Robert Schuman

Miami-Florida European Union Center of Excellence

EUMA

EU-US Data Protection
Vindicating Rights to Privacy

Ramón Mullerat

EUMA
Vol. 4 No. 14
June 2007

Published with the support of the EU Commission.

EUMA

***European Union Miami Analysis* (EUMA)** is a bi-weekly service of analytical essays on current, trend setting issues and developing news about the European Union.

These short papers (between 2,000 and 2,500 words in length) are produced by the Miami-Florida European Union Center of Excellence (a partnership of the University of Miami and Florida International University) as an outreach service for the academic, business and diplomatic communities.

Among the topics to be included in the series, the following are suggested:

- The collapse of the Constitution and its rescue
- Turkey: prospects of membership
- Immigration crisis and cultural challenges
- Security threats and responses
- The EU and Latin America
- The EU as a model and reference in the world
- The Common Agricultural Policy and other public subsidies
- The euro and the dollar
- EU image in the United States

These topics form part of the pressing agenda of the EU and represent the multifaceted and complex nature of the European integration process. These short papers also seek to highlight the internal and external dynamics which influence the workings of the EU and its relationship with the rest the world.

Miami - Florida European Union Center
University of Miami
1000 Memorial Drive
101 Ferré Building
Coral Gables, FL 33124-2231
Phone: 305-284-3266
Fax: (305) 284 4406
E-Mail: jroy@miami.edu
Web: www.miami.edu/eucenter

Jean Monnet Chair Staff:
Joaquín Roy (Director)

Astrid Boening (Assistant Editor)
Eloisa Vladescu (Research Assistant)
María Lorca (Research Assistant)

Miami-Florida European Union Center
Nicol Rae (Co-Director), FIU

EU-US Data Protection Vindicating Rights to Privacy[♣]

Ramón Mullerat[♦]

La plus grande menace sur la liberté, c'est la liberté elle-même.
Comment défendre la liberté contre elle même?
En garantissant à tous la sécurité.
La sécurité, c'est la liberté.
La sécurité, c'est la protection.
La protection, c'est la surveillance.
La surveillance, c'est la liberté.
Jean-Christophe Rufin, Globalia (a future ideal democracy)[1]

I. The right to choose

One of the greatest gifts bestowed to the human being is undoubtedly the right to choose. But at same time this gift may be a heavy servitude. Today to be free or to be secure has become a dilemma, a situation requiring choosing between two goods. Since both absolutes are impossible, the question arises because the ideal proportion of freedom and security varies human being from human being. The dilemma is not new but it recently burst again in the US after 11-S and later in the whole globe, including Europe (London 7-J and Madrid 11-M).

In the following paragraphs I intend to present the different attitudes and views in the EU and the US with regard to privacy and data protection in a world specially obsessed with security.

II. The right to privacy

There is no private life
Which has not been determined
By a wider public life[2]

Privacy is the ability of an individual or group to keep their lives and affairs out of public view, or to control the flow of information about them. Today, the right against unsanctioned invasion of

---

[♣] Paper presented at the "EU-US Law Symposium" held at the University of Central Florida on April 12, 2007, under the co-sponsorship of the Miami-European Union Center.

[♦] Ramon Mullerat OBE is a lawyer in Barcelona and Madrid, Spain; Avocat à la Cour de Paris, France; Honorary Member of the Bar of England and Wales; Honorary Member of the Law Society of England and Wales; Professor at the Faculty of Law of the Barcelona University; Adjunct Professor at the John Marshall Law School, Chicago; Member of the European Board of the Emory University (Atlanta); Former President of the Council of the Bars and Law Societies of the European Union (CCBE); Member of the American Law Institute (ALI); Member of the American Bar Foundation (ABF); Member of the Council of the Institute of North-American Studies (IEN); Member of the Council of the Section of International Law of the American Bar Association (ABA); Former Co-Chairman of the Human Rights Institute (HRI) of the International Bar Association (IBA); Member of the Council of Justice of Catalonia; Member of the London Court of International Arbitration (LCIA); Former Chairman of the Editorial Board of the European Lawyer; Member of the Editorial Board of the Iberian Lawyer.

[1] Jean-Christophe Rufin, Globalia, 2004.

[2] George Elliot, Felix Holt, 1866.

privacy by the government, corporations or individuals is part of many countries' laws, and in some cases, constitutions or privacy laws.

The right to privacy is not new but it was not recognized until late in history. Already in 1890, Warren and Brandeis[3] stated that "the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses "vi et armis". Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible … Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed …"
If one hundred years ago privacy was felt to be attacked by instantaneous photographs, circulation of portraits and newspapers, with the advance of communication and particularly the electronic revolution, the situation is extremely serious and preoccupying.

Today it is generally believed that privacy and data protection issues are central in citizens' lives: at work, in their relations with public authorities, in the health field, when they travel or surf the internet. The right to data protection is also the prerequisite for the exercise of other fundamental rights, such as the right to freedom of speech or conscience.

As the EU Parliament has recently recognized[4], there is a growing fear that the technologies of surveillance and law enforcement are becoming so powerful so quickly that society is not getting an opportunity to absorb them safely. Let us hope, however, that George Orwell's Big Brother, Aldoux Huxley' New World or Jean-Christophe Rufin's Globalia remain just imaginary bad dreams.

III. The OECD recommendations

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data. The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;

[3] Warren and Brandeis, "The right of privacy", Harvard Law Review, 15 December 1890, n. 50.
[4] Mark Ballard, "Europe demands say in US data trawling", The Register, 15 February 2007.

6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

The OECD Guidelines were nonbinding, and data privacy laws still varied widely across Europe. However, all seven principles were incorporated into the EU Directives. The US, while endorsing the OECD's recommendations, did not implement them within the US.

IV. Privacy in the EU and the US

1. In the EU

In the last decade privacy and data protection has attracted increasing attention of world society and particularly of the EU. As we will see, the EU has introduced a good number of rules to protect privacy and data protection and is the indisputable leader in the defence of this fundamental right.

In 2007, the Council of Europe celebrated for the first time a Data Protection Day on 28 January. This was the occasion for European citizens to become more aware of personal data protection and of what their rights and responsibilities are in that regard.

In spite of this, a 2003 Eurobarometer survey on the protection of privacy in the EU showed that 70% of European citizens feel they know little about what is done in their country to protect their personal data.

2. In the US

In the "war against terror", the US increasingly requires the collecting and processing of more personal data.

Recently, the US has introduced a new system for screening and profiling of passengers, called the "Automated Targeting System" (ATS). This system scrutinizes all travelers to the US by screening their personal habits, registration numbers of their cars, mode of paying of their tickets, their seating preferences and other travel scores. Based on these records, passengers will be assigned a "risk assignment score", which will be held on file for 40 years. Passengers will not be able to correct or verify their own data, whereas a great range of agencies and individuals may have access to the data base, since ATS is not limited to fighting terrorism and crime.

It is due to the disclosure of the ATS being used by the Department of Homeland Security (DHS) that some organizations like Privacy International and the American Civil Liberties Union have appealed the EU Council, Parliament and Commission and the privacy commissioners in 31 countries[5]. EU Justice Commissioner, Franco Frattini also said that ATS violated the undertakings given by the DHS on the use of passenger data

Google's recent victory in a US court opposing a request to obtain data by the US Department of Justice shows the challenges raised by this massive thirst of accumulating personal data. Conscious of this, the US administration is seeking to improve the situation with some steps: a) the establishment of privacy officers or independent privacy agency, who are to undertake privacy assessments of all initiatives that could impinge on privacy; and b) setting up a mechanism to guarantee US citizens a right of appeal in the event of incorrect use of their data.

[5] Privacy International, 11 January 2007.

V. EU Directives in data protection

The EU has issued a number of rules to regulate the protection of personal data:

1. 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 ("Data Protection Directive").
2. Directive 97/66/EC of the European Parliament and of the Council on the right of privacy.
3. Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
4. Regulation 2001/45 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
5. Directive 2002/58/EC on Privacy and Electronic Communications, as a complement to the existing Framework Data Protection Directive 97/66/EC
6. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC.
7. Communication of 7 March 2007 on the follow-up of the Work Programmed for better implementation of the Data Protection Directive. It concludes that while the Directive should not be amended, there should be a programmed of measures in pursuit of the Directive's proper implementation by member states.
8. New draft of the Framework Decision on data protection in police and judicial cooperation of 13 March 2007.

Special mention needs to be made of the EU Charter of fundamental rights, which set out very clear principles about how personal data should be handled and gave people rights to challenge mishandling of their data.

VI. The EU Data Protection Directive

1. The Directive

In 1995, the EU issued 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 ("Data Protection Directive").

2. Content

The Data Protection Directive regulates the processing of personal data, regardless if the processing is automated or not. It incorporated the OECD Recommendations.

3. Scope

Personal data are defined 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" (art. 2 a). Some examples of personal data are: address, credit card number, bank statements, criminal record, etc.

The notion “processing” means "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" (art. 2 b).

The responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d).

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data (art. 4). Controllers from outside the EU, processing data in the EU, have to follow data protection regulation. In principle, any on line shop trading with EU citizens will process some personal data and is using equipment in the EU to process the data (the customers’ computer). As a consequence, the website operator would have to comply with the European data protection rules. The Directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject.

4. Principles

Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency (the data subject has the right to be informed when his personal data are being processed), legitimate purpose (personal data can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes), and proportionality (personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed).

5. Transfer of personal data to third countries

“Third countries” is the term used to designate countries outside the EU. Personal data may only be transferred to third countries if that country provides an “adequate protection”. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.

The European Commission set up a "Working party on the Protection of Individuals with regard to the Processing of Personal Data" ("Article 29 Working Party"). The Working Party gives advice about the level of protection in the EU and third countries.

6. Implementation by the EU member states

EU directives are addressed to the member states, and are not legally binding for citizens in principle. The member states must transpose the directive into internal law. The Data Protection Directive had to be transposed by the end of 1998. All member states have enacted their own data protection legislation.

7. The Directive and the US

The Data Protection Directive raised many concerns in the US about trans-border movement of personal information. The Directive’s high standard of data privacy protection and restrictions on transfers of data to countries such as the US that might not meet that standard threaten the flow of personal information that is essential to business operations. US organizations doing business in

the EU must therefore decide how to address the challenges posed by the Directive to continued data flows.

Since the US has no equivalent legislation to the EU Data Protection Directive and just relies on a self-regulatory system, the Directive limits the transfer of consumer data in the insurance, financial services, tourism and aviation sectors from the EU to the US6.

As we have seen, the Data Protection Directive prohibits the transfer of personal information from the EU to a non-EU country, such as the US, unless the non-EU country provides "adequate protection" for the information. The Directive also confers certain powers on EU Data Protection authorities to enforce this provision, including the power to levy fines on EU organizations and to order the discontinuation of data flows to foreign countries.

VII. The EU Data Retention Directive

The EU dealt with the security/privacy dilemma once again last year when adopting Directive 2006/24/EC of 15 March 2006 on the retention of data in connection with the provision of publicly available electronic communication services or public communications network in the fight against crime ("Data Retention Directive").

As we have seen, to protect citizens' fundamental rights and freedoms, in 2005 the Data Protection Directive had imposed the obligation to delete traffic data once is no longer needed. But invoking public order to justify further processing of data, retention regimes were introduced by the member states varying with respect to the scope, purpose and duration of the retention. The Directive aims at harmonizing member state provisions concerning the obligation of the providers to retain the data in order to ensure that they are available for the purpose of investigation, detection and prosecution of serious crime. The Directive requires firms to store data that can trace fixed or mobile phone calls, time and duration of calls, location of the phone, connections made to internet, details (but not the content) of internet, e-mail and internet phone services. Records must be kept for 6 to 24 months under he new measures. The data retained can be made available only to competent authorities in accordance with national law. Member states had to bring into force their laws necessary to comply with this Directive by no later than 15 September 2007.

In some EU countries with strong data protection laws like Germany there has been fierce opposition to this Directive. Chambers of commerce and about 10.000 people already have signed in to challenge the upcoming German data retention law for violating the German constitution. The Austrian government is neither in favor of changing core data
protection laws that have been enacted only a few years ago.

The Data Retention Directive has been denounced as representing an attack against fundamental rights reminding Benjamin Franklin's warning that "they that waive essential liberty to obtain a little temporary safety deserve neither liberty nor safety". Many accuse the Directive as illegal in terms of the European Convention of Human Rights, invading the privacy of persons, threatening consumer confidence, burdening EU industry, requiring more invasive laws and, because of the cross-border nature of Internet communications, likely to have negative repercussions for citizens of other countries. Effectively, non-EU law enforcement agencies may seek data held in Europe that they can not obtain at home, either because it is not retained or because their national law does not permit it. Finally, the concern that governments may permit the abuse of the data for other purposes that the ones looked for by the EU legislator is a real concern.

[6] OJ L 281 of 23/11/1995, p.31. available at
http:// europa.eu.int/comm./internal_market/en/media/dataprot/index_en.htm

As convincing of these arguments may be, the Directive strikes a tolerable balance of the fundamental rights of the individuals against the collective right for security. Not perfectly because perfect equilibrium never exists, but acceptably. However, the EU needs to have a broad and open public discussion about how to make sure that the EU laws incorporate safeguards to ensure that law enforcement is provided in data that is relevant and proportionate but not provided with unlimited access to data that most Europeans expect to be kept private[7].

VIII. The Data Protection Day

> Today, it is more important than ever
> that we process personal data according to our European principles.
> The threat presented by terrorist organizations
> creates a new challenge to balance
> with fully respecting privacy and data protection rights[8]

28 of January was declared the Data Protection Day by the Council of Europe. EU Vice-President Frattini, made a statement on the occasion of the first Data Protection Day on 28th January 2007: "Data protection issues affect everyone, but are not always well understood. That is why I welcome and support the Council of Europe's initiative to raise the profile of data protection by declaring 28 January 2007 "Data Protection Day", date of signature of the Convention 108 regulating the processing of personal data".

"We need to balance access to data for those protecting our security and fighting crime with protecting people's privacy rights. This is not a balance which stands still. Rather both sides are able to move forward with technological advances. Today, it is more important than ever that we process personal data according to our European principles. The threat presented by terrorist organizations creates a new challenge to balance with fully respecting privacy and data protection rights. We live in the era of globalization. Technology enables information to circulate round the world in a flash. This technology also enables us to better control access to data and to pinpoint relevant data".

"All individuals in Europe need to be better informed about these issues which are central to their lives. Every time people surf the internet, make travel arrangements, receive health treatment, use their credit card and in countless other transactions, they supply their personal data which, if misused, could result in a serious invasion of their privacy".

"Data protection laws are designed to ensure that personal data is handled with the respect and care it deserves. But legal rights and protections are only useful if people know that they exist and know how to use them. Data Protection Day is an excellent opportunity to engage the people of Europe in the debate and, above all, to make them aware of their rights regarding that most precious of assets – their own private and intimate details".

IX. The European Data Protection Supervisor

The European Data Protection Supervisor (EDPS), an independent authority, has published its annual report. The Supervisor is responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies with respect to the processing of personal data.

According to the report, the EDPS received some 27 complaints last year, although only 5 of them were declared admissible and further examined. In practice, a large majority of complaints

[7] Peter Fleicher, Privacy …?, 11 January 2007.
[8] Franco Frattini, EU Justice Commissionner, 28 January 2007.

received fall outside the area of competence. In such cases, the complainant is informed in a general way and, if possible, advised on a more appropriate alternative.

The report states that considerable efforts were also invested in the elaboration of a background paper on how the two fundamental rights public access to documents and data protection relate in the context of the EU institutions and bodies. Work on another paper, concerning the use of electronic communications is also being carried out by the EDPS[9].

X. The Safe Harbor

As a consequence of the Data Protection Directive, the US Department of Commerce began discussions with the European Commission in 1997 to create a "Safe Harbor" that would enable US organizations to meet the Directive's adequacy requirement. The Safe Harbor discussions concluded in March 2000, and the arrangement was approved in July 2000. The Department of Commerce opened the Safe Harbor for business in November 2000 and began to post a list of participating US companies on its website.

Although the Safe Harbor is operational, the EU promised US organizations a period of "flexible implementation" of the adequacy requirement, so that US organizations can decide whether to enter the Safe Harbor or to determine what other steps they will take to meet the adequacy requirement. Accordingly, all US firms that do business with EU Member States should decide whether to enter the Safe Harbor or take other approaches to ensure continued data flows from the EU.

The problem of exporting personal data from Europe to other countries that do not have adequate data protection continues to concern multinational companies. The EU Data Protection Directive recognizes several methods for exporting data. Consent is one method. Another method is a contractual agreement between a data exporter and its third country affiliate. Contracts are widely used, but they can be cumbersome to manage with multiple parties. The Safe Harbor agreement between the EU and the US provides another way to export data. However, Safe Harbor only works for data moving from Europe to the US, so many corporations do not find it useful.

According to critics the Safe Harbor principles do not provide for an adequate level of protection, because it contains fewer obligations for the controller and allows the contractual waiver of certain rights.

XI. EU and US different perspectives

The EU and the US have different perspectives on privacy and data protection. The US prefers 'sectoral' approach to data protection legislation, relying on a combination of legislation, regulation, and self-regulation, rather than overarching governmental regulations. In his "Framework for Global Electronic Commerce", President Clinton recommended that the private sector should lead, and companies should implement self-regulation in reaction to issues brought on by Internet technology. To date, the US has no single, overarching privacy law comparable to the EU Data Protection Directive. Privacy legislation in the US tends to be adopted on an "as needed" basis, with legislation arising when certain sectors and circumstances require (e.g., the Video Protection Act of 1988, the Cable Television Consumer Protection and Competition Act of 1992, and the Fair Credit Reporting Act). Therefore, while certain sectors may already satisfy the EU Directive, most do not. The reasoning behind this approach has as much to do with American laissez-faire economics as with just different societal values. The First Amendment of the US Constitution guarantees the right to free speech, which necessarily implicates privacy. While free

[9] Elina Miaouli, Europa, 20 April 2006

speech is an explicit right guaranteed by the US Constitution, privacy is an implicit right guaranteed by the Constitution as interpreted by the US Supreme Court.

On the other hand, Europeans are acutely familiar with the dangers associated with uncontrolled use of personal information from their experiences under World War II-era fascist governments and post-War Communist regimes, and are highly suspicious of unchecked use of personal information. In the age of computers, Europeans' guardedness of secret government files has translated into a distrust of corporate databases, and governments in Europe took decided steps to protect personal information from abuses in the years following World War II. Germany and France, in particular, set forth comprehensive data protection laws[10].

Dorothee Heisenberg[11] notes the fundamental differences in US and EU approaches: a) the EU Directive, reflecting national practices in Western European countries (France and Germany) mandates a comprehensive national regulatory scheme enforced by a national data protection commissioner. US data protection is piecemeal. Where regulation exists, there are differences between the handling of public and private sectors, state and federal regimes, and particular industries. Each company or agency is charged with enforcing its own guidelines; b) the EU Directive focuses on direct regulation of the collection and use of personal data, prohibiting "excess" data collection and restricting use to the original and purposes of the collection. Notification to the national authority and to the data subject of the collection and use of the data are required at several stages. The US framework assumes that most data collection and use is acceptable, that guidelines should be primarily voluntary, and that regulation should only address documented instances of abuse. Enforcement in the US depends on the initiation of action by a data subject rather than a government official; c) Heisenberg looks at the political processes and interest groups by which the EU Directive and later the EU bargaining position on Safe Harbor were formulated and compares these to the formulation of the US bargaining position on Safe Harbor. She concludes that the US and EU publics similarly viewed privacy protection as an important government function and therefore that there were no fundamental cultural or historical reasons for the difference in the approaches. Rather, the difference could be attributed to the participation of different interest groups. The EU Directive was primarily formulated by a Working Party of privacy experts and particularly the national Data Protection Commissioners in a process that did not include business interest groups because they were already subject to extensive data protection regulation in member countries and because many had not yet recognized the profitable transfer of data made possible by the Internet. The US position was primarily formulated by business and technology interests under the guidance of the Department of Commerce; d) there are historical and cultural reasons behind these differences, particularly if one looks at political and legal culture, not simply public opinion. Western European countries have regulated the processing of personal data by both public and private entities under the rubrics of 'human dignity' and 'liberty' and these efforts have been furthered by the courts. The US political culture is more dependent on the financial contributions of business interests, and therefore more responsive to these interests, than the Western European political culture of parliamentary systems, multiple parties and limited election periods.

XII. Transfer of passenger reservation data from the EU

1. EU-US agreement on access to EU airlines reservation data

[10] The Register.

[11] Dorothee Heisenberg, Negotiating privacy: the European Union, the United States and personal data protection, Lynne Rienner Publishers, 2005

.

After 9-11, the US adopted a number of laws requiring airlines flying into their territory to transfer to the US administration data relating to passengers flying to or from he US. In particular the US imposed on airlines the obligation to give the US Department of Homeland Security (DHS) electronic access to passenger data contained in the Passenger Name Record (PNR). Airlines not complying with this request may face heavy fines and even lose landing rights as well as seeing their passengers subject to delays. This requirement came into conflict with the 1995 EU Data Protection Directive.

An EU legal framework allowing airlines to transfer PNR was put in place by the EU Commission on 14 May 2004, accompanied by the International Agreement EU-US on 24 May 2004. The PNR included up to 34 pieces of data on each person, including name, reservation date, travel agent, itinerary, form of payment, flight number and seating information[12] [13].

When the International Agreement was first negotiated, it was a highly contentious exercise. The EU insisted that the data from the EU carriers could not be submitted to the US without explicit safeguards. The US authorities were demanding that the data be accessed directly by the CBP officials whilst logging into airline's data bases that data were kept for more than 40 years, and be used for any law enforcement purpose. The EU officials called for stringer protections, limited retention periods, limited access to the data bases (including restricted access to medical and religious information of travelers). Eventually the EU and the US came to the Agreement that permitted for the transfer of data with some safeguards including 3.5 year period of retention, some rights of access by European citizens to correct their data and promises that the data would only be used for combating terrorism and crime and that it would not be used for automated profiling of risk-assessment scoring.

2. The European Court of Justice (ECJ)'s decision

A decision of the ECJ on 30 May 2006[14] annulled the International Agreement as of 30 September 2006. The ECJ was called on to consider whether the transfers of personal data to the US adequately defended privacy and human rights. Instead the ECJ decision focused only on whether the European Commission and the Council had legal authority to complete such an agreement. The Court found that when the Commission declared that the data is adequately protected by the US it was in fact acting beyond the confines of EU law, and when the European Council approved the agreement it did not do so on an appropriate legal basis.

This decision was seen as more than just a technical legal court decision and instead as a chance for a new start on these matters to reconsider and question if personal data should be the currency of international travel, if it is morally right to extend powers created for combating terrorism and then to apply them to other uses, and if privacy and security can be seen as complementary goals instead of how governments are currently dispensing with privacy in the name of security.

3. The new (interim) agreement for sharing airline passenger data

Since the alternative was a patchwork of 25 bilateral agreements, the EU and the US reached an interim agreement on 6 October 2006 on the processing and transfer of PNR data by airlines to the US government. Airlines flying from the EU to the US can transfer passenger information including names, addresses, phone numbers, itineraries and credit card numbers to US

[12] Available at http://ec.europa.eu.justice_home/fsj/privacy/thirdocuntries/index_en.htm

[13] See Art. 29 Working Party, Opinion of 30 September 2004 and Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, 15 February 2007.

[14] Judgment of the Court (Grand Chamber), 30 May 2006 (Protection of individuals with regard to the processing of personal data – Air transport – Decision 2004/496/EC.

government agencies defined in the agreement. This agreement replaces the one of May 2004 reached between the European Community and the US, which was struck down by the ECJ and is set to expire on 31 July 2007. Negotiations over a permanent deal will begin in November 2007.

The deadlock had put airlines in a difficult situation where they had to choose whether to break EU Data Protection Directive or US rules. With no agreement, airlines that continued to transfer data to the US faced the threat of lawsuits in Europe for breaching EU data-privacy rules, and those that refused to pass on information risked heavy fines ($6,000 per passenger) or withdrawal of landing rights if they fly to the US without supplying the data.

The US wanted the information made available automatically to a number of different domestic agencies, but the EU would not allow "unconditional direct electronic access" by agencies such as the FBI and wanted to be sure that if the information did move between agencies then it would remain secure.

The content of the interim agreement does not differ from the 2004 agreement but new principles have been integrated into the text: a) Availability of information: Whereas the 2004 agreement was based on a “pull system” where all legitimate US authorities were allowed to directly extract data from airlines’ databases, the system will now be based on a “push system”, in which US authorities can only request information and airlines have to pass it on. This means that the US CPB no longer has direct access to passenger data – one of the main requests of the European Parliament; b) Comparable standards of data protection: The US had insisted that the DHS’s CBP agency be allowed to share passenger-data freely with other agencies, but only if they have comparable standards of data protection. Under the new agreement, the EU has agreed to allow passenger information to be passed on to other agencies, but without direct electronic access to data. This will allow the EU to ensure that data is only disclosed to other agencies provided that they have comparable levels of data protection as in the EU.
In the present negotiations the US seeks more flexibility regarding how to use the information and to hold the data for longer than it is currently allowed to. The UE seeks to provide less information and for the US to give legally binding commitments in how the data will be used.

With respect to the new agreement currently under negotiation, the chairman of the Article 29 Working Party expressed "concern that also the new agreement will not respect European data protection requirements". He added: "Any new agreement must of course meet legal requirements, but we also have to look at possible technical safeguards, such as anonymising or pseudonominising the data. Wouldn't it be sufficient if the identity of a passenger were revealed to the US authorities only once their screening systems have found indications for a suspect? There must be proof that practices meet the requirements, including the requirement that they are necessary, not just useful for the US side. The way to ensure this is an independent audit of the practices, to be carried out jointly by both sides and including data- protection authorities".

XIII. The SWIFT case

After a national data privacy committee ruled that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) violated EU privacy laws by allowing the US to access its records in the wake of 9/11, the EU and the US have been working to find a solution that better meets the needs of both parties. Apparently SWIFT made a secret deal with the US Treasury to hand over the information mostly because it was operating in a legal black hole. There are no laws that cover which nation has jurisdiction over wireless transfers. The goal is coming up with a common set of guidelines for data privacy rather than renegotiating each international agreement as problems come to light.

SWIFT had handed data containing the details of private international financial transactions to US terrorist finance investigators under a secret arrangement since late 2001. Since the transfers came to light last June, Europe's data protection authorities have declared that SWIFT is a data controller and, as such, it should take responsibility for the privacy of the data it

administers for its banking clients. In open defiance of European privacy officials, SWIFT has declared that it has applied to the US Federal Trade Commission (FTC) for 'safe harbor' protection for the data it holds on US soil.

A main point of contention between SWIFT and the EU authorities is whether it is a financial organization. SWIFT maintains that it a mere messaging service, as it only handles messages that facilitate the international transactions of banks. Hence, it can apply for Safe Harbor. If the FTC has indeed told SWIFT it is eligible for Safe Harbor protection, that could imply that it also accepts its assertion that it is a mere messaging service – financial institutions are not eligible for safe harbor. Yet the EU maintains that SWIFT a financial institution.

According to EU regulators, the only way for SWIFT to avoid infringing data protection law would be to pull its data out of the US. Meanwhile, both sides insist they want to work together to find a solution and they are pinning their hopes on the US and EU agreeing an overarching instrument that would satisfy both anti-terror investigators on the West-side of the ocean and data protection defenders on the East[15].

XIV. Increasing police bodies and Europol powers

> The response adopted by the EU in the face of terrorism must be proportionate and properly targeted on the fight against terrorism, bearing in mind that, until proven otherwise, the most productive measures in the fight against new forms of terrorism are effective intelligence and police services.[16]

The European Parliament has proposed increasing the police body's powers and changing Europol's legal basis in order to give it more powers to fight radical Islamic terrorism, the biggest threat to European security. Its mandate will change, according to the proposals, in a way that will affect how data is exchanged in relation to the European police body.

However, the European Data Protection Supervisor (EDPS) said that Europe's police data protection policies must be more consistent before Europol's powers can be increased. It also said that once more sharing is commonplace, those swapping information must make sure that information collected from commercial activities are accurate, that strict guarantees are given when databases are linked together, and that rules are agreed on in relation to a subject's right of access to the shared information.

The EU is currently discussing a draft Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
The Commission submitted the proposal in October 2005, the European Data Protection Supervisor (EDPS) issued an Opinion in December 2005, the European Parliament agreed its report (with 60 amendments) in May 2006 and adopted it in September 2006, in November 2006 the EDPS issued a second critical Opinion and in December 2006 the European Parliament adopted a report saying that it intended to re-examine the issue as the Council had ignored its views. Between November 2005 and November 2006 the Council's Multidisciplinary Group on Organized Crime produced 29 reports - substantially changing the Commission proposal and ignoring the views of the EDPS and the European Parliament - without reaching agreement on the text.

The proposal is being discussed in the Council by the Multidisciplinary Group on Organized Crime whose primary interest is to ensure the greatest possible powers to exchange any and all data between all agencies - at the national, European and international levels - with the fewest possible obstacles created by data protection rights.

[15] Nick Farrell, 24 November 2006.
[16] EU Parliament.

XV. Towards a global regulation

> Information flows do not recognize international boundaries. The internet is rightly called the World Wide Web. Likewise travel, finance, commerce, telecoms, crime, scams and terrorism all increasingly operate internationally. We can no longer go on with different privacy controls in different parts of the world.[17]

It is clear that the sharing of data and information is a valuable tool in the international fight against terrorism and crime. But it is also clear that an adequate protection of the privacy and civil liberties of citizens is fundamental human rights. A right balance needs to be struck. However the different attitudes towards the two scales of this balance constitute a serious obstacle to this necessary equilibrium.

As the EU Parliament's stresses[18], during the last few years several agreements prompted by US requirements, notably the agreements on PNR, SWIFT and the existence of the US ATS, have led to a situation of legal uncertainty with regard to the necessary data protection guarantees for data sharing and transfer between the EU and the US for the purpose of ensuring public security and, in particular, preventing and fighting terrorism.

With the rise of the global economy, regulatory compliance concerns now extend across borders. More than 50 countries have enacted data protection laws that require organizations in the public and private sectors to safeguard sensitive personal information. Consequently, as organizations enter new geographic markets, or outsource business processes or suppliers to gain a competitive advantage, they need a holistic solution for complying with the myriad privacy laws around the globe.

US privacy officials have made advances about formulating an international data protection law for the era of globalization. The US has been pushing for more widespread data sharing between governments so it can track people it thinks are not safe to travel. But privacy officials in Europe have already hindered US attempts to routinely collect intelligence from foreign commercial databases, such as the passenger name records it takes from airlines and the bank data it took from the Belgian firm SWIFT. Data protection officials from countries outside the US also seem to assume that an international agreement would require the US to meet European standards. Whereas, their previous skirmishes with the US, and a desire among some Europeans to weaken data protection rules to allow less restrained anti-terror investigations, might require the EU take a step down

Many organizations are pressing for a global agreement on inter-government data sharing. The EU Parliament said also that data-sharing programs must at all times be subject to parliamentary scrutiny and judicial review. The UK Information Commissioner recently highlighted[19] the need for the international community to 'Do global privacy better', outlining the benefits of a more harmonized and consistent world-wide approach to protecting people's personal information and regulating privacy laws[20]. Richard Thomas concluded: "Although there

[17] Richard Thomas, Speech at the International Association of Privacy Professionals' Summit in Washington, 9 March 2007.

[18] European Parliament, Motion for a Resolution, 7 February 2007.

[19] Richard Thomas, Speech at the International Association of Privacy Professionals' Summit in Washington, 9 March 2007.

[20] Richard Thomas argued: "We must all do global privacy better. Information flows do not recognize international boundaries. The internet is rightly called the World Wide Web. Likewise travel, finance, commerce, telecoms, crime, scams and terrorism all increasingly operate internationally. We can no longer go on with different privacy controls in different parts of the world. Inconsistencies cause unnecessary confusion and complexity, increased costs and reduced consumer trust and confidence. Privacy has shot up the agenda everywhere and businesses and governments now accept that privacy safeguards for citizens are needed wherever the information goes. Greater consistency – especially between US and EU approaches - will reduce barriers to transferring data and give people better assurances that their

are different political and legal cultures, it is too easy to exaggerate the gap. In fact, there are promising signs of emerging common ground between the US and the EU. Let us concentrate on the substantive agreement about the protections which are needed, rather than the detailed differences about how we regulate. For example, there is already considerable support for a global privacy standard which includes the need for genuine consent to be obtained for the collection, use or disclosure of personal information, a duty of care for personal information and limitations on the use and retention of personal data. It will not be easy to build a greater consensus, but we must make a start".

The EU Parliament and the US Congress are now working together in privacy and security and discussions are in the agenda for the next EU-US summit on 30 April. Let us hope that the summit will constitute a big step towards the global regulation of data protection.

---

personal information is protected wherever it goes. Doing global privacy better means an active commitment to harmonization. Just as it is important that US privacy laws are not discussed in isolation from the rest of the world, so too must the EU be ready to consider changes. There may be scope for less bureaucracy, less emphasis on prior authorization and a more concrete focus on preventing real harm. Richard Thomas's call for a new debate comes in the wake of continuing concerns about cross border privacy issues. For instance, the European Court of Justice ruled last year that in entering into an agreement on transferring airline passengers' personal information to US authorities the European Commission were acting in breach of EU law. There have also been concerns about US authorities gaining access to international financial transactions that are routed through servers in the US".