STEPTOE & JOHNSON LLP
ATTORNEYS AT LAW

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
Tel 202.429.3000
Fax 202.429.3902
steptoe.com

ANONYMIZATION, DATA-MATCHING AND PRIVACY: A CASE STUDY

Stewart Baker
Kees Kuilwijk
Winnie Chang
Daniel Mah

December 2003

One of the challenges posed by terrorism is how to catch or foil terrorists without sacrificing the democratic values that the terrorists are attacking. One promising tool is the use of modern data processing to correlate the large amounts of information generated or collected by private industry. Properly marshalled and processed, such data holds the promise of identifying suspicious actors and activities before they coalesce into an attack. At the same time, the use of such capabilities raises concerns about privacy and the possible misuse of the capabilities for purposes other than foiling terrorism. The thesis of this paper is that cryptography and related technologies will allow democratic nations to make effective use of data-processing capabilities while dramatically reducing the risk of misuse. In particular, advanced techniques for "anonymizing" personal data will help to preserve privacy while obtaining the many benefits of data processing technology.

This is not simply a philosophical question. Protection of privacy and personal data are enshrined in law by most democracies. For that reason, any effort to use private data in the fight against terrorism must pass legal muster. This paper examines the extent to which sophisticated anonymization techniques can resolve some of the most difficult conflicts between privacy and security.

We sought to test our thesis by examining a particularly intransigent problem under particularly strict data protection rules and chose the CAPPS II dispute between the United States and the European Union over the sharing of passenger information possessed by airlines. CAPPS II provides a good case study for demonstrating the uses of anonymous data matching technology because it implicates the EU Directive on data protection, arguably the most rigorous and broadly applicable standard for the protection of personal data anywhere in the world today.

I. Introduction and Summary

The United States and European Union are engaged in difficult negotiations concerning the transfer of Passenger Name Record ("PNR") data from EU airlines to the U.S. government for the purposes of detecting and preventing possible terrorist and other criminal activity. The underlying problem is that the United States would like to be able to search a large volume of PNR data for terrorism and other criminal suspects whom it has identified from a variety of intelligence and law enforcement sources. While there is little doubt that specific information about individual suspects could be transferred to the U.S. pursuant to an exception to the EU data protection laws, the U.S. cannot send such a sensitive list to a large number of companies. Instead, it needs to be able to search for the names by comparing its list to a list of all passengers. This would give the U.S. government access to the PNR data of numerous ordinary passengers in whom the U.S. has no law enforcement or national security interest. This creates a conflict between the legitimate needs of the U.S. government and EU data protection laws designed to preserve the privacy of EU citizens.

This paper considers whether the CAPPS II issues can be resolved through the use of anonymization and anonymous data matching technology. Under our proposal, the airlines would provide anonymized PNR data to a trusted third party intermediary who would then match that data against a similarly anonymized list of suspects provided by the U.S. government. Only if this "blind" process yielded a match would information about particular passengers be revealed to the U.S. government. We conclude that the anonymous matching process outlined above (or some variant thereof) meets the stringent requirements of the data protection laws of the EU, including the data protection laws of four of its Member States – Germany, Spain, France, and the United Kingdom.

In summary, under the EU Directive and the data protection laws of these four Member States:

- PNR data that have been anonymized so that the person who possesses the data cannot easily identify the individuals involved is no longer "personal data" that is subject to the EU data protection laws.

- As a result, the transfer of such anonymized PNR data to the United States is not subject to the restrictions on cross-border data transfers under those laws, provided that the recipient in the United States cannot easily de-anonymize the data upon receipt.

- Even if the transferred data could be easily de-anonymized by the Unites States, the transfer would be permissible if it was "necessary or legally required" to transfer that information "on important public interest grounds." This would likely be the case for information about suspected terrorists (and possibly other serious criminal offenders).

- Finally, the process of anonymization might itself be "data processing" that is subject to the EU data protection laws, but no additional notice or consent is required before PNR data may be anonymized.

This analysis suggests that a properly designed and implemented system of anonymization and anonymized data processing has real promise in the effort to use modern technology to provide protection against terrorism without sacrificing privacy. In particular, anonymization could solve the

current deadlock over CAPPS II and the sharing of PNR data. The system would have to ensure that anonymized PNR data is not received in the United States by anyone who could easily rediscover the identities of the individual passengers, and limit the transfers of identifiable information or data that could be de-anonymized to only that which is necessary "on important public interest grounds."

II. Background and Context

A. U.S.-EU Debate Over Passenger Data Transfers – CAPPS II

The U.S. Aviation and Transportation Security Act of 2001 introduced the requirement that airlines operating passenger flights to, from or through the United States, provide the U.S. Customs and Border Protection Bureau ("CBP"), upon request, with electronic access to PNR data contained in their reservation and departure control systems.

From a European legal standpoint, EU airlines may not transfer personal data from the EU to a non-EU country that does not provide an "adequate level of protection" for such data. The European Commission has raised the data protection concerns in bilateral contacts with the United States. On February 18, 2003, the European Commission and CBP issued a Joint Statement reflecting an interim agreement under which it became possible for airlines to transfer personal data of passengers to the United States. Since early March 2003, the United States government has been collecting PNR data from U.S.-bound flight passengers from the EU.

The two sides agreed to work together towards a final bilateral arrangement to reconcile U.S. requirements with the requirements of data protection law in the EU. Several rounds of talks have taken place, but the interim agreement has come under attack from the European Parliament and the data protection agencies of the Member States.

Any final agreement with the U.S. will have to address the new U.S. passenger filtering system. This Computer Assisted Passenger Pre-Screening ("CAPPS II") system is due to be launched in 2004. CAPPS II will be used to cross-check a set of data so as to "weigh" the risk of each airline passenger. The European Parliament has particularly raised concerns about providing data for the CAPPS II system, fearing that data would be circulated on an even wider scale than is currently the case.

B. Current Major Open Issues in the Debate

At the time of writing, press reports indicate that disagreement remains on several issues in particular. The Commission reportedly is concerned about the purposes for which the data may be used. The U.S. wants to use the data not only for combating terrorism but also for combating "other serious criminal offenses," such as narcotics offenses and money laundering, which sometimes have been linked to terrorism. The EU considers the phrase "other serious criminal offences" to be too vague to be a limitation on the kinds of investigations that could be conducted with PNR data. Also, some disagreement remains on whether and to what extent "sensitive" information (*e.g.,* religious or health information) needs to be transferred.

In addition, discussions have focused on the length of time that the data will be available to the U.S. authorities. Currently, the U.S. seeks access for seven years, while the Commission is seeking to limit archiving to a period of three years.[1]

Finally, the U.S. has not fully resolved concerns about remedies for passengers in cases where errors may have been made. Any passenger who wants to review his personal data will be able to do so, and a chief privacy officer has been appointed in the department that handles these issues. However, the EU is seeking further assurances. Since no formal procedures have been established with regard to access to data, the EU believes the rights of data subjects are not sufficiently protected.

C. Anonymization and Anonymous Data-Matching as a Possible Solution

"Anonymization" is a recognized method for dealing with personal data in the U.S. and EU alike. It has spawned technical approaches that can be quite sophisticated. For example, some anonymization technology uses cryptographic methods to transform identifying information using a "one-way hash function," which converts a record to a character string that serves as a unique identifier (like a fingerprint). Correctly implemented, anonymization would make it extremely difficult to extract the person's identity from the anonymized information. Such a system can be particularly useful in determining whether the same name appears on two lists owned by different parties that do not wish to share the lists themselves. Thus, by using such technology, it would be possible for EU airlines to provide a list of passengers and to have that checked against a list of U.S. government terrorism suspects without the airlines seeing the U.S. list or the U.S. government seeing the airlines' list. To ensure that the data matching is truly "blind," the anonymized data could be provided by each party to a trusted intermediary with no access to the original data. Only if there was a match would any personal data of any kind be provided to the U.S. government.

Use of anonymization and anonymous data-matching technology could help eliminate many of the issues in the current U.S.-EU dispute. A properly designed and implemented system would (i) allow the data-matching to be conducted without disclosing the identities of the vast majority of passengers in the data set, and (ii) limit disclosures of personal data to the U.S. to information about passengers who appear or are closely associated with individuals on the U.S. list of suspects. Transfers of personal information about passengers on the suspect list to the U.S. would ordinarily be justified under the recognized "public interest" exception to the EU restriction on personal data transfers.

III. EU Data Protection

The European Union's Data Protection Directive[2] lays down rules regarding the protection of the "personal data" of EU citizens. The two aspects of the EU Directive that are of concern here are the

---

[1] This is most likely because three years is the term granted by the Computer Reservation System ("CRS") Regulation. Regulation (EEC) No. 2299/89 on computerized reservations systems, as amended by Regulation (EC) No. 323/1999. Under Article 6(1)(a), personal data have to be taken off-line within 72 hours of the completion of the booking (*i.e.*, flight arrival), can be archived for a maximum of three years, and access to the data is allowed only for billing-dispute reasons.

rules on transfers of personal data outside of the EU and principles for the "processing" of personal data.[3]

A. Restrictions on Transfers of Personal Data Outside of the EU

Articles 25 and 26 of the EU Directive prescribe restrictions on the transfer to countries outside the EU of "personal data" that are subject to processing or which are intended to be processed in other countries outside the EU after being transferred. Data transfers to non-EU countries that do not offer an "adequate level of protection"[4] are only permitted in certain defined situations, for example:

- when the data subject has given his or her unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or is at the request of the data subject;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interest of the data subject; or
- when a binding contract protecting the exported data, or a similar binding arrangement, such as the EU-U.S. Safe Harbor[5] arrangement, is in place.

---

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EU Member States were required to bring their existing domestic laws, regulations and administrative provisions relating to data protection in compliance with the Directive at the latest by October 24, 1998. Not all Member States succeeded in doing so before this deadline, but currently only France has not yet fully implemented the Directive.

[3] The European Commission has competence to address any external relations questions arising under the Directive, such as cross-border data transfers to non-EU countries. Specifically in the area of airline passenger data transfers, the Commission also has responsibilities under the CRS Regulation. The Regulation provides a code of conduct for computerized booking systems, and contains data protection provisions in Article 6. Article 11(1) of the Regulation provides that: "Acting on receipt of a complaint or on its own initiative, the Commission shall initiate procedures to terminate infringement of the provisions of this Regulation."

[4] The Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25(6) of Directive 95/46/EC whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. The Commission has so far recognized Switzerland, Hungary, the U.S. Department of Commerce's Safe Harbor Privacy Principles, Canada, and Argentina as providing adequate protection.

[5] The Safe Harbor is an arrangement between the EU and the U.S. which provides a way for U.S. companies that are not subject to Directive 95/46/EC to nonetheless provide "adequate" privacy protection, as defined by this Directive. This means that personal data can be transferred from the EU to U.S. companies that have signed up to Safe Harbor even though the U.S. as such is not recognized as providing adequate protection. To benefit from Safe Harbor companies must comply with seven specific privacy principles. *See*

The data protection laws of the Member States considered in this paper treat transfers of personal data to non-EU countries in similar ways.

B. Restrictions on Processing of Personal Data Without Consent (or Other Appropriate Basis) and Notification Requirements

The Directive also stipulates that any processing of personal data must be lawful and fair to the individuals concerned (the "data subjects"). The data kept by "data controllers" (*e.g.*, airlines) must be adequate, relevant and not excessive in relation to the purposes for which they are processed.[6] In order to be lawful, any processing of personal data must be carried out with the "unambiguous consent" of the data subject or, alternatively, must be "necessary" on certain specific grounds – for example:

- necessary to perform a contract binding on the data subject, or to take steps at the request of the data subject prior to entering into a contract; or
- necessary for compliance with a legal obligation to which the controller is subject; or
- necessary in order to protect the vital interests of the data subject; or
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (except where such interests are overridden by the data subject's privacy rights).[7]

The data protection laws of all Member States considered in this paper (Germany, United Kingdom, Spain, and France) include similar provisions.

More stringent rules apply to the processing of "sensitive data" which are defined by the Directive as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership," and data "concerning health or sex life." In principle, such data can only be processed with the data subject's "explicit" consent or in very specific circumstances, such as where the processing of data is mandated by employment law, or where it may be necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable

---

http://www.export.gov/safeharbor for information on the Safe Harbor arrangement and the companies that have joined it.

[6] Art. 6 of the Directive.

[7] Art. 7 of the Directive.

of giving his consent.[8] The data protection laws of the Member States considered in this White Paper define and treat "sensitive data" in essentially the same way.

In addition, the EU Directive requires the data controller to notify the data subject of certain information when collecting personal data, including the identity of the data controller, the purposes of the processing for which the data are intended, and recipients or categories of recipients of the data, unless the data subject already has this information.[9]

IV. Analysis

A. Anonymized PNR Data is not "Personal Data"

Once PNR data has been anonymized, it is no longer "personal data" and thus no longer subject to the restrictions on processing or transfers of personal data in the EU Directive and data protection laws. The issue that may be disputed, however, is whether the data has been sufficiently "anonymized" so that the individuals involved cannot be identified.

"Personal Data" and Identifiability. The Directive and national laws show remarkable consistency in defining personal data. The Directive defines "personal data" as: "any information relating to an identified or identifiable natural person ("data subject")." An identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[10] Recital 26 of the Data Protection Directive states that: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." The data protection laws of the Member States considered in this paper define "personal data" in essentially the same way.[11]

---

[8] Art. 8 of the Directive.

[9] Art. 10 of the Directive.

[10] Art. 2(a) of the Directive.

[11] The German Data Protection Act defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)." *See* German Data Protection Act, Sec. 3(1). The United Kingdom defines personal data as "data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual." *See* UK Data Protection Act, Sec. 1(1). In Spain, personal data means "any information concerning identified or identifiable natural persons." *See* Spanish Data Protection Act, Art. 3(a). In the draft French law, personal data included "all information with regard to an identified natural person or one that can be identified, directly or indirectly, by reference to an identification number or by one or several elements that are his. To determine whether a person is identifiable one needs to consider all means that can be reasonably employed either by the data controller or by a third person." *See* French Draft Data Protection Act, Art. 2(2).

In other words, data that cannot be used to identify a particular individual is not "personal data." Accordingly, if personal data have been stripped of all personal identifiers such that the data can no longer be used to identify the data subject, then the data will cease to be personal data, and non-personal data are not subject to the EU Directive and data protection laws.

Anonymization. This reasoning is confirmed by Recital 26 of the Data Protection Directive which states that: "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." Similarly, the data protection laws of the Member States considered in this paper all address the issue of anonymization.

Most of the EU members considered here take the view that anonymized data are not personal data and that their data protection laws do not restrict the processing of such data. The Spanish Data Protection Act refers to anonymization (literal translation: "depersonalization"), which it defines as: "any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person."[12] Article 11, the basic provision on data processing, stipulates that "personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject," or for a limited number of other legitimate reasons.[13] But Article 11(6) explicitly provides that "if the communication is preceded by a depersonalization procedure, the provisions of the preceding paragraphs shall not apply." In other words, anonymized data can be freely processed.

Similarly, under the French (draft) Data Protection Act, most forms of data processing are excluded from the application of the Act where the processing is preceded by an "anonymization procedure" that has been approved by the French Data Protection Agency (the "CNIL").[14] While the CNIL has not yet established official standards for approved anonymization procedures, it has previously expressed a view (in a related context) that techniques such as hashing ("hachage") or encryption are recognized methods for handling medical data.[15]

The United Kingdom and Germany take a less categorical approach but come to the same conclusion. The guidance issued by the UK data protection authority provides that "whether or not data which have been stripped of all personal identifiers are personal data in the hands of a person to whom they are disclosed, will depend upon that person being in possession of, or likely to come into possession of, other information, which would enable that person to identify a living individual."[16]

---

[12] Spanish Data Protection Act, Art. 3(f).

[13] Spanish Data Protection Act, Art. 11(a)-(f).

[14] Art. 8:IIbis and Art. 32:IIbis of the French (draft) Data Protection Act.

[15] Recommendation n° 97-0008 (Feb. 4, 1997)

[16] U.K. OFFICE OF THE INFORMATION COMMISSIONER, DATA PROTECTION ACT 1998 LEGAL GUIDANCE 14, *available at* http://www.informationcommissioner.gov.uk (last visited Nov. 26, 2003) ("U.K. LEGAL GUIDANCE").

What matters to the UK authority, in other words, is the data controller's ability to identify the data subject, not its intent to do so.[17]

The German Data Protection Act also defines anonymization (literal translation: "depersonalization") as: "the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual."[18] The Act does not require elaborate technological guarantees against matching data with names. Nor does it take the strict UK view adopted that what matters is a controller's ability to recombine the anonymized data. It provides that data may be processed without data protection obligations where "the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual" are "stored separately."[19]

When is data anonymized? This raises the question of when personal data is anonymized. Unfortunately, as the discussion above suggests, there is no clear standard. Some countries, like Germany and the UK, put an emphasis on the separate storage of information capable together of identifying individuals. Other countries make reference to how easily a person in possession of the anonymized data can use "reasonable efforts" to identify a person. In the words of the Directive, "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."

The strictest view, taken by the UK Guidance Notes, suggests that if a person possesses both the anonymized data and the original data set, all of the data (even the anonymized data) remains personal data. Where this strict view prevails, it might be further argued that the transfer even of anonymized data by an entity that also holds the original data set is still subject to the cross-border data transfer restrictions in the EU Directive. However, this is an unduly strict reading of the data transfer restrictions. In ordinarily usage, the "transfer" of personal data connotes the combined acts of sending *and* receiving data. So, even if anonymized data remains "personal data" in the hands of the person that sends the data, there is no "transfer" of that data if no personal data are received by the entity at the other end of the line.

In short, even in jurisdictions that treat anonymized data as personal data while in the possession of entities that have the ability to "de-anonymize" the data, it is unlikely that those entities are "transferring" personal data when they convey the data to a party that cannot de-anonymize the data. Finally, even if this were viewed as a transfer of personal data, the anonymization process could easily be tailored to eliminate any doubt, simply by using a trusted intermediate party. That is, the airlines

---

[17] "The fact that the data controller is in possession of the original data set which, if linked to the data that have been stripped of all personal identifiers, will enable a living individual to be identified, means that all the data (including the data stripped of personal identifiers), remain personal data in the hands of the data controller and cannot be said to have been anonymised. The fact that the data controller may have no intention of linking these two data sets is immaterial." *Id.* at 13.

[18] German Data Protection Act, Sec. 3(7).

[19] German Data Protection Act, Sec. 30(1).

could retain the original data set while giving anonymized data to an intermediary in the EU. Provided that the intermediary cannot access the original data set, it would not be a data controller in possession of personal data. The export of the anonymized data by the intermediary would not then be subject to the cross-border data transfer restrictions in the EU Directive and data protection laws.[20]

B. Transfers of Anonymized PNR Data Outside of the EU Are Not Transfers of Personal Data, Provided the Recipient Cannot Easily De-anonymize the Data

Because anonymized data, at least in the hands of an intermediary, are not "personal data," anonymized data are no longer subject to the EU restrictions on transfers of such data to non-EU countries that do not provide an "adequate level of protection" for personal data. There is a second reason for the use of an intermediary in the CAPPS II context. Remember that the use of hashing to anonymize the data is designed to allow the U.S. government to identify a "match" between data tied to terrorism suspects (names, phone numbers, credit cards, and the like) and similar data on passenger lists – all without gaining access to the identities of any other passenger. This means that, for a very limited group of passengers – terrorism suspects – the government may learn that a particular passenger has an important characteristic in common with someone on its terrorism suspect list. Whether this constitutes de-anonymization is open to question, but taking a strict view of the question, one might conclude that the personal data of persons associated with terrorism suspects (and only terrorism suspects) has been transferred to the U.S. government, at least if the transfer occurs directly.

Does this matter? We are inclined to doubt that it does. Even extreme advocates of data protection would not argue that a nation could not be alerted by the airlines when a terrorism suspect gets on a plane bound for that nation. In such a case, personal data would ordinarily be transferable under the EU Directive pursuant to the "necessary . . . on important public interest grounds" exception to the restriction on transfers. And in any event, because only the U.S. government has the ability to identify the terrorism suspects whose data has been matched, transfers to intermediaries do not transfer the personal data even of the terrorism suspects. In consequence, such transfers would seem to comply fully with EU law.

C. Anonymization is Data "Processing," But No Additional Notice or Consent Procedures are Required

As noted above, the last issue is whether the process of anonymization is itself data "processing" under the EU Directive and data protection laws. If so, then anonymization is only permissible with the data subject's "unambiguous consent" or if anonymization is "necessary" in the ways described in Section III.B. Anonymization might fall within the broad definition of "processing of personal data," but additional notice and consent of the passenger is not required.

---

[20] This is a variant on a proposal by the Austrian data protection agency for PNR data to be filtered through a short-term storage intermediary, whereby controlled access would then be permitted to foreign governments. The difference here is that the data intermediary would be a private entity located within the EU that would only hold the anonymized PNR data. The original personal data remains with the airline that collected it.

"Processing of Personal Data." The Directive defines "processing of personal data" as: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[21] The data protection laws of the Member States considered in this paper define "processing of personal data" in essentially the same way.

This broad definition suggests that anonymization, because it involves "alteration" or "erasure or destruction" of personal data may be data "processing" under the EU Directive. The guidance notes issued by the UK data protection authority state that "[i]n anonymizing personal data [a] data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the [Data Protection] Act."[22] This is implicit in the Spanish Data Protection Act as well, which refers to anonymization as "any *processing of personal data* carried out in such a way that the information obtained cannot be associated with an identified or identifiable person."

On the other hand, anonymization is a measure designed to improve the privacy of personal data and it seems strange to impose the notice and consent requirements of the Directive and data protection laws on a measure designed to increase the protection offered to personal data. Even in the UK, the Court of Appeal in *Regina v. Department of Health, ex parte Source Informatics Ltd.*[23] has expressed a view that the Directive should be construed purposively so that "anonymization" is not considered "processing" under the Data Protection Act.

Notice and consent requirements? If anonymization is not "processing of personal data," then the notice and consent requirements in the EU Directive and data protection laws will not apply. But even if anonymization constituted "processing of personal data," it is our view that no additional notice or consent is required before such processing can take place.

For non-sensitive data, additional notice and consent of the passenger is not required. First, anonymization actually improves the privacy of the passenger's personal data. Because anonymization will actually increase the protection of the data subject's personal data, it would be inappropriate to require data controllers to obtain prior consent before doing so. Second, the anonymization is necessary to comply with existing legal requirements, including the data security requirement as well as the obligation not to transfer personal data outside of the EU to countries without adequate safeguards. (Some would argue that compliance with U.S. law ought also to be considered under this heading, but data protection authorities have resisted this conclusion.) And finally, anonymization is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed," except where the passenger's privacy interests override.[24] Here, the legitimate

---

[21] Art. 2(b) of the Directive.

[22] U.K. LEGAL GUIDANCE, *supra* note 16, at 13.

[23] [2001] Q.B. 424.

[24] *See* Art. 7 of the Directive.

interests are the security of the data as well as the security and law enforcement interests of the U.S. and EU governments, the airlines, and the passengers themselves.

A different analysis is required for "sensitive data" (*i.e.*, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and information concerning health or sex life). In many cases, sensitive data may simply be excluded from the database. Such information is not routinely gathered in PNR data, although it might be argued that sensitive data could be inferred from a passenger's dietary preferences or wheelchair requests. But such information is, of course, provided initially with the consent of the passenger – it is the passenger's request after all – and for flights to the United States. Thus, the information almost by definition must be exported to that country, and in today's world it certainly must be subjected to electronic data processing. It is reasonable to conclude that the very act of requesting a particular type of meal or a wheelchair includes an explicit consent to the use of that information on an electronic network. It cannot be necessary to obtain a separate consent for each step in the electronic process – *e.g.*, transmitting to a server, populating a database, encrypting for security, transferring to a client from the server, etc. This is particularly true in the case of measures, such as encryption or anonymization, designed to protect the passenger's personal data. Indeed, the passenger has a right to expect the airline to keep his or her sensitive information secure, and anonymization is simply one means by which the airline can do so.

Finally, as to the notification requirement, the airline is required to inform the passenger of "the purposes of the processing for which the data are intended" unless the passenger already has this information. As with sensitive data, the passenger plainly knows that the airline will process the personal data that is collected and has a right to expect that it will be stored securely. Since anonymization is one means of ensuring the security of personal data, the passenger is already aware of the relevant purpose for which his or her personal data will be processed.

V. CONCLUSION

Terrorism poses one of the most difficult challenges facing democratic nations today – how to combat terrorism while protecting the privacy of ordinary citizens. On the one hand, modern data processing technology is a promising tool for combating terrorism. On the other hand, such technology raises privacy concerns and the possibility of misuse. These competing concerns are particularly evident in the current U.S.-EU deadlock over the sharing of airline passenger data. The analysis in this paper presents a possible solution to this deadlock in the form of a properly designed and implemented system of anonymization and anonymous data processing. By securely anonymizing personal data before it is processed by an intermediary, relevant data about suspected terrorists can be shared while fully complying with the strict privacy protections of the EU Directive on data protection. Thus, this technique of anonymizing personal data before the data is processed represents an important means in a wide variety of contexts by which benefits of data processing technology can be realized without sacrificing privacy.