Potential Conflict of the Total Information Awareness System with EU Regulations

February 2003

LL File No. 2002-14112
LRA-D-PUB-000269

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

2002-14112

LAW LIBRARY OF CONGRESS

POTENTIAL CONFLICT OF THE TOTAL INFORMATION AWARENESS SYSTEM WITH EU REGULATIONS

Introduction

The Total Information Awareness System is a new counter-terrorism intelligence program designed to detect, classify, and identify foreign terrorists. The TIA system is being developed by the Defense Advance Research Projects Agency (DARPA), an agency within the U.S. Department of Defense.

If fully implemented as planned, the TIA would allow law enforcement to retrieve and analyze data from various government and commercial databases in order to detect patterns and clues about potential terrorists.

In the last decade, the tremendous growth of Internet and electronic commerce has led to a proliferation of personal data collected by companies, such as airlines, banks, insurance, or credit card companies. These databases contain a wealth of information not only about U.S. citizens but also citizens of the European Union (EU). The information may relate not only to one's personal data, such as first and last name, address or social security number which are sufficient to identify a particular person, but also other data classified under EU law as "sensitive" that relates to one's health, age, racial or ethnic background, political affiliation, religious belief, or sexual orientation.

Recently, public concern has been raised not only in the United States but also among EU officials about the U.S. government's potential use of the TIA to access, retrieve, and further process of information held in databases. Currently, the EU and the United States have different approaches to the issue of personal data protection and privacy and have treated it in a different manner. The United States does not have omnibus legislation on privacy but relies on a sectoral approach. The EU considers the right to protect one's personal data a basic human right, distinct from the right to privacy, and has adopted comprehensive legislation. The legislation consists of two directives that are binding on the Member States. The Directives strictly regulate the manner by which personal data and the right to privacy in the electronic communication sector are processed within the Community and the European Economic Area.

These different approaches to privacy protection led to two agreements on personal data. Each was drafted for a distinct purpose and under different circumstances. The first, the so-called Safe Harbor agreement, signed in 2000, was agreed upon for commercial purposes after long negotiations between the Department of Commerce and the European Commission. The agreement was signed because the EU privacy legislation prohibits transfers of personal data outside the EU area unless the third country meets the adequacy standards of the EU.

The second agreement, signed on December 20, 2002, regulates the exchange of personal data in the law enforcement field. The agreement establishes the terms and

conditions under which transfer of personal data is possible in the law enforcement. It was preceded by a cooperation agreement, signed December 6, 2001, between Europol and the United States as part of increased cooperation and solidarity between the EU and United States in the aftermath of September 11.

This report deals with whether or not the use of the TIA system may infringe upon the EU Directives on personal data protection and privacy in the telecommunications sector. The report is divided into two parts.

Part I deals with three issues: **A)** whether U.S. authorities who engage in processing personal data either from EU based websites or non- EU based websites will fall within the scope of the Directive. **B)** a synopsis of substantive law focusing on the principles of processing personal data that are embodied in the privacy directives; and **C)** whether processing and analysis of personal data of passengers collected by airlines is compatible with EU privacy rules. This example serves as an illustration of possible infringements of personal data of EU citizens protected by EU law from the vast number of Internet websites which gives the TIA system unlimited possibilities to "mine" data from a variety of sources.

Part II includes an overview of the recently signed agreement on exchange of personal data and other related information between Europol and the United States.

I. European Union Legal Framework

The EU recognizes the right to protection of one's personal data as a separate right distinct from the right to privacy. Article 7 of the Charter of Fundamental Rights[1] provides for the right to private and family life, whereas article 8 ensures the right to protection of one's personal data. There are two directives in the field of personal data and privacy: a) Directive 95/46/E.C. on the protection of individuals with regard to the processing of personal data and on the free movement of such data,[2] hereafter the Data Protection Directive, and b) Directive 2002/58/E.C. on the processing of personal data and the protection of privacy in the electronic communications sector,[3] hereafter the Privacy and Electronic Communications Directive. The first is a general framework directive, that contains strict rules on the processing of personal data whereas the second, as its title indicates focuses on the protection of privacy in the electronic communications field.

[1] It has been officially proclaimed by the European Parliament the Council and the Commission, on Dec. 7, 2000.

[2] OJ L 201/31 (Nov. 23, 1995).

[3] OJ L 201/37 (July 31, 2002).

A. International Effects of Data Protection Directive (95/46/E.C.)

The Data Protection Directive has extraterritorial effects. Consequently, national law on processing personal data applies not only within the community territory and the European Economic Community but also in third countries. Choice of law and jurisdiction issues are matters for the courts of the Member States to decide. More specifically, national law applies in the following instances:

- the processing is carried out in the context of the activities of an establishment of the controller in the territory of the Member State; when the same controller is established in several Member States, he/she is obliged to ensure that all the establishments under his/her responsibility comply with the provisions of the Directive. The Data Protection Directive defines "controller" as the person or body "which determines the purposes and the means of processing;"
- the controller is not established in the territory of a Member State, but in a place where its national law applies based on private international law;
- the controller is not established within the territory of the Community. However, the controllers uses equipment, automated or otherwise, in order to process personal data situated in the territory of a Member State, unless such equipment is used only for purposes of transit through the territory. Recital 20 further elaborates "the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice." Therefore, in this case, the connecting factor between the legal system and the action is the location of the equipment used.

Based on the above principles, the following points may be made:

(d) The Directive attempts to protect the individual whose rights are violated by applying the substantive law of the place where the individual is located when a controller outside the EU processes the data of that individual.

(e) As the Data Protection Working Party has clarified , the word "means" include cases where a text file installed on the hard drive of a computer which will store and send back information to a server located in another country.[4] Thus, when a controller is in the United States and decides to process personal data via equipment, automated or otherwise, he/she is obliged to follow the domestic data protection law of that Member State where the equipment is located.

(f) The above two EU directives protect the personal data of individuals within the European Union, regardless of citizenship. Consequently, if personal data of non-European citizens are processed through means, automated or otherwise, located in the Community territory and in direct violation of the provisions of the Directive, this situation gives rise to liability of those persons or bodies responsible for processing.

---

[4] Data Protection Working Party, WORKING DOCUMENT PRIVACY ON THE INTERNET - AN INTEGRATED EU APPROACH TO ON-LINE DATA PROTECTION, 28 (Nov. 21, 2000).

B. Substantive Law

1. Data Protection Directive

The scope of the Data Protection Directive extends to processing personal data in the public and private sectors. Processing data for reasons of public security, defense, State security, criminal law, or processing falls within the exclusive domain of the Member States, as well as processing performed as a household activity. Processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means." An indicative list of processing activities includes collection, organization, storage, retrieval, disclosure by transmission, and erasure. The definition of personal data includes "any information relating to an identified or identifiable natural person," the so-called data subject. In order to ensure that personal data are effectively safeguarded, the Directive on one hand confers on the data subject a number of significant rights while on the other hand, imposes a number of obligations on processors, *i.e.*, persons, public authorities, enterprises, and other bodies.

The following fundamental principles of processing personal data are derived from the Directive:

- Personal data must be processed lawfully and fairly.
- Personal data must be accurate and kept up to date.
- Personal data must be gathered for legitimate and explicit purposes and be used accordingly (principle of finality).
- Personal data must not be kept longer that it is necessary.
- Appropriate safeguards, such as technical and organizational, must be taken to protect the data from unauthorized or unlawful preceding of personal data.
- Data subjects must be granted certain rights associated to access, erase, correct, or block incorrect data.
- The transfer of personal data to a third country which does not meet the adequacy standards of the EU is prohibited.

a) Rights of Data Subjects

Data subjects have the following basic rights: right of information, right of access, and right to object. The right to information refers to the right of the data subject to know the identity of the controller, purpose of processing, and any other information related to the data recipients. This right applies when the data subject releases personal data and when data about him/her have been obtained through a third person. The right of access encompasses the following elements: a) immediate confirmation of the purpose of processing, groups of data, and recipients of data; b) opportunity to remedy the processing or erase or block the processing in the case of inaccurate of incomplete data; and c) notification to third parties of any rectification or blocking that has occurred.

b) Responsibilities of Controllers

A controller is the person or body "which determines the purposes and the means of processing" and is obliged to ensure that processing personal data occurs under the principles of security and confidentiality. To this end, the controllers must apply certain safety measures to protect personal data from unlawful destruction, alteration, accidental loss, or unauthorized disclosure. When personal data are processed under the control of a processor, the Directive requires that the controller personally selects the processor and their working relationship is secured through the signing of a contract. In this case, the processor only follows the instructions of the controller and is obliged to follow the same safeguards applicable to processing personal data.

c) Criminal Records

Processing data relating to criminal offenses or criminal convictions may be done only under the control of an official authority, unless the Member States adopts exceptions to this rule with sufficient safeguards of the person's fundamental rights.

d) Sensitive Personal Data

Certain data, such as those that relate to one's racial or ethnic origin, religious or philosophical beliefs, political opinions, memberships in trade unions as well as data pertaining to one's health or sex life are considered sensitive and afforded even greater protection. The Directive bars the processing of such data, subject to some exceptions. For instance, if the individual consents to the processing. However, Member States have the option to provide otherwise. Another case of the lawful processing of sensitive data is when the individual has made such data public or when the processed data is related to offenses, criminal convictions, or security purposes and the processing occurs under the responsibility of an official and with safeguards afforded by law.

Medical data fall within the definition of sensitive personal data and are also barred from processing. However processing is allowed, provided that the data subject has granted consent and the processing occurs for preventive purposes or medical diagnosis.

e) Safe Harbor Agreement and Principles

The safe harbor covers the transfer of data of U.S. organizations that fall within the competence and authority of Federal Trade Commission and the Department of Transportation. Thus, other organizations that remain outside the ambit of the above two government bodies have to enter into contracts that incorporate the clauses approved by the Commission

Currently, U.S. organizations have two options to ensure compliance with the EU rules on personal data and privacy. The company may voluntarily enter the Safe Harbor Agreement and follow the Safe Harbor Principles. This applies only to those that fall within the jurisdiction of Federal Trade Commission and Department of Transportation. For those companies that fall outside the scope of these may still comply with EU rules by incorporating the principles by signing contracts with third parties in the EU.

It should be noted that processing personal data that occurs within the EU is subject to the laws of the Member State that has transposed the Directive into national law. Once data are transferred to the United States, then they are subject to the Safe Harbor Principles. U.S. organizations that receive personal data from the EU upon joining the Safe Harbor agreement must subject the personal data to the principles of the agreement and must publish their policies on privacy. Those companies that do not fall within the jurisdiction of the bodies responsible for monitoring compliance must enter into agreements with parties concerned in the United States. Otherwise, Member States are obliged to block the transfer of data to the United States. In brief, U.S. organizations that voluntarily commit to the Safe Harbor Principles must adhere the following requirements:

- **Notice.** Individuals must be informed about the purposes and uses of data about them and whether such data will be transferred to third persons.
- **Choice.** Individuals must be given a choice to decide whether or not their personal data can be disclosed to a third party or used for purposes other than.
- **Onward Transfer.** Organizations that transfer data to a third party, must comply with the first two requirements. Moreover, the organizations must ensure that the third party adheres to the Principles or that it meets the adequacy criterion. In this case, the organization does not bear liability if the third party processes the data in a matter incompatible with the Directive.
- **Integrity.** Personal data must be used only for the intended purposes for which they were collected.
- **Access.** Individuals must be granted the right to access their personal data and the right to amend, correct, or delete the information about them. The access right is not absolute. Organizations may refuse or limit access in a number of cases, such as interference with execution or enforcement of the law, including the prevention, investigation, or detection of offenses; disclosure of personal information concerning other individuals; or breaching a legal or other professional obligation.
- **Enforcement.** Organizations are obliged to provide individuals with recourse mechanisms in case their rights are violated. Organizations also must be subject to penalties in case of infringement of the above principles.

2. Privacy and Electronic Communications Directive (2002/58/E.C.)

The Privacy on Electronic Communication Directive[5] must be implemented by the Member Sates by October 31, 2003. It has a broader scope than the Data Protection Directive, since its objective is to protect the legitimate interests of subscribers of electronic communications who are legal entities. The Working Party on the Protection of Individuals concerning the Processing of Personal Data, as established by the Data Protection Directive is also responsible for matters that fall within the scope of the Directive on Privacy and Electronic Communications. Among the most important aspects of the Directive are

[5] O J L 201/37.

the following:

a) Confidentiality of Communications

The Directive guarantees the confidentiality of communications and traffic data. It requires that Member States prohibit the following actions:

> Listening, taping, storage or other kinds of interception of surveillance of communications and other related traffic data by persons other than users, without the consent of the users concerned, except in specified cases.

This prohibition does not apply to any legally permitted recording of communications and traffic data when such recording occurs during lawful business for evidentiary purposes. Parties involved should be informed, prior to the recording, about the recorded communication, its purpose, duration and storage. Retention of traffic data for law enforcement purposes may take place following the conditions of article 15(1) of the Directive.

b) Traffic Data

Traffic data are defined broadly to include not only data generated through traditional telephone calls but also data created through the transmission of communications over the Internet. The Directive established rules concerning processing traffic data specifies the persons who are legally authorized to do so. In general, traffic data, which are essential for billing purposes and interconnection payments, may be processed for a limited period. Only persons who act under the authority of the providers of public communications networks and publicly available electronic communications services that deal with billing or traffic management, customer inquiries, and fraud services are permitted to process traffic data and only to the extent that is necessary in order to perform the above mentioned tasks.

c) Location Data

The Directive introduces protection for subscribers and users concerning the mobile location information services. Location data may refer to "latitude, longitude and altitude of the users's terminal equipment, to the direction of the travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located."

Procession location data is possible if the data are made anonymous and the users or subscribers have been informed and have consented to the processing for a specific period.

d) Directories of Subscribers

The person who collects data to be included in public directories is responsible to provide subscribers with information related to the purpose of the directory and whether the directory will be further disseminated and the nature of the recipients.

Moreover, it specifies that subscribers must be given specific information free of charge and prior to their personal data being included in a Directory with regard to the purpose of the printed or electronic directory and on any additional usage based on search functions inserted in electronic versions of the directive, such as reverse search capability which allows users of the directory to find out the name and address of subscribers based solely on their telephone number.

C. Access to Personal Data Collected on Passengers Entering the United States through Air or Sea[6]

Post September 11, 2001, airlines arriving or leaving the United States are required by U.S. law[7] to transfer electronically to the Commissioner of Customs and to the U.S. Immigration and Naturalization Service data related to passengers and cabin crew (passenger Manifest Information) 15 minutes before departure. Similar rules apply to maritime transport. All the data are further forwarded to a central database shared by the Customs and INS authorities. Other federal authorities also have access to this database.

Initially, the data collected were limited to identification information, visa or residence permit. Currently, additional data are required such as date of birth, nationality, sex, passport number, and any other data deemed necessary to identify the passengers. Moreover, under the requirement of the Passenger Name Records (PNR), additional data are required on prospective travelers, including date of reservation, credit card number, address, itinerary, seat number, and medical data or dietary needs.

1. Impact of TIA

Based on the EU principles on personal data stated above, the following general observations can be made:

- If U.S. authorities through the TIA are able to access personal data directly within the European territory, it would appear that they fall within the scope of Data Protection Directive which applies in such cases in its entirety. In such a case, they would be bound to follow the provisions of the Directive related to the safeguards afforded to personal data and all the rights to data subjects guaranteed by the Directive.
- If U.S. authorities, through the TIA, access personal data located in a database within the United States, they may still be in violation of several EU rules including the rule that data are processed only for a specific purpose.
- The above situation may also give rise to liability of organizations that operate under the Safe Harbor Agreement and are bound by its rules. Onward transfer of data is possible only if such organizations notify the individuals about the

---

[6] The Data Protection Working Party, which was established pursuant to art. 29 of Directive 95/46/E.C., and has an advisory status has issued a number of opinions on a variety of questions that have been raised related to the personal data and privacy. In case of transmission of personal data and airlines, *see* Opinion 6/2002 on the *Transmission of Passenger Manifest Information and other data from Airlines to the United States* adopted on Oct. 24, 2002.

[7] The Aviation and Transportation Security Act of 2001, P.L. 107-071.

processing and give them a choice as to whether they wish to have their data further processed.

- U.S. authorities may also be in violation of sensitive data that reveal information on one's race, religious beliefs.
- Possible liability of airlines would arise because ai,rlines which are obliged to follow all the security measures required by the Directive in order to protect personal data.
- U.S. authorities may infringe upon the rights of data subjects, especially the right to consent to processing personal data, right to access on the files created by TIA, and the right to have them corrected or erased.

II. Exchange of Personal Data for Law Enforcement Purposes – The Agreement between Europol and the United States

A. Background

Personal data can be transferred by EU Member States within the context of judicial and police cooperation. Under the Europol Convention, the exchange of personal data between Europol and a third country is possible only if the third country in question, in this case the United States, provides an adequate level of data protection and for the purposes of preventing or combating serious crimes. For this purpose and pursuant to EU rules governing the transmission of personal data by Europol, a separate agre ement is necessary that specifically deals with this issue. Such agreements are reviewed by the Joint Supervisory Body which under the Europol Convention is responsible for monitoring compliance with the established rules on transmitting data.

The draft Supplemental Agreement was signed in December 2002, between Europol and the United States. There is also an Exchange of Letters related to the Supplemental Agreement between the United States and Europol on the exchange of personal data and related information.[8]

B. Purpose

Article 1 of the agreement states that its purpose is to prevent, detect, and investigate criminal offenses which fall within the jurisdiction of each party and for any specific analytical purposes, by facilitating the mutual exchange of information including personal data. For the purposes of this agreement, personal data, identifiable natural person and processing personal data have been defined as provided for in the EU legislation.

Some significant highlights of this agreement are the following:

- Any information exchanged based on this agreement, with the exception of information

[8] COUNCIL OF THE EUROPEAN UNION, *Note from Europol to COREPER on Exchange of Letters Related to the Supplemental Agreement between the United States of America and Europol on the exchange of personal data and related information* (Doc. 13996/02, Europol 95), Brussels, Nov. 11, 2002.

that is already in the public domain, will be deemed as law enforcement information and be afforded all the necessary safeguards.

- The phrase "analytical purposes" includes also exchange of information related to immigration investigation and proceedings and to those relating to *in rem* or *in personam* seizure or restraint and confiscation of assets used to finance terrorism.
- Europol may transmit personal data to the United States only upon prior consent of the Member State where the personal data originated.
- Europol shall not consent to onward transmission of personal data by the United States.

C. Requests for Sending Personal Data

The Agreement regulates the manner under which exchange of personal data may occur, the authorities responsible to request and receive information, and the content of each request. Thus, requests for exchange can take place when initiated by either the points of contact established by the December 2001 Agreement (in this case the U.S. Department of Justice and Europol for the EU) or directly between Europol and designated U.S. federal, state, or local authorities.

A request and a response to the request must be in writing or orally with a written confirmation following. In cases where it is possible, a request may be transmitted through fax or email provided that appropriate security measures have been taken. The request must identify the authority making the request, the subject matter, reason for the request, and the nature of the assistance sought.

Based on the above, U.S. authorities either at the federal or state level must strictly follow the provisions of this Agreement in order to receive personal data from an EU Member State. Doing otherwise, either through the use of TIA or in any other manner, will be a direct infringement not only of EU privacy legislation but also of the terms and conditions of this Agreement.

Prepared by Theresa Papademetriou
Senior Legal Specialist
Directorate of Legal Research
Law Library of Congress
February 2003