"	"		"	"	"	"	–	–	"	"	"	"	"	"
11	"	"	60	"	"	"	friend: Joe Pirola, Reeseville Wisc.	5	7	"	bl.	gr.	"	"	"
12	"	"	260	"	"	"	"	5	10	"	blck.	gr.	"	"	"
13		uncle	25	"	"	"	uncle: Joe Look, Chicago, Ill. 2223 Cortland str.	6	–	"	dbl.	br.	"	"	Wilhelmsburg
14	yes	br.i.l.	25	"	"	"	br.i.l.: Ernst Reuff, New-York N.Y. 1773 1st Ave.	5	5	"	bl.	bl.	scar on right knee	"	Gernsheim
15	no	cousin	50	"	"	"	cousin: Fritz Goetze, New-Brunswick N.J. /Middle Essex/	5	7	"	gr.	br.	none	France	Metz
16	"	"	200	"	"	"	"	5	8	"	br.	bl.	"	Germany	Oelsbehausen
17	"	"		"	"	"	"	–	–	"	dbr.	bl.	"	"	Bremen
18	"	"		"	"	"	"	–	–	"	bl.	bl.	"	"	"
19	"	aunt	25	"	"	"	aunt: Mary Leverenz, Dundee Ill. 448 Crystall Str	5	8	"	bl.	bl.	"	"	Pritzenow
20	yes	uncle	25	"	"	"	uncle: John Busch, Philadelphia Pa. 1213 N. fancy Str.	5	2	"	bl.	br.	"	"	München
21	"	cousin	25	"	"	"	cousin: Karl Locher, Philadelphia Pa. 1624 Fairmont ave.	5	9	"	dbr.	br.	"	"	Zuffenhausen
22	"	br.i.l.	25	"	"	"	br.i.l.: John W. Keller, Jersey City N.J. 85-87 Kestnic Ave.	5	11	"	bl.	gr.	"	"	Spandau
23	"	self	40	yes	1921 23	Brooklyn N.Y.	sister: Marie Anstin, Brooklyn N.Y. 7109 - 18th Ave.	5	10	"	bl.	bl.	"	"	Wirsitz
24	no	uncle	25	no	no	no	uncle: Johann Krallinger, Buskirk N.Y. /Farm/	5	1	"	bl.	gr.	"	"	Wiedorf
25	yes	"	5	"	"	"	uncle: John Fritz, South Amboy N.J. /Sayerville/	5	4	"	bl.	gr.	"	"	Plehingen
26	no	aunt	25	"	"	"	aunt: Kati Hummel, Los Angeles Cal. 307 Lincoln Ave.	5	3	"	bl.	bl.	"	"	Miesbach
27	"	"	25	"	"	"	aunt: Louise Danner, East Orange N.J. 57 Dodd Str.	5	4	"	dbr.	bl.	"	"	Altgemünd
28	yes	"	15	"	"	"	aunt: Kate Laub, New-York N.Y. 744 - 10th Ave.	5	8	"	bl.	bl.	"	"	Kaiserslautern
29	"	self	50	"	"	"	uncle: Gust. Wilkening, Ambridge Pa.	5	7	"	dbl.	br.	"	"	Einbachhausen
30		"	85	"	"	"	"	5	8	"	bl.	bl.	scar on right cheek	"	"

Note.—Full text of question 24 is as follows: Whether a person who believes in or advocates the overthrow by force or violence of the Government of the United States or of all forms of law, or who disbelieves in or is opposed to organized government, or who advocates the assassination of public officials, or who advocates or teaches the unlawful destruction of property, or is a member of or affiliated with any organization entertaining and teaching disbelief in or opposition to organized government or which teaches the unlawful destruction of property, or who advocates or teaches the duty, necessity, or propriety of the unlawful assaulting or killing of any officer or officers, either of specific individuals or of officers generally, of the Government of the United States or of any other organized government because of his or their official character.

Passenger Manifest for the SS Thuringia, arrived New York, November 27, 1923 (cont.).

Appendix 4 – Contact Information for Selected European Data Protection Authorities

For further information about the collection of hotel guest registration data, Americans may contact the following European Data Protection Authorities (DPA):

EU Countries

Austria
Österreichische Datenschutzkommission
Ballhausplatz, 1
A - 1014 WIEN
Tel. +43 1 531 15 25 25
Fax +43 1 531 15 26 90
e-mail: dsk@dsk.gv.at
website: http://www.dsk.gv.at/indexe.htm

Belgium
Commission de la protection de la vie privée
Rue Haute, 139
B - 1000 BRUXELLES
Tel. +32 2 213 8540
Fax +32 2 213 8545
e-mail: commission@privacy.fgov.be
website: http://www.privacycommission.be/fr (in French)

Bulgaria
Commission for Personal data Protection
Mr. Ivo STEFANOV
1 Dondikov Blvd.
Sofia 1000
Tel. +3592 940 2046
Fax +3592 940 3640
e-mail: kzld@govenment.bg
website: http://www.cpdp.bg/en_index.html

Cyprus
Commissioner for Personal data Protection
Ms. Goulla Frangou
40, Th. Dervis Street
CY - 1066 Nicosia
Tel. +357 22 818 456
Fax +357 22 304 565
e-mail: commissioner@dataprotection.gov.cy
website:
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument

Czech Republic
Mr. Igor Němec
The Office for Personal data Protection
Urad pro ochranu osobnich udaju
Pplk. Sochora 27
CZ - 170 00 Prague 7
Tel. +420 234 665 111
Fax +420 234 665 444
e-mail: posta@uoou.cz
website:
http://www.uoou.cz/index.php?l=en&m=bottom&mid=01&u1=&u2=&t=

Denmark
Datatilsynet
Borgergade 28, 5
DK - 1300 Copenhagen K
Tel. +45 33 19.32.00
Fax +45 33 19.32.18
e-mail: dt@datatilsynet.dk
website: http://www.datatilsynet.dk/english/

Estonia
Estonian Data Protection Inspectorate
Director General
Mr. Urmas Kukk
Väike-Ameerika 19
10129 Tallinn
Tel. +372 6274 135
Fax +372 6274 135
e-mail: urmas.kukk@dp.gov.ee

Finland
Office of the Data Protection
Ombudsman
P.O. Box 315
FIN-00181 Helsinki
Tel. +358 10 3666 700
Fax +358 10 3666 735
e-mail: tietosuoja@om.fi
website: http://www.tietosuoja.fi/1560.htm

France
Commission Nationale de l'Informatique et des Libertés
8, rue Vivienne, CS 30223
F-75002 Paris, CEDEX 02
Tel. +33 (0) 1 53 73 22 22
Fax +33 (0) 1 53 73 22 00
website: http://www.cnil.fr/index.php?id=4

Germany
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30
53117 Bonn
Tel. +49 (0) 228 997799 0 or +49 (0) 228 81995 0
Fax +49 (0) 228 997799 550 or +49 (0) 228 81995 550
e-mail: poststelle@bfdi.bund.de
website: http://www.bfdi.bund.de/EN/Home/homepage__node.html

Greece
Hellenic Data Protection Authority
Kifisias Av. 1-3, PC 11523
Ampelokipi Athens, Greece
Tel. +30 210 6475 600
Fax +30 210 6475 628
e-mail: kkosm@dpa.gr

Hungary
Data Protection Commissioner of Hungary
Parliamentary Commissioner for Data Protection and Freedom of Information
Dr. Attila Péterfalvi
Nádor u. 22.
H - 1051 Budapest
Tel. +36 1 475 7186
Fax +36 1 269 3541
e-mail: adatved@obh.hu
website: http://abiweb.obh.hu/dpc/

Ireland
Data Protection Commissioner
Canal House
Station Road
Portarlington
Co. Laois
Tel. +353 57 868 4800
Fax +353 57 868 4757
e-mail: info@dataprotection.ie
website: http://www.dataprotection.ie/docs/Home/4.htm

Italy
Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
I - 00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
e-mail: garante@garanteprivacy.it

Latvia
Data State Inspection
Latvia, Riga Director
Ms. Signe Plumina
Kr. Barona Street 5-4
LV - 1050 Riga
Tel. +371 722 3131
Fax +371 722 3556
e-mail: info@dvi.gov.lv
website: http://www.dvi.gov.lv/eng/

Lithuania
State Data Protection
Inspectorate Director
Mr. Algirdas Kunčinas
Žygimantų str. 11-6a
LT - 011042 Vilnius
Tel. + 370 5 279 14 45
Fax +370 5 261 94 94
e-mail: ada@ada.lt
website: http://www.ada.lt/index.php?lng=en

Luxembourg
Commission nationale pour la protection des données
68, rue de Luxembourg
L - 4100 Esch-sur-Alzette
Tel. +352 2610 60 1
Fax +352 2610 60 29
e-mail: info@cnpd.lu
website: http://www.cnpd.lu/en/index.html

Malta
Office of the Data Protection Commissioner
Data Protection Commissioner
Mr. Paul Mifsud Cremona
2, Airways House
High Street, Sliema SLM 16, Malta
Tel. +356 2328 7100
Fax +356 2328 7198
e-mail: commissioner.dataprotection@gov.mt
website: http://www.dataprotection.gov.mt/

The Netherlands
College bescherming persoonsgegevens (CBP)
Dutch Data Protection Authority
Juliana van Stolberglaan 4-10
P.O.Box 93374
NL - 2509 AJ Den Haag/The Hague
Tel. +31 70 888 8500
Fax +31 70 888 8501
e-mail: info@cbpweb.nl
website: http://www.dutchdpa.nl/

Poland
The Bureau of the Inspector General for the Protection of Personal data
Mr. Michał Serzycki
Inspector General for Personal data Protection
ul. Stawki 2
00-193 Warsaw
Tel. +48 22 860 70 81
Fax +48 22 860 70 90
e-mail: sekretariat@giodo.gov.pl
website: http://www.giodo.gov.pl/168/j/en/

Portugal
Comissão Nacional de Protecção de Dados
R. de São. Bento, 148-3°
P - 1200-821 LISBOA
Tel. +351 21 392 84 00
Fax +351 21 397 68 32
e-mail: geral@cnpd.pt
website: http://www.cnpd.pt/english/index_en.htm

Romania
The National Supervisory Authority for Personal data Processing
Ms. Raluca POPA
Str. Olari nr. 32
Sector 2, BUCUREŞTI
Cod poştal 024057
Tel. +40 21 252 5599
Fax +40 21 252 5757
e-mail: anspdcp@dataprotection.ro
website: http://www.dataprotection.ro/

Slovak Republic
Office for Personal data Protection of the SR
Mr. Gyula Veszelei
President
Odborárske námestie č. 3
817 60, Bratislava
Tel. + 421 2 5023 9418
Fax + 421 2 5023 9441
e-mail: statny.dozor@pdp.gov.sk or gyula.veszelei@pdp.gov.sk
website:
http://www.dataprotection.gov.sk/buxusnew/generate_page.php?page_id=93

Slovenia
Information Commissioner
Ms. Natasa Pirc Musar
Vošnjakova 1
SI - 1000 LJUBLJANA
Tel. +386 (0) 1 230 9730
Fax +386 (0) 1 230 9778
e-mail: gp.ip@ip-rs.si
website: http://www.ip-rs.si/?id=195

Spain
Agencia de Protección de Datos
C/Jorge Juan, 6
E - 28001 MADRID
Tel. +34 91399 6200
Fax +34 91455 5699
e-mail: internacional@agpd.es
website: https://www.agpd.es/index.php?idSeccion=8

Sweden
Datainspektionen
Fleminggatan, 14
9th Floor
Box 8114
S - 104 20 STOCKHOLM
Tel. +46 8 657 6100
Fax +46 8 652 8652
e-mail: datainspektionen@datainspektionen.se
website:
http://www.datainspektionen.se/in_english/start.shtml

United Kingdom
Mr. Richard Thomas
Information Commissioner
The Office of the Information Commissioner Executive Department
Water Lane, Wycliffe House
UK - WILMSLOW - CHESHIRE SK9 5AF
Tel. +44 1 625 54 57 00 (switchboard)
e-mail: please use the online enquiry from website
website: https://www.ico.gov.uk/Global/contact_us.aspx

EFTA Countries

Iceland
Icelandic Data Protection Agency
Rauðarárstíg 10
105 Reykjavík, Ísland
Tel. +354 510 9600
Fax +354 510 9606
e-mail: postur@personuvernd.is
website: http://personuvernd.is/information-in-english/

Lichtenstein
Dr. Philipp Mittelberger
Datenschutzbeauftragter des Fürstentums Liechtenstein
Stabsstelle für Datenschutz
Kirchstrass 8, Postfach 684
9490 Vaduz
Tel. +423 236 6091
Fax +423 236 6099
e-mail: info@sds.llv.li
website:
http://www.liechtenstein.li/en/eliechtenstein_main_sites/portal_fuerstentum_liechtenstein/home.htm

Norway
Datatilsynet
The Data Inspectorate
P.O.Box 8177 Dep
N - 0034 OSLO
Tel. +47 22 39 69 00
Fax +47 22 42 23 50
e-mail: postkasse@datatilsynet.no
website: http://www.datatilsynet.no/templates/Page____194.aspx

Switzerland
Data Protection Commissioner of Switzerland
Eidgenössischer Datenbeauftragter
Mr. Hanspeter THÜR
Feldeggweg 1
CH - 3003 Bern
Tel. +41 (0) 31 322 4395
Fax +41 (0) 31 325 9996
e-mail: info@edsb.ch
website: http://www.edoeb.admin.ch/index.html?lang=en

German State Data Protection Offices

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
Baden-Württemberg
Urbanstraße 32
70182 Stuttgart
Postfach 10 29 32
70025 Stuttgart
Tel.: 07 11 - 61 55 41 - 0
Fax: 07 11 - 61 55 41 - 15
http://www.baden-wuerttemberg.datenschutz.de

Berlin
Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4 - 10
10787 Berlin
Tel.: 030 - 1 38 89 - 0
Fax: 030 - 2 15 50 50
http://www.datenschutz-berlin.de

Brandenburg
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77, Haus 2
14532 Kleinmachnow
Tel.: 033 203 - 356 - 0
Fax: 033 203 - 356 - 49
http://www.lda.brandenburg.de

Bremen
Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen
Arndtstraße 1
27570 Bremerhaven
Postfach 10 03 80
27503 Bremerhaven
Tel.: 04 21 - 361 - 2010
Fax: 04 21 - 496 - 18495
http://www.datenschutz-bremen.de

Hamburg
Der Hamburgische Datenschutzbeauftragte
Klosterwall 6 Block C
20095 Hamburg
Tel.: 040 - 428 54 - 4040
Fax: 040 - 428 54 - 4000
http://www.hamburg.de/datenschutz

Hessen
Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Postfach 31 63
65021 Wiesbaden
Tel.: 06 11 - 1408 - 0
Fax: 06 11 - 1408 - 900
http://www.datenschutz.hessen.de

Mecklenburg-Vorpommern
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Johannes-Stelling-Straße 21
19053 Schwerin
Schloß Schwerin
19053 Schwerin
Tel.: 03 85 - 5 94 94 - 0
Fax: 03 85 - 5 94 94 - 58
http://www.lfd.m-v.de

Niedersachsen
Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstraße 9
30169 Hannover
Postfach 221
30002 Hannover
Tel.: 05 11 - 120 - 45 00
Fax: 05 11 - 120 - 45 99
http://www.lfd.niedersachsen.de

Nordrhein-Westfalen
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf
Postfach 20 04 44
40102 Düsseldorf
Tel.: 02 11 - 38 424 - 0
Fax: 02 11 - 38 424 - 10
http://www.ldi.nrw.de

Rheinland-Pfalz
Der Landesbeauftragte für den Datenschutz
Rheinland-Pfalz
Deutschhausplatz 12
55116 Mainz
Postfach 30 40
55020 Mainz
Tel.: 06 131 - 208 2449
Fax: 06 131 - 208 2497
http://www.datenschutz.rlp.de

Saarland
Landesbeauftragter für Datenschutz und
Informationsfreiheit Saarland
Fritz-Dobisch-Straße 12
66111 Saarbrücken
Postfach 10 26 31
66026 Saarbrücken
Tel.: 06 81 - 94 781 - 0
Fax: 06 81 - 94 781 - 29
http://www.lfdi.saarland.de

Sachsen (Freistaat)
Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden
Postfach 12 09 05
01008 Dresden
Tel.: 03 51 - 49 35 - 0
Fax: 03 51 - 49 35 490
http://www.datenschutz.sachsen.de

Sachsen-Anhalt
Landesbeauftragter für den Datenschutz
Sachsen-Anhalt
Berliner Chaussee 9
39114 Magdeburg
Postfach 19 47
39009 Magdeburg
Tel.: 03 91 - 81 803 - 0
Fax: 03 91 - 81 803 - 33
http://www.datenschutz.sachsen-anhalt.de

Schleswig-Holstein
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Holstenstr. 98
24103 Kiel
Postfach 7116
24171 Kiel
Tel.: 04 31 - 988 - 12 00
Fax: 04 31 - 988 - 12 23
http://www.datenschutzzentrum.de

Thüringen
Der Thüringer Landesbeauftragte für den
Datenschutz
Jürgen-Fuchs-Straße 1
99096 Erfurt
Postfach 900455
99107 Erfurt
Tel.: 03 61 - 37 71 9 - 00
Fax: 03 61 - 37 71 9 - 04
http://www.thueringen.de/datenschutz/

Appendix 5 – A History of US Government Use of Commercially-collected Manifest Lists and Passenger Name Record Data

A. Immigration Authorities Requiring Manifest Lists

The US Government mandated passenger reporting requirements for transportation companies for the first time in the 1819 Steerage Act.[48] The Act required the master of every vessel landing passengers from any foreign port to deliver a manifest listing "particularly, the age, sex, and occupation, of the said passengers, respectively, the country to which they severally belong, and that of which they intend to become inhabitants." The law did not require the passengers to be listed by name. This information was collected primarily for statistical purposes, which aided the US Government's understanding of migration patterns. The Secretary of State was responsible for the collection of this information.

Sea lines traditionally collected personal data on passengers, doubtless not only for fare collection purposes, but also for accountability reasons, should something happen to the ship or any passengers while en route. An example of a form intended to comply with the Steerage Act is provided at Appendix 2. Note that the form begins with a blank for "Names."

The US Passenger Act of 1882[49] required ships entering US ports to provide a list of all passengers taken on board the vessel at any foreign port and further required the following information about all passengers:

> [T]he names of the cabin passengers, their age, sex, calling, and the country of which they are citizens, and the number of pieces of baggage belonging to each passenger, and also the name, age, sex, calling, and native country of each emigrant passenger, or passengers other than cabin passengers, and their intended destination or location, and the number of pieces of baggage belong to each passenger, and also the location of the compartment or space occupied by each of such passengers during the voyage…[50]

In 1891, Congress established Federal control over US immigration policy and created the first Federal immigration agency, the Office of the Superintendent of Immigration, within the Treasury Department.[51] Of relevance to this report, Section 8 of the Act began: "That upon the arrival by water at any place within the United States of any alien immigrants it shall be the duty of the commanding officer and the agents of the steam or sailing vessel by which they came to report the name, nationality, last residence, and destination of every such alien, before any of them are landed, to the proper inspection officers . . . ."[52]

---

[48] Act of March 2, 1819, ch. 47, 3 Stat. 489 (1819).
[49] Act of August 2, 1882, ch. 374, § 9, 22 Stat. 186, 189, (1882).
[50] Id. at 190. Congress amended this provision in 1905, limiting the information collected to the name, sex, age (if over eight years of age), marital status, location of compartment or space occupied, whether a citizen of the U.S., and number of bags. *An Act to amend the Act of August 2, 1882, ch. 564,* 33 Stat. 711 (1905).
[51] See Act of March 3, 1891, ch. 551, 26 Stat. 1084 (1891).
[52] Id. at 1085.

In 1903, Congress moved the Bureau of Immigration from the Department of the Treasury to the newly-created Department of Commerce and Labor, and recodified Federal immigration law.[53] Under Sections 12 through 15 of the Act, which address "Manifests of Aliens," the amount of personal data required from non-US citizens traveling to the US increased significantly. Ships arriving at US ports were required to produce passenger lists "at the time and place of embarkation," providing the following information:

> [F]ull name, age, and sex; whether married or single; the calling or occupation; whether able to read or write; the nationality; the race; the last residence; the seaport for landing in the United States; the final designation, if any, beyond the port of landing; whether having a ticket through to such final destination; whether the alien has paid his own passage, or whether it has been paid by any other person or by any corporation, society, municipality, or government, and if so, by whom; whether in possession of fifty dollars, and if less, how much; whether going to join a relative or friend, and if so, what relative or friend and his name and complete address; whether ever before in the United States, and if so, when and where; whether ever in prison or almshouse or an institution or hospital for the care and treatment of the insane or supported by charity; whether a polygamist; whether an anarchist; whether coming by reason of any offer, solicitation, promise, or agreement, expressed or implied, to perform labor in the United States; and what is [sic]the alien's condition of health, mental and physical, and whether deformed or crippled, and if so, for how long and from what cause.[54]

In 1906, Congress established a standard naturalization form, which called for the immigrant's name, date and place of birth, and port and date of arrival.[55] Immigration authorities verified the arrival information by checking the original immigration records, which were typically the ship manifests.

Congress then passed the Immigration Act of 1917,[56] the Nation's first "widely restrictive immigration law,"[57] with immigration restrictions now mainly based on national security concerns. The Act required a literacy test for immigrants over 16 years of age, increased the tax paid by new immigrants, and gave immigration officials greater discretion over whom to exclude. Finally, the Act excluded from entry anyone from the "Asiatic Barred Zone," with the exceptions of Japanese and Filipinos. Section 12 of the 1917 Act added extensively to the list of information required under Section 12 of the 1903 Act.[58] See Appendix 3 for an example of a

---

[53] Act of March 3, ch. 1012, 1903, 32 Stat. 1213 (1903).
[54] Id. at 1216.
[55] Act of June 29, 1906, ch. 3592, 34 Stat 596 (1906).
[56] Act of February 5, 1917, ch. 29, 39 Stat. 874 (1917).
[57] U.S. Department of State, "The Immigration Act of 1924," http://www.state.gov/r/pa/ho/time/id/87718.htm (accessed December 30, 2008)
[58] Data elements added to the list included a personal description (including height, complexion, color of hair and eyes, and marks of identification); country of birth; name and address of the nearest relative in the country from which the alien came; whether [the alien is] a person who (1) believes in or advocates the overthrow by force or violence of the Government of the United States or of all forms of law, (2) disbelieves in or is opposed to organized government, (3) advocates the assassination of public officials, (4) advocates or teaches the unlawful destruction of property, (5) is a member of or affiliated with any organization entertaining and teaching disbelief in opposition to organized government, or which teaches the unlawful destruction of property, or (6) advocates or teaches the duty, necessity, or propriety of the unlawful assaulting or killing of any officer or officers, either of specific individuals or

1923 manifest list form that reflects the extensive information required of non-US citizens seeking entry into the United States.

The Immigration Act of 1924,[59] or Johnson-Reed Act, was intended to further restrict immigration to the United States. It further tightened quota restrictions and made them permanent in the National Origins Quota System,[60] which had first appeared in 1921. The information collection requirements of the 1917 Act remained in effect and were a key means of determining admissibility.

The Bureau of Immigration and Naturalization[61] at the Department of Labor[62] was responsible for promulgating rules under the 1917 and 1924 Acts. In the rules, published on July 1, 1925, the Bureau instructs transportation companies on the proper means of preparing manifests, with different forms for "first cabin, second cabin, and steerage," as well as for immigrants and non-immigrants.[63] The 1917 and 1924 Acts and the Bureau rules focused on manifests from seagoing vessels. Executive Order No. 4049 of July 14, 1924, imposed the same documentary requirements on passengers arriving in the United States on "airships."[64]

The Immigration and Nationality Act (INA) of 1952,[65] also known as the McCarran-Walter Act, repealed and replaced the Immigration Acts of 1917 and 1924. Enacted during the early years of the Cold War, INA was the product of those who believed a link existed between national security and immigration. INA maintained the National Origins Quota System but ended prior immigration laws' Asian exclusions and introduced a system of preferences based on skill sets and family.[66]

Section 231 of INA provided that for any vessel or aircraft arriving by water or by air at any port within the United States from any place outside the United States, the responsible person for that vessel or aircraft must provide a list or manifest of the persons on board the vessel or aircraft at the time of arrival. The statute did not list the specifics of the manifest or list, leaving those details to the Attorney General.[67]

---

of officers generally, of the Government of the United States or of any other organized government because of his or their official character; whether [an alien is] coming with the intent to return to the country whence such alien comes after temporarily engaging in laboring pursuits in the United States; and

" such other items of information as will aid in determining whether any such alien belongs to any of the [classes excluded by the Act]. 39 Stat. at 882-83.

[59] Act of May 26, 1924, ch. 190, 43 Stat. 153 (1924).

[60] Congress abolished the National Origins Quota System in 1965, but maintained numeric restrictions for countries and hemispheres and the preferences based on skill sets and family. See: INS Act of 1965, also known as the Hart-Celler Act (Pub.L. 89-236).

[61] In 1933, the Bureau is renamed the Immigration and Naturalization Service.

[62] The Department of Labor was established in 1913, with the bifurcation of the Department of Commerce and Labor into the Departments of Commerce and Labor.

[63] Rule 2, subdivisions A and B

[64] Section 7(d) of the Air Commerce Act of 1976 authorized the Immigration and Naturalization Service to station officers at airports of entry to collect the required manifests and perform other lawful duties. The Act of May 20, 1926, ch. 344, 44 Stat. 572-73 (1926).

[65] Act of June 27, 1952, ch. 477, 66 Stat. 163 (1952).

[66] U.S. Department of State, "The Immigration and Nationality Act of 1952 (The McCarran-Walter Act)" (accessed on December 30, 2008).

[67] In 1940, President Roosevelt moved the Bureau from the Department of Labor to the Department of Justice.

On March 1, 2003, the Immigration and Naturalization Service (INS) was abolished with the creation of DHS. The former INS' border functions (including the Border Patrol and INS inspectors) were transferred to DHS Customs and Border Protection, which also included inspectors from the former Customs Service.

The requirement for manifest lists found in Section 231 of INA is extant today, in 8 U.S.C. § 1221, which requires the provision of passenger manifests for all commercial vessels or aircraft transporting "any person to any seaport or airport of the United States from any place outside the United States…prior to arrival at that port." Under Section 1221, the following information is required:

1. complete name;
2. date of birth;
3. citizenship;
4. sex;
5. passport number and country of issuance;
6. country of residence;
7. United States visa number, date, and place of issuance, where applicable;
8. alien registration number, where applicable;
9. United States address while in the United States; and
10. such other information the Attorney General, in consultation with the Secretary of State, and the Secretary of Treasury determines as being necessary for the identification of the persons transported and for the enforcement of the immigration laws and to protect safety and national security.[68]

B. Customs Authorities on Passenger Name Registration Data

As early as 1996, the former Department of Treasury US Customs Service (now DHS Customs and Border Protection) used electronic PNR data from air carriers on a voluntary basis. In the aftermath of September 11, 2001, Congress enacted the Aviation Transportation Security Act of 2001 (ATSA), requiring the US Customs Service to collect PNR data from air carriers for purposes of screening individuals traveling to and from the United States.[69] In 2002, the US Customs Service promulgated interim PNR implementing regulations[70] before being transferred in 2003 to DHS.

Under ATSA, as implemented at 19 C.F.R. § 122.49d, air carriers operating passenger flights to or from the United States must provide CBP with access to PNR data that is in their automated reservation/departure control systems. This data is stored in and processed by DHS through the Automated Targeting System (ATS). ATSA was amended by Section 4012 of the Intelligence

[68] Under the Homeland Security Act, 6 U.S.C. § 557, the Attorney General's functions are transferred to the Secretary of Homeland Security.
[69] Aviation and Transportation Security Act of 2001, Public Law 107–71—Nov. 19, 2001 (codified at 49 U.S.C. 44909(c)(3)).
[70] 67 Fed. Reg. 42710 (June 25, 2002).

Reform and Terrorism Prevention Act of 2004, which strengthened DHS' authority for collecting PNR by adding Section 44909(c)(6), stating that the Department should conduct passenger screening before individuals depart on a flight destined for the United States.[71] Further, the Act required the DHS Secretary to issue rules on the comparison of PNR data against the US Government's "consolidated and integrated watchlist." Finally, Section 4012 also mandated redress procedures for the correction of erroneous information.

Anyone traveling on a commercial air carrier into or out of the US has an electronic reservation or "passenger name record." PNR are generally created within air carriers' reservation and/or departure control systems ("reservation systems") to fill seats and collect revenue. There is a wide spectrum of air carrier reservation systems; each air carrier has made changes to their system tailored to their specific needs. As a result, very few of the air carriers' systems are exactly the same or provide CBP with the same information in the same format. [72]

When considering how a private entity (*i.e.*, airline) collects personal information on a traveler, it is interesting to note the lifecycle of PNR (how it is collected and then shared with DHS).

1. Individual traveler or agent makes a reservation with an airline to fly to or from the United States.
2. Information about the traveler and the reservation are loaded into the airline reservation system.
3. DHS/CBP pulls or, if an appropriate push system exists, CBP receives pushed data 72 hours before scheduled flight time and maintains it in ATS.
4. If data is pulled, unformatted PNR with all information is accessed and then filtered for "sensitive" terms and codes. Symbols are put in the location where "sensitive" terms and codes have been removed and original PNR is filtered.
5. PNR is filtered for the approved categories of data stated in the ATS System of Records Notice (SORN). The remaining elements of the PNR are deleted by CBP and are not accessible through the system. Categories outside those in the ATS SORN are deleted and cannot be re-created after 30 days.
6. Individual traveler arrives at the airport to fly to or from the US, the travel document (Passport or Visa) is swiped by the airline and full name and other relevant passport information is transmitted to CBP as Advanced Passenger Information (API). API is maintained in the API section of the Treasury Enforcement System (TECS) Information Technology Platform and PNR is maintained in Automated Targeting System (ATS).
7. At seven years after the end of travel specified in the itinerary of the PNR, the PNR data will be moved to a dormant, non operational status, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.

---

[71] Section 4012 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 118 Stat. 3714, Public Law 108–458 (Dec. 17, 2004).

[72] See DHS Privacy Office, "A *Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union,"* (2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

8. At 15 years from receipt date/time given in the record, PNR will be deleted, with the exception of the PNR related to a specific enforcement action, which will be available for the life of the enforcement record.[73]

C. Oversight on the Use of Manifest Lists and PNR Data

PNR is protected under the Privacy Act of 1974, the E-Government Act, the Freedom of Information Act, and the numerous laws, Executive Orders, court decisions and DHS policies that protect the collection, use, and disclosure of PII. The DHS Privacy Office has led two reviews of the use of PNR data. Pursuant to the PNR agreement with the EU in 2004, the DHS Privacy Office conducted its first review of the PNR program and issued a public report reviewing CBP's policies and practices consistent with the US-EU arrangement. That review resulted in findings of substantial compliance, but included key areas for improvement. The Report was issued in conjunction with the US-EU Joint Review of the Undertakings on EU PNR held September 2005. With the 2007 PNR Agreement, the parties again agreed to conduct periodic, reciprocal reviews.

In advance of the second Joint Review with the EU, originally planned for December 2008, the DHS Privacy Office again conducted an assessment of the Department's and CBP's policies and uses of PNR. The DHS Privacy Office reviewed the requirements of the ATS System of Records Notice (SORN), the 2007 Agreement and relevant letters, and issued its 2008 PNR Report[74] finding that the Department complied with the representations made in the Agreement and letters, as well as those representations made in the SORN for ATS. After initially committing to participate in the joint review, the European Commission unfortunately postponed its participation for unknown reasons.

[73] The PNR data elements, as well as the use, retention, safeguarding, and other protections of this data, are spelled out in the ATS Privacy Impact Assessment (PIA), System of Records Notice (SORN), and the Notice of Proposed Rulemaking (NPRM) for Privacy Act exemptions published on August 6, 2007 in the Federal Register at 72 FR 43650 (SORN) and 72 FR 43567 (NPRM). The API data elements, as well as the use, retention, safeguarding, and other protections of this data are covered by the PIAs published on December 16, 2008; November 18, 2008; September 11, 2007; August 9, 2007; and March 21, 2005. The SORN and Final Rule for Privacy Act exemptions were published in the Federal Register on November 18, 2008 (73 FR 68291). All of these documents are publically available at www.dhs.gov/privacy.

[74] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf

Appendix 6 – The Future of Data Protection in the Third Pillar

At the time of this writing, the future of data protection for law enforcement, intelligence, and security in the EU as a whole is ambiguous. Data protection in the Third Pillar strikes at the heart of the EU structure, because it affects state accountability and control in law enforcement, a core value of sovereignty. These issues are being worked out through the EU's political apparatus in tandem with the Member States.

If ratified, the Treaty of Lisbon (Lisbon Treaty) will amend the EU's two core treaties, the TEU and the Treaty establishing the European Community. The Lisbon Treaty would significantly modify the institutional framework of the entire EU, most particularly in the area of EU criminal justice. The Treaty would expand the EU from a "common market" to include a "common area of Freedom, Security and Justice" (AFSJ). The Pillars would cease to exist and all matters, including information sharing agreements between the EU and third countries, would have to be passed with the full participation of Parliament and a weighted majority vote of the Council. Moreover, the EU would have authority to pass a data protection framework decision over all personal data use by Member State law enforcement and security agencies without seeking the unanimous consent of each Member State, as it would now.

The Informal High Level Advisory Group on the Future of European Home Affairs Policy (the Future Group) may also have an impact on the future of data protection for law enforcement and security agencies. The Future Group, chaired by the Council President's Minister of Justice and the European Commission Vice-President, addresses the priorities and the future of European justice and home affairs policy after the five-year Hague Programme, which is set to expire at the end of 2009. The Future Group issued a report in June 2008 anticipating challenges in the period 2010-2014 "essential to safeguard and complete the area of justice, freedom, and security in the light of continuously changing framework conditions." [75] Most encouraging for the US, the Future Group takes a perspective similar to ours, *i.e.,* that the goals of privacy and security are not mutually exclusive, and acknowledges that mobility, security, and privacy are all of value to the citizen and should not be seen as opposing concepts. The Future Group endorses the use of new technologies and databases to ensure security while preserving privacy.[76] Recognizing the increasing interdependence of internal and external security, the Future Group called for the EU to shift its attention toward cooperating with third countries.[77] In short, the report calls for greater convergence of law enforcement and security tools, based within and without the EU, implemented in a manner that protects the individual's privacy.[78]

[75] http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf
[76] Id. at para. 32.
[77] Id. at para 33-34.
[78] Id. See also para. 168, supporting the work of the EU-US High Level Contact Group on Data Protection, with the aim of concluding a binding agreement based on reciprocity.

Appendix 7 – Summary of the Application of the Pillar Structure to US Collection of PNR Data

DHS experience with the EU Pillar Structure may be understood by reviewing the history of the US-EU PNR Agreements. Below is a summary of this experience.

1. US – EU 2004 PNR Agreement

In the aftermath of September 11, 2001, the US Customs Service sought to implement recent revisions to ATSA, to obtain access, for border and air security purposes, to PNR originally collected by airlines and airline reservation systems for commercial purposes. In 2004, the IRTPA gave further authority for the Federal government to conduct passenger screening before individuals board a flight destined for the US. CBP sought to carry out the statutory mandates, but before it could do so, the European Commission advised that the 95 Directive prohibited cross-border sharing with non-EU countries absent a demonstration that the receiving entity in a third country has adequate data protection standards. In order to achieve a harmonized approach throughout the EU, and to provide certainty to the private sector about the permissibility of data transfers, the US Government and the European Commission negotiated an agreement to allow airlines to share information while maintaining safeguards for PNR data related to flights to and from the EU. The Commission deemed the transfers "adequate" under the 95 Directive.

Before and after the signing of the Agreement, the Article 29 Working Party issued a series of public Opinions and press releases.[79] These Opinions and press releases highlighted concerns of the Working Party with the data protection afforded by the DHS to European PNR and also reflected the Working Party's assumed authority in this area. Most notable for the purposes of this paper is the first Opinion, which calls for the EU to incorporate the concept of the Third Pillar in its negotiations with the US. The Opinion recognizes that "data transfers made to the public authorities of third countries for reasons of public order in this country should be understood in the context of cooperation mechanisms set up under the Third Pillar (judicial and police cooperation)."[80] The Opinion recommends conditions for PNR transfers to be made analogous with those under the Europol Convention and Eurojust Decision.[81] Ultimately, the Working Party found the 2004 PNR Agreement to be inadequate under the requirements of the EU Directive.[82]

Shortly after the signing of the 2004 Agreement, the European Parliament, disturbed over what it viewed as an attack on its purview within the European system to be consulted on international agreements, and a perceived dilution of EU fundamental personal privacy rights, filed two suits in the European Court of Justice (ECJ) arguing against the European Commission's competency to enter into a such an agreement with the US. On November 22, 2005, the ECJ's Advocate General released his Opinion, finding that the Parliament's concerns were unfounded and recommending that the EC's decision to find adequacy under the 95 Directive be annulled. On May 30, 2006, the ECJ ruled that the EC's decision to grant adequacy did not fall within the

[79] Opinion 6/2002, Opinion 4/2003 and press release, Opinion 8/2004, Opinion 6/2004, Opinion 2/2004.
[80] Opinion 6/2002 at 9.
[81] The EU Council has deemed DHS adequate to receive personal data from Europol and Eurojust.
[82] Opinion 2/2004.

scope of the 95 Directive because it concerns processing of personal data for public security, which is excluded from the scope of the 95 Directive. Consequently, the Court annulled the decision on adequacy and required termination of the agreement by September 30, 2006.

Subsequently, the Article 29 Working Party issued *Opinion 5/2006 of The Working Party on the Protection of Individuals with Regard to the Processing of Personal data on the ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States*. In this Opinion, the Working Party "assumes that the national data protection authorities and the European Data Protection Supervisor are heard and consulted [regarding further negotiations between the EU and US on PNR transfers]." The Opinion also notes that "the Court ruling shows once more the difficulties arising from the artificial division between the pillars and the need for a consistent cross pillar data protection framework." Two months later, the Working Party went on to issue Opinion 7/2006, stressing the urgent need for a new agreement.

2. US-EU 2007 PNR Agreement

The US negotiated a third PNR Agreement (a second agreement was an interim agreement negotiated immediately following the expiration of the 2004 Agreement) with the EU Council, this time advised by the European Commission. On August 1, 2007, this third agreement came into force. The new agreement stipulates that all passengers traveling to the US be protected against terrorist and serious transnational criminal threats while ensuring a high level of protection for their personal information. It also provides legal certainty for air carriers – ensuring that their compliance with the DHS PNR regulation does not result in enforcement activities by European data protection or other authorities.

In August 2007, the Article 29 Working Party issued *Opinion 5/2007 on the follow-up 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 concluded in July 2007*. The Opinion criticizes the 2007 PNR Agreement for not "strik[ing] the right balance between demands for the protection of public safety and other public interests, such as the privacy rights of individuals."

Also subsequent to the signing of the 2007 Agreement, the EU Parliament passed a resolution requiring a legal evaluation of the Agreement. In its Legal Opinion, the EU Parliament Legal Service noted that neither the TEU nor any applicable EU or European Commission legislation provides specific criteria against which to judge the validity of the 2007 PNR Agreement. The Opinion emphasized the inapplicability of the 95 Directive.[83]

[83] Legal Opinion SJ-0634/07, Oct. 25, 2007 found at http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/pnr_sj0634_2007_legal_opinion_25_10_07/PNR_SJ0634_2007_legal_opinion_25_10_07en.pdf. The Legal Opinion went on to evaluate the Agreement against the EU's duty to respect fundamental rights "as guaranteed by the European Convention of the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950." The Legal Opinion concluded the Agreement was "globally satisfactory."