3 Information society and data protection

Two themes – security and technology – dominated debate in the field of the information society and data protection in 2011, a year which marked 10 years since the terrorist attacks of September 11 in the United States. The anniversary stoked debate on how to find the right balance between security, rights to privacy and data protection and centred on topical issues such as the retention of telecommunications data; the collection and analysis of passenger data; the creation of a terrorist finance tracking system; and the use of body scanners. Another concern was how to update the data protection framework to cope with technological advances, with interest focusing particularly on social networking sites.

This chapter explores key changes in European Union (EU) and Member State legislation, policies and practices in the area of data protection in 2011. The chapter will first look at the main developments at European level and then turn to the year's high-profile topics: data retention, Passenger Name Record (PNR) data, terrorist finance tracking systems, the use of body scanners and social networking sites.

Key developments in the area of information society and data protection:

- courts and parliaments in some EU Member States raise concerns about national legislation implementing the Data Retention Directive; the European Commission adopts, in late 2010, an evaluation report on the directive;
- in the context of Passenger Name Records (PNR), the European Parliament endorses the EU-Australia PNR agreement, while parliamentary approval is pending on the EU-US PNR agreement; the European Commission proposes a directive to exchange PNR data amongst EU Member States for law enforcement purposes;
- the EU institutes new rules on the use of body scanners at European airports. Meanwhile, a number of EU Member States test and evaluate the practical use of these scanners;
- the European Commission presents options for a European terrorist finance tracking system, while the implementation of the existing EU-US cooperation, known as the terrorist finance tracking programme, undergoes two reviews, both calling for more transparency.

3.1. General overview

In November 2010, the European Commission presented its plans in the area of data protection.[1] The communication outlines the Commission's approach to the review of the EU system for the protection of personal data in all areas of EU activities, taking into account the challenges resulting from globalisation and new technologies. Several objectives are set out including: strengthening individuals' rights, increasing transparency and the level of awareness of data protection rights, enhancing individual control over one's data, ensuring free and informed consent, updating the protection for sensitive data and making remedies and sanctions more effective. In his opinion on the communication, the European Data Protection Supervisor called for more ambitious solutions giving citizens better control over their personal data to make the system more effective. He highlighted that the inclusion of police and

1 European Commission (2010a).

justice cooperation in the legal framework was a condition for effective data protection.[2]

The Eurobarometer survey on *Attitudes on Data Protection and Electronic Identity* was published in 2011.[3] One of the key findings of the survey – in which 26,574 Europeans aged 15 and over were surveyed in the 27 Member States – is that three out of four Europeans accept that revealing personal data is part of everyday life, but they are also worried about how companies – including search engines and social networks – use their information. The report reveals that 62 % of people in the EU give the minimum information required so as to protect their identity, while 75 % want to be able to delete personal information online whenever they want to – the so-called 'right to be forgotten'. There is also strong support for EU action: 90 % want to have the same data protection rights across the EU. The survey was conducted between the end of November and mid-December 2010. All interviews were conducted face-to-face in people's homes in the appropriate national languages.

"Over half of the Europeans surveyed say a fine should be imposed on [...] companies (that use people's personal data without their knowledge) (51 %). Four out of ten think such companies should be banned from using such data in the future (40 %), or compelled to compensate the victims (39 %)."

Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union*, Special Brussels, June 2011, p. 190*

In *The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines,*[4] the OECD described current trends in the processing of personal data and the corresponding privacy risks. It highlighted initiatives and innovative approaches to privacy, with a primary focus on economic activities. The OECD also published an economic paper on the regulation of trans-border data flows to address the growing risk to individual privacy posed by the increasing number of Internet-based data transfers in a globalising world economy. The paper took a systematic inventory of regulation at a global level and examined the policies underlying the regulation,[5] aiming to contribute to the debate on future regulation of the trans-border data flow.

At the Council of Europe, the debate on the revision of its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) continued.[6] In the Council of Europe report on the corresponding consultation,[7] respondents pointed to the importance of ensuring consistency with the EU's protection rules. Moreover, the Council of Europe's Committee of Ministers adopted in late November 2010 a Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[8] It aims at defining fair and lawful profiling in full respect of fundamental rights, notably the right to privacy and to the protection of personal data and the principle of non-discrimination. The Council of Europe also published on 20 September 2011 a draft Strategy on Internet Governance (2012-2015) – adopted on 15 March 2012 – mentioning the advancing of data protection and privacy as one of its main objectives. Finally, a review was launched in 2011 of the Committee of Ministers' Recommendations (87) 15 regulating the use of personal data in the police sector and (89) 2 on the protection of personal data used for employment purposes.

At EU level, the role of data protection in the Area of Freedom, Security and Justice prompted interest. A study prepared for the European Parliament addressed the new challenges stemming from data protection policies and systems falling within the scope of police and judicial cooperation in criminal matters.[9] It identified a set of common basic principles and standards for the genuine assurance of data protection in all phases of EU policy making and for the effective implementation of this fundamental right.

The European Data Protection Commissioners' Conference adopted a resolution stressing the need for a comprehensive data protection framework that covers the law enforcement sector.[10]

The Regulation establishing the agency for the operational management of large-scale information technology (IT) systems in the area of freedom, security and justice was adopted on 25 October 2011.[11] The new agency will act as the management authority for large-scale IT systems in the area of freedom, security and justice: the next generation of an EU database that maintains and distributes information on persons and property of interest to national security, border control and law enforcement (SIS II); a visa-data exchange system (VIS); and a European fingerprint database designed to identify asylum seekers and those who are crossing borders irregularly (Eurodac).

On a more general level, the independence of data protection authorities (see Table 3.1 for listing of national Data Protection Authorities) remained a concern. As reported in last year's annual report the Court of Justice of the European Union (CJEU) handed down

2 European Data Protection Supervisor (2011a).
3 European Commission (2011a).
4 Organisation of Economic Co-operation and Development (OECD) (2011a).
5 OECD (2011b).
6 Council of Europe (2011a).
7 Council of Europe (2011b).
8 Council of Europe (2010).
9 Bigo, D. *et al.* (2011).
10 European Data Protection Commissioners' Conference (2011).
11 Regulation (EU) No. 1077/2011, OJ 2011 L 286.

Table 3.1: Bodies required under EU law – data protection authorities, by country

Country	Name of body in English	*Name of body in national (alternative) language*
AT	Austrian Data Protection Commission	*Österreichische Datenschutzkommission*
BE	Commission for the protection of privacy	*Commission de la protection de la vie privée/Commissie voor de bescherming van de persoonlijke levenssfeer/Ausschuss für den Schutz des Privatlebens*
BG	Commission for Personal Data Protection	*Комисията за защита на личните данни*
CY	Commissioner for Personal Data Protection	*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
CZ	The Office for Personal Data Protection	*Úřad pro ochranu osobních údajů*
DE	The Federal Commissioner for Data Protection and Freedom of Information	*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*
DK	Danish Data Protection Agency	*Datatilsynet*
EE	Estonian Data Protection Inspectorate	*Andmekaitse Inspektsioon*
EL	Hellenic Data Protection Authority	*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
ES	Spanish Data Protection Authority	*Agencia Española de Protección de Datos, AEPD*
FI	Office of the Data Protection Ombudsman	*Tietosuojavaltuutetun toimisto, Dataombudsmannens byrå*
FR	National Commission for information technology and freedoms	*Commission Nationale de l'Informatique et des Libertés*
HU	Authority for Data Protection and Freedom of Information	*Nemzeti Adatvédelmi és Információszabadság Hatóság*
IE	Data Protection Commissioner	*An Coimisinéir Cosanta Sonraí*
IT	Data Protection Authority	*Garante per la protezione dei dati personali*
LT	State Data Protection	*Valstybinė duomenų apsaugos inspekcija*
LU	National Commission for the Protection of Data	*Commission nationale pour la protection des données*
LV	Data State Inspectorate	*Datu valsts inspekcija*
MT	Office of the Data Protection Commissioner	
NL	Dutch Data Protection Authority	*College bescherming persoonsgegevens*
PL	The Bureau of the Inspector General for the Protection of Personal Data	*Generalny Inspektor Ochrony Danych Osobowych*
PT	Portuguese Data Protection Authority	*Comissão Nacional de Protecção de Dados*
RO	The National Supervisory Authority for Personal Data Processing	*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*
SE	The Swedish Data Inspection Board	*Datainspektionen*
SI	Information Commissioner	*Informacijski pooblaščenec*
SK	Office for Personal Data Protection of the Slovak Republic	*Úrad na ochranu osobných údajov*
UK	The Office of the Information Commissioner	*Swyddfa'r Comisiynydd Gwybodaeth*

Source: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm as of 31 December 2011

a judgment[12] on the lack of sufficient independence of German data protection authorities at federal state (*Länder*) level and the European Commission referred Austria to the CJEU for a lack of independence of its data protection authority.[13] Discussions on the new Hungarian constitution, which entered into force at the beginning of 2012, centred on the independence of the Hungarian data protection authority. The European Commission launched accelerated infringement proceedings against Hungary on 17 January 2012 over this issue.[14]

> *"The independence of data protection supervisors is guaranteed under Article 16 of the Treaty on the Functioning of the EU and Article 8 of the Charter of Fundamental Rights. In addition, EU rules on data protection (Directive 95/46/EC) require Member States to establish a supervisory body to monitor the application of the Directive acting in complete independence. […] The mere risk of political influence through state scrutiny is sufficient to hinder the independent performance of the supervisory authority's tasks […]"*
>
> *European Commission, Press release IP/12/24, Brussels, 17 January 2012*

12 CJEU, C-518/07, *Commission v. Germany*, 9 March 2010.
13 European Commission (2010b).
14 European Commission (2012).

3.2. Data retention

The EU has a directive in place which requires internet service providers and telephone operators to retain comprehensive traffic data about non-content-related Internet and telephone use. This EU **Data Retention Directive**[15] has been the subject of fundamental rights concerns ever since its adoption in 2006. In April 2011 the European Commission published a report evaluating its implementation and application.[16] The directive itself, according to the report, does not guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data. The Commission says that the directive only sought partial harmonisation of approaches to data retention. It is therefore unsurprising that EU Member States do not share a common approach, even in fields covered by the directive such as retention periods, let alone on issues not covered by the directive, such as who ultimately covers the cost of the obligatory data retention.[17] The Commission concluded that historic communications data were important in criminal investigations, and that therefore the EU should continue to support and regulate data retention as a security measure.

The Commission consulted stakeholders on options for changing the data retention framework. The European Data Protection Supervisor, in his opinion on the *Evaluation Report* of the Directive, concluded that the directive does not meet the requirements imposed by the fundamental rights to privacy and data protection.[18]

> *"[The Data Retention Directive] is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects".*
>
> *European Data Protection Supervisor,* 'The moment of truth for the Data Retention Directive', *Speech given in Brussels on 3 December 2010*

At the national level, Cyprus, the Czech Republic, Germany, the Netherlands, Sweden and Romania also criticised the Data Retention Directive. On 22 March, the Constitutional Court of the **Czech Republic** declared certain national provisions[19] implementing the directive unconstitutional,[20] in proceedings initiated by a group of 51 deputies of the Czech parliament. The Court referred, for example, to a lack of: proportionality in the national provisions' interference with the right to privacy; a clear definition of the purpose of the data retention; an explicit list of institutions authorised to access the data; an obligation to inform affected persons; and appropriate judicial review. In **Cyprus**, the Supreme Court also declared certain national provisions implementing the Data Retention Directive unconstitutional.[21] The case concerned the access of police officers to telecommunications data on the basis of court orders. The court held that the data retention directive does not oblige Member States to enact legislation enabling police access to such data, as this falls outside the scope of the directive. The court also noted that the relevant court orders were issued prior to a constitutional amendment which provides for exceptions to the right to confidentiality of communications.

Two committees of the Senate in the **Netherlands** expressed their disappointment with the European Commission's evaluation of the Data Retention Directive, in a letter to the Minister of Security and Justice on 31 May.[22] The committees took issue with several points. They said that the evaluation was not satisfactory, because it failed to establish the need for the directive and because it paid insufficient attention to the proportionality of data retention. The committees also raised questions about the methodology used and suggested withdrawing the directive.[23]

Germany plans to transpose the Data Retention Directive into German law in line with the directive itself as well as the conditions laid down in a 2010 German Constitutional Court judgment.[24] To date, however, no consensus on a new legislative proposal has been reached. The Research Service of the House of Representatives (*Bundestag*) said that the Data Retention Directive cannot be implemented in a way that is, beyond all doubt, compatible with the Charter on Fundamental Rights in Europe.[25] These doubts centre on the freedom to conduct business since the directive obliges private enterprises to create and maintain cost-intensive structures for the retention of communication data. Another German House of Representatives' (*Bundestag*) study came to the conclusion that data retention has not significantly increased the rate of crimes solved in any EU country.[26] The study pointed out, however, that there are no statistical data available to assess the directive's effect on the crime clearance rate. The Federal Commissioner on Data Protection and Freedom of Information also argued that there is no proof that data retention has significantly increased crime detection rates.[27] The Ger-

15 Directive 2006/24/EC, OJ 2006 L 105.
16 European Commission (2011b).
17 *Ibid.*, p. 31.
18 European Data Protection Supervisor (2010).
19 Czech Republic, Electronic Communication Act No. 127/2005 Coll., Section 97, subsections 3 and 4; the decree implementing the Data Retention Directive.
20 Czech Republic, Constitutional Court, Decision File No. Pl ÚS 24/10, 22 March 2011.
21 Cyprus, Supreme Court, *Christos Matsias and Others*, Apps. 65/2009, 78/2009, 82/2009, 15-22/2010, Decision of 1 February 2011.
22 Netherlands, Senate (2011a).
23 Netherlands, Senate (2011b).
24 Germany, German Constitutional Court, BVerfG, *1 BvR 256/08 vom 2.3.2010*, 2 March 2010.
25 Derksen, R. (2011).
26 Becher, J. (2011).
27 Germany, Federal Commissioner on Data Protection and Freedom of Information (2011).

man federal police have, however, published evidence of the negative impact the absence of data retention has on criminal investigations.[28] The results of a study commissioned by the Ministry of Justice and carried out by the Max Planck Institute for Foreign and International Criminal Law questioned the value added by data retention. The results of this large-scale empirical research were presented to the Committee on Legal Affairs of the German Bundestag on 27 January 2012.[29]

To implement the Data Retention Direction, **Sweden** presented a bill in late 2010 on the retention of traffic data for law enforcement purposes.[30] The Green party, Sweden Democrats and the Left Party, however, pushed through a minority vote, further delaying the directive's transposition. The Parliament will not now consider it before 17 March 2012. Similarly, in **Romania,** the plenum of the Senate unanimously dismissed the new legislative proposal on 21 December 2011, following a 2009 Constitutional Court ruling that the national implementing legislation was unconstitutional.[31]

3.3. Passenger Name Record data

Passenger Name Record (PNR) data is information provided by passengers, and collected by and held in the carriers' reservation and departure control systems. Soon after the terrorist attacks of 11 September 2001, countries outside the EU adopted legislation requiring air carriers operating flights to, from or through their territory to provide their authorities with PNR data stored in their automated reservation systems. Sent well in advance of a flight's departure, PNR data should help law enforcement authorities screen passengers for potential links to terrorism and other forms of serious crime.[32]

EU institutions discussed agreements with various countries on the exchange of PNR data in 2011. The European Parliament endorsed the EU-Australia PNR agreement,[33] while parliamentary approval is pending on the EU-US PNR agreement.[34] These PNR agreements will replace previous agreements from 2008 and 2007, respectively. The European Parliament requested a modification of the draft agreement with the US to reduce the length of data storage and to ensure EU citizens have a right to appeal travel bans linked to PNR data.[35] The European Data Protection Supervisor released opinions in relation to both agreements,[36] welcoming the safeguards on data security and oversight foreseen in both agreements, but expressed some concern regarding general fundamental rights principles such as necessity and proportionality.

The European Commission introduced in February a new proposal for a directive to exchange PNR data amongst EU Member States for law enforcement purposes.[37] The proposed PNR directive picks up a legislative proposal of 2007, namely the PNR Framework Decision,[38] introduced before the Lisbon Treaty entered into force. Several EU bodies questioned the proportionality of the proposal in view of its impact on the right to respect for privacy and the right to protection of personal data (Articles 7, 8 and 52 of the Charter of Fundamental Rights of the EU). The European Data Protection Supervisor pointed out that the necessity and proportionality of this system – which involves large-scale collection of PNR data for the purpose of a systematic assessment of all passengers – must be clearly demonstrated.[39] It made recommendations regarding various aspects of the proposal including: limiting the scope of application; the length of data retention; the list of PNR data stored; enhancing data protection principles; and ensuring an exhaustive evaluation of the system. The Article 29 working party also questioned the necessity and proportionality of PNR systems and requested further clarification as regards the scope of the proposal.[40] The European Economic and Social Committee (EESC) considered the proposal disproportionate because it lacked sufficient justification of the need for the indiscriminate use of the PNR data of all citizens travelling on international flights.[41]

> *"Before submitting new measures, applicable measures on the collection of personal data for law enforcement and migration control purposes should be evaluated and 'security gaps' identified. Any new draft on the transfer of PNR data should include an extended impact assessment with reliable and up-to-date information on the efficiency, financial costs, and consequences with regard to the aforementioned fundamental rights."*
>
> *A letter from the Standing committee of experts on international immigration, refugee and criminal law (Meijers Committee) to Commissioner Cecilia Malström, Reference CM1108, 21 June 2011, available at: www.commissie-meijers.nl*

28 Germany, Ministry of the Interior (2011a).
29 Max Planck Institut für Ausländisches und Internationales Strafrecht (2012).
30 Sweden, Government Offices of Sweden (2010).
31 Romania, Constitutional Court of Romania, decision No. 1258, 8 October 2009.
32 European Commission (2011c), p. 3.
33 European Parliament (2011a).
34 Council of the European Union (2011).
35 European Commission (2011d).
36 European Data Protection Supervisor (2011a); European Data Protection Supervisor (2011b).
37 European Commission (2011c).
38 European Commission (2007).
39 European Data Protection Supervisor (2011a).
40 Article 29 Data Protection Working Party (2011).
41 EESC (2011a).

FRA ACTIVITY

Second opinion on the fundamental rights compliance of a proposal for a PNR data directive

Upon the European Parliament's request, the FRA presented an opinion on the fundamental rights compliance of the European Commission's new proposal for a PNR directive.[42] The FRA had earlier presented a first opinion related to the PNR in October 2008 at the invitation of the Council of the European Union.

This second opinion raises fundamental rights concerns focusing on the risks of indirect discrimination in relation to profiling and the importance of the collection of appropriate statistics to detect this type of indirect discrimination, the requirements of necessity and proportionality for fundamental rights compliance and effective proactive supervision to ensure the rights of passengers. The opinion will feed into the discussions taking place at the Council of the European Union and the European Parliament.

The **United Kingdom** is in support of an EU PNR Directive that includes provision for intra-EU flights. The government believes that "clear Passenger Name Records (PNR) agreements between the EU and third countries play a vital role in removing legal uncertainty for air carriers flying to those countries, and help ensure that PNR information can be shared quickly and securely, with all necessary data protection safeguards in place".[43] The House of Lords European Union Committee (Home Affairs Sub-Committee) said the case for EU-wide legislation is compelling. It is of the opinion that a single legislative measure should cover the collection of PNR data on flights into all the Member States, and the sharing of those data with the authorities of other Member States.[44] Concerns in relation to PNR were addressed in a statement given to the House of Commons by the UK Immigration Minister on 10 May, questioning whether PNR are necessary and proportionate.[45]

In **France**, the Ministry of the Interior indicated that it "actively [supports] the creation of a European PNR", and announced that an "interministerial team had been set up to consider the establishing" of a system "capable of handling PNR data and covering all the countries outside the Schengen area".[46] But critical voices also registered their views. The French data protection authority issued an opinion on 17 February 2011, stressing that despite four years of testing a national precursor to a PNR system, the effectiveness of the system had not yet been clearly demonstrated. It added that "the rate of false alarms remains abnormally high". The French data protection authority, however, expressed its willingness to carry on with the current testing as preparation for a future French platform for PNR data processing in the context of an EU-wide PNR system.[47]

In other Member States, notably Austria, the Czech Republic and Romania, parliaments have expressed doubts with regard to an EU system of PNR data collection and analysis.

Austria takes a skeptical view of the use of PNR data within the EU as an additional tool in the fight against terrorism, an opinion underscored by Members of Parliament from all political parties in April. According to the then Federal Minister of the Interior three conditions needed to be fulfilled before Austria would support such a system: solutions must be in conformity with human rights; the use of PNR data must be of significant added value to the fight against terrorism; and financial and personal resources have to be proportionate to the value of the system.[48] The Austrian Data Protection Board (*Datenschutzrat*) issued a statement on the EU proposal for a PNR Directive in February 2011, saying that storing personal data of all passengers independent of any suspicion constitutes an interference with the right to privacy. In such cases, the legislator needs to substantiate the adequacy and necessity of such infringements. The EU proposal does not prove such adequacy and necessity, the Data Protection Board added. [49]

In the first half of 2011, the Senate [50] and the Chamber of Deputies of the **Czech Republic**[51] called on the government to adhere carefully to constitutional guarantees on the right to privacy when drafting the PNR proposal. In the opinion of both legislative Chambers, crimes related to the use of Passenger Name Record data should be defined in more detail to ensure proportionality. They also pointed out the absence of further regulation related to the form in which the data are retained and said that the retention period was inappropriate. The two chambers also declined to extend the obligation to store and transmit data on flights between EU countries.

The **Romanian** Senate (*Senatul*) issued an opinion regarding the proposed PNR Directive,[52] finding it in compliance with the principle of subsidiarity but not

42 European Commission (2011c).
43 United Kingdom, Home Office (2011a).
44 United Kingdom, House of Lords (2011), p. 7.
45 United Kingdom, Home Office (2011b).
46 France, Le Fur (2010).
47 France, Data Protection Authority (2011).
48 Austria, Parliament (2011).
49 Austria, Data Protection Board (2011).
50 Czech Republic, Senate, Resolution No. 207, 28 April 2011.
51 Czech Republic, Chamber of Deputies, Resolution No. 446, 28 April 2011.
52 European Commission (2011c).

with that of proportionality. The Senate based the latter opinion on its view that the definitions of some of the data types requested for collection are unclear and that any decision with a serious impact should not be taken based on automatic processing of PNR data.[53] Similar concerns were also voiced in Lithuania,[54] Portugal[55] and Germany.[56]

The debate on the fundamental rights compliance of the proposed EU PNR system is likely to continue in 2012.

3.4. Terrorist Finance Tracking Programme

The Terrorist Finance Tracking Programme (TFTP) has unleashed another important EU debate that requires a balance to be found between data protection and security concerns. These plans concern the provision to security services of financial transaction data from certain financial messaging services, which are secure platforms developed for intra- and inter-bank applications. The basic idea is to fight terrorism by following the money trail via common messaging data standards developed for financial transactions worldwide. The Terrorist Finance Tracking Program was originally a US government programme and part of its 'Global War on Terrorism'.

The EU-US TFTP Agreement,[57] which entered into force in 2010, tasks Europol with verifying whether the US requests are proportionate and necessary according to conditions laid down in the agreement. The agreement sets up a periodic joint review mechanism entrusted with the task of monitoring the implementation and effectiveness of the agreement, including Europol's role under the latter.[58] In November 2010 Europol's Joint Supervisory Body (JSB) carried out an inspection and found that the written requests Europol received were not specific enough to allow it to decide whether to approve or deny them. Nevertheless, Europol approved every request received.

"Europol advised that orally-provided information plays a role in its verification of each request. [...] The significant involvement of oral information renders proper internal and external audit, by Europol's Data Protection Office and the JSB respectively, impossible."

The president of the Joint Supervisory Body (JSB) on 2 March 2011

When discussing the JSB's report on 16 March in the European Parliament Committee on Civil Liberties, Justice and Home Affairs, Members of the European Parliament raised serious data protection concerns. The committee's reaction was one of "dissatisfaction, unrest and discomfort" said the committee chair adding that "the EP [European Parliament] has to exert control on the implementation of this agreement".[59] According to the Federal Data Protection Authority in **Germany** most financial messaging data transmitted to the US authorities, where they are stored for many years, are unrelated to international terrorism, and risk being used for other purposes. In the view of the Federal Data Protection Authority Europol, the monitoring authority of the data exchange with the US according to the agreement, is not an appropriate guarantor as it also profits from the data exchange.[60]

The European Commission published the first joint EU-US review of the TPTP carried out according to the agreement in March.[61] The joint review report concluded that Europol had taken its tasks most seriously, and had put in place the necessary procedures to execute them in a professional manner and in accordance with the agreement. It, however, concurred with the JSB that "there seems to be scope to provide more detailed and targeted justifications for the requests" in order to enable Europol "to perform its functions even more effectively".[62] The joint report also issued several recommendations in order to further improve the application of the agreement, concluding in particular that more transparency on the added value of the programme to the fight against terrorism, on the overall volumes of data concerned and on other relevant aspects would go a long way toward convincing a wider audience of the real benefits of the TFTP and the agreement, as well as raise the level of trust towards the programme, and that such transparency should be sought wherever possible without endangering the effectiveness of the programme.

In response to an invitation by the European Parliament and the Council of the European Union, the European Commission presented different options for a European Terrorist Finance Tracking System in July.[63] The Commission's communication was discussed once briefly in the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, but not dealt with further. The Council of the European Union held several rounds of discussions, including at ministerial level, with key considerations being the costs of a future EU TFTS and its compatibility with the existing agreement with the US.

53 Romania, Senate of the Romanian Parliament (2011).
54 Lithuania, Committee on European Affairs of the Seimas (2011).
55 Portugal, Data Protection Authority (2011).
56 Germany, Federal Commissioner on Data Protection and Freedom of Information (2011), p. 145.
57 European Union, United States of America (2010).
58 Europol Joint Supervisory Body (2011).
59 European Parliament (2011b).
60 Germany, German Federal Commissioner on Data Protection and Freedom of Information (2011).
61 European Commission (2011e).
62 *Ibid.*, p. 12.
63 European Commission (2011f).

The Communication stresses the need to fully comply with fundamental rights, namely the right to data protection. At EU Member State level, there is no consensus yet on the issue. The government of the **United Kingdom** stressed that it is committed to engaging fully with the existing TFTP, but considers that the fundamental question of the reason for establishing an EU TFTS is yet to be adequately answered. According to the Federal Data Protection Authority in **Germany,** the European Commission proposal would follow similar principles as the EU-US agreement and would lead to a mass storage of data of mostly unsuspicious persons.[64]

3.5. Body scanners

The use of body scanners (or 'security scanners' – the term used by the European Commission in its 2010 Communication *on the Use of Security Scanners at EU airports*)[65] was a controversial topic in 2011 due to the implications of their use for human dignity and privacy. The European Parliament[66] and the European Economic and Social Committee[67] held hearings on the matter. At the end of 2011, the European Commission adopted legislation on the use of body scanners at EU airports.[68] The European Data Protection Supervisor criticised the adoption of the new legislation via a regulatory procedure, because the proposals are not merely technical but have an impact on fundamental rights.[69]

FRA ACTIVITY

Body scanners and fundamental rights

The FRA presented its paper *The use of body scanners: 10 questions and answers* at a European Economic and Social Committee hearing in January 2011. The paper suggested the following practical steps to safeguard passengers' fundamental rights: consulting images by a screener remote from the person under examination, with no storage or archiving of pictures; blurring the face of the person screened to render the images obtained anonymous; using mimic boards to display results instead of images. Passengers should be given a choice, the paper suggested, between being screened by body scanners or more conventional security checks like pat downs. Passengers should also receive full information in advance to enable them to make an informed choice.

The legislation allows EU Member States and airports to deploy and use body scanners as one possible method to screen passengers at EU security checkpoints under specific conditions that address fundamental rights concerns. Security scanners should not, for instance, store, retain, copy, print or retrieve images; any unauthorised access and use of the image is prohibited and shall be prevented; the human reviewer analysing the image should be in a separate location and the image should not be linked to the screened person and others. Passengers must be informed about conditions under which the security scanner checks take place. In addition, passengers are given the right to opt out of a scanner check and choose an alternative method of screening.[70]

> *"Security scanners are not a panacea, but they do offer a real possibility to reinforce passenger security. Security scanners are a valuable alternative to existing screening methods and are very efficient in detecting both metallic and non-metallic objects. It is still for each Member State or airport to decide whether or not to deploy security scanners, but these new rules ensure that where this new technology is used, it will be covered by EU wide standards on detection capability as well as strict safeguards to protect health and fundamental rights."*
>
> *Vice-President Siim Kallas, EU Commissioner responsible for transport, Press release IP/11/1343, 14 November 2011*

EU Member States approaches are expected to continue to differ. In **Italy**, for instance, a second testing phase was launched at the beginning of 2011 in three airports (Rome Fiumicino, Milan Malpensa and Venice) using a new technology,[71] but it had only been implemented, as of May, in two of the three (Rome and Milan).[72] The first testing phase took place in 2010 (Rome Fiumicino, Milan Malpensa, Venice and Palermo). According to the National Body for Civil Aviation,[73] the "tested security scanners do not have any impact on health and ensure the respect of privacy for passengers." But the results produced were only partially those that had been expected, it said, given false alarms and long check-in times. The **German** Federal Minister of the Interior decided that, based on field testing, full-body scanners would not be used at airports in Germany for now. It became apparent during the field testing of two full-body scanners at Hamburg Airport, that the technology was not yet at a stage where the available devices were suitable for everyday use.[74] Body scanners, according to the Data Protection Commissioner, may lawfully be used only under the condition that the data are not stored, and that the image of the body contours is not visible on the screen.[75]

64 Germany, Federal Commissioner on Data Protection and Freedom of Information (2011).
65 European Commission (2010c).
66 Committee on Civil Liberties, Justice and Home Affairs (LIBE) (2010).
67 EESC (2011b).
68 Commission Regulation (EU) No. 1141/2011; Commission Implementing Regulation (EU) No. 1147/2011.
69 European Data Protection Supervisor (2011c).
70 European Commission (2011g).
71 Italy, National Body for Civil Aviation (2010).
72 Italy, National Body for Civil Aviation (2011).
73 *Ibid.*
74 Germany, Ministry of the Interior (2011b).
75 Germany, German Federal Commissioner on Data Protection and Freedom of Information (2011).

Concerns relating to the right of privacy, data protection, dignity and possible health risks were also voiced in Sweden[76] and in Slovenia.[77]

3.6. Social networking services

The use, retention and transfer of personal information by social networking services has become another key issue in the public debate given the personal nature of the information involved and the resulting implications for the right to privacy.

Data protection authorities in the Nordic countries sent some 40 questions to Facebook about how the company handles personal data. Facebook responded in September.[78] Facebook confirmed that the company could use information from users' status updates and 'like' buttons to display targeted advertising. The company said, however, that it does not disclose any personal information to other companies, other than the data the user agrees to supply in the process of installing apps. Facebook considers that by having its European headquarters in Ireland the company is subject to European data protection laws.[79]

An Austrian group called 'Europe versus Facebook', seeing their right to privacy violated, lodged 22 complaints against Facebook Ireland, which is responsible for all Facebook activities outside the US and Canada, with the Irish Data Protection Commissioner in August. The complaints include the following allegations: the 'like' button creates data that can be used to track users; tags can be applied without the consent of the user; and 'pokes', posts, pictures and messages can still be seen after deletion.[80] In September, the Irish Data Protection Commissioner announced plans to conduct an investigation into these complaints.[81] Given that Facebook's International Headquarters are in Ireland, the Irish Data Commissioner will examine all activities which are subject to Irish and European Data Protection laws. Any decision it takes could have implications for millions of users worldwide.

The following issues led to concern in the EU Member States with regard to social networking services: uncertainty about the private or public status of statements made on social networking sites; the creation of profiles and tracking of users by social networking sites; the lack of protection of children by social networking sites.

76 Sweden, Committee of Justice, Swedish parliament (2010).
77 Slovenia, Ministry of the Interior (2010); Slovenia, Information Commissioner (2011).
78 Norway, Data Inspection Board (2011).
79 Sweden, Data Inspection Board (2011).
80 For more information, see: www.europe-v-facebook.org.
81 See also: http://m.zdnet.com/blog/facebook/irish-data-protection-commissioner-to-begin-facebook-audit/4262, accessed on 14 October 2011.

In **France**, the industrial tribunal in Boulogne-Billancourt ruled on 19 November 2010 in a case about the public nature of statements made on social network sites. The case concerned three employees who were dismissed for having criticised their managers on Facebook.[82] The court considered that the comments posted on the social networking site were available to the public as they were accessible to 'friends of friends'. The posts were no longer private as they were accessible to persons not involved in the discussion. Therefore, the dismissal was deemed founded. There is, however, some uncertainty with relation to the case law in this matter. The prosecutor of Périgueux, for example, handled a similar case differently. The prosecutor felt that the statements made by two employees about their superiors were sufficiently protected to be viewed as private, visible only to the employee's contacts, and not the 'second circle of contacts'.[83] In response to this legal uncertainty, sector operators reacted quickly. On 30 June, Google launched the Google+ network, another social networking service, where messages carry different levels of privacy depending on various 'circles', as defined by the user. On 13 September, Facebook launched new tools allowing users to organise their lists of 'friends' to better manage what information is shared.[84] Nevertheless, the public or private nature of messages posted on social networking sites remains relatively uncertain.

German websites based in the province of Schleswig-Holstein had until the end of September to remove Facebook's 'like' button or face a fine of up to €50,000 following an intervention by the Independent Centre for Data Protection Schleswig-Holstein. The concern was that this service was used to track users and create user profiles.[85]

> *"The wording in the conditions of use and privacy statements of Facebook does not begin to meet the legal requirements relevant for compliance of legal notice, privacy consent and general terms of use."*[88]
>
> *Germany, Independent Centre for Data Protection Schleswig-Holstein*

The **Spanish** data protection authority expressed its concern about the increased number of reported violations of privacy in social networks, in particular with regard to children (40 in 2010 against 32 in 2009). To address the issue, the Spanish data protection authority met with important social networks, such as Tuenti and Facebook, to improve their privacy policies and to prevent children under 14 years of age from joining

82 France, Boulogne-Billancourt Industrial Tribunal, 19 November 2010, *Mme. B. v. SAS Alten Sir; Mme. S. v. SAS Alten Sir.*
83 Le Monde (2011a).
84 Le Monde (2011b).
85 Germany, Data Protection Commissioner Schleswig-Holstein (2010).

them. Tuenti responded by saying it would review up to 300,000 profiles a year, taking out the profiles of children under the age of 14. Facebook, at the Spanish data protection authority's request, announced that it would increase the minimum age to join its network from Spain to 14. In addition, Facebook also promised to develop better controls and to consider several options to implement an age-verification system along with a parental consent system.[87]

Outlook

Striking a balance between fundamental rights obligations and security concerns will continue to pose a challenge for EU institutions and EU Member States. The on-going discussion on the Data Retention Directive will be one facet of this wider debate.

EU institutions will also continue to debate the EU framework in the area of data protection. The European Commission tabled proposals in January 2012 to reform the existing framework. They consist of a proposal for a regulation replacing the 1995 data protection directive and a proposal for a new directive setting out rules on the protection of personal data processed for the purposes of the prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The attitude towards data protection of both users and providers of social platforms and other online tools will continue to fuel public debate and is likely to increasingly become the subject of court deliberations. The availability and uptake of redress mechanisms will need to be examined closely to ensure that fundamental rights are fully respected in the use of new information and communication technologies.

The CJEU is likely to once more address another area of concern, the independence of data protection authorities.

86 *Ibid.*
87 Spain, Spanish Data Protection Agency (2011a), p. 28.

References

Article 29 Data Protection Working Party (2011), *Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, 00664/11/EN WP 181, 5 April 2011.

Austria, Data Protection Board (*Datenschutzrat*) (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime – Comments of the Data Protection Board (*Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdaten für die Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Richtlinie EU-PNR): Stellungnahme des Datenschutzrates*).

Austria, Parliament (*Parlament*) (2011), Annexes to the stenographic protocol of the XXIV legislative period of the National Assembly of the permanent board of the main board regarding issues of the European Union (*V-19 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV.GP – Beratungen des Ständigen Unterausschusses des Hauptausschusses in Angelegenheiten der Europäischen Union*), 5 April 2011.

Becher, J. (2011), *Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedsstaaten*, WD 7 – 3000 – 036/11, March 2011.

Bigo, D., Carrera, S., González Fuster, G., Guild, E., De Hert, P., Jeandesboz, J., Papakonstantinou, V. (2011), *Towards a new EU legal framework for data protection and privacy: challenges, principles and the role of the European Parliament*, EP studies, Brussels, 15 September 2011.

Commission Implementing Regulation (EU) No. 1147/2011 of 11 November 2011 amending Regulation (EU) No. 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ 2011 L294/7.

Commission Regulation (EU) No. 1141/2011 of 10 November 2011 amending Regulation (EC) No. 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ 2011 L 293/22.

Committee on Civil Liberties, Justice and Home Affairs (LIBE) (2010), *Meeting of the Committee on Civil Liberties, Justice and Home Affairs on recent developments in Counter-terrorism policies*, European Parliament, Brussels, 27 January 2010.

Council of Europe (2010), Recommendation of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec(2010)13, 23 November 2010.

Council of Europe (2011a), The Consultative Committee of the Convention with regard to automatic processing of personal data (STE No. 108) T-PD (2011) Roadmap, 19 April 2011.

Council of Europe (2011b), *Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data*, T-PD-BUR(2011) 10 en, Strasbourg, 21 June 2011.

Council of the European Union (2011), *Agreement between the United States of America and the European Union on the use and transfer of PNR data to the United States Department of Homeland Security*, 17434/11, 8 December 2011.

Court of Justice of the European Union (CJEU) Joined Cases C-468/10 and C-469/10, *ASNEF and FECEMD v. Administracion del Estado*, 24 November 2011.

CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs*, 24 November 2011.

Czech Republic, Electronic Communication Act (*Zákon o elektronických komunikacích*) No. 127/2005 Coll.

Czech Republic, Chamber of Deputies, Resolution No. 446, 28 April 2011.

Czech Republic, Constitutional Court (*Ústavní soud*), Decision File No. Pl ÚS 24/10, 22 March 2011.

Czech Republic, Senate, Resolution No. 207, 28 April 2011.

Cyprus, Supreme Court, *Christos Matsias and Others*, Apps. 65/2009, 78/2009, 82/2009, 15-22/2010, Decision of 1 February 2011.

Derksen, R. (2011), *Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta*, WD 11 – 3000 – 18/11, February 2011.

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, OJ 1995 L 281.

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 amending Directive 2002/58/EC, OJ 2006 L 105.

European Commission (2007), *Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, Brussels, 6 November 2007.

European Commission (2010a), *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4 November 2010.

European Commission (2010b), *Data Protection: Commission to refer Austria to Court for lack of independence of data protection authority*, Press release, IP/10/1430, 28 October 2010.

European Commission (2010c), *Communication from the Commission to the European Parliament and the Council on the use of security scanners at EU airports*, COM(2010) 311 final, Brussels, 15 June 2010.

European Commission (2011a), *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 359, Brussels, 16 June 2011.

European Commission (2011b), *Evaluation report on the Data Retention Directive* (Directive 2006/24/EC), COM(2011) 225, Brussels, 18 April 2011.

European Commission (2011c), *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February 2011.

European Commission (2011d), *Draft Agreement on the use of PNR between the EU and the United States*, SJ (2011) 603245, Legal service, 18 May 2011.

European Commission (2011e), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Commission staff working paper*, SEC(2011) 438 final, Brussels, 30 March 2011.

European Commission (2011f), *A European terrorist finance tracking system: available options*, COM(2011) 429 final, Brussels, 13 July 2011.

European Commission (2011g), 'Aviation security: Commission adopts new rules on the use of security scanners at European airports', Press release, IP/11/1343, 14 November 2011.

European Commission (2012), 'European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary', Press release IP/12/24, Brussels, 17 January 2012.

European Data Protection Commissioners' Conference (2011), *Resolution on the need for a comprehensive data protection framework,* Brussels, 5 April 2011.

European Data Protection Supervisor (2010), *The moment of truth for the Data Retention Directive*, Speech, Brussels, 3 December 2010.

European Data Protection Supervisor (2011a), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union'*, 14 January 2011.

European Data Protection Supervisor (2011b), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security*, 9 December 2011.

European Data Protection Supervisor (2011c), *Letter of Mr Giovanni Buttarelli, Assistant Supervisor, to Mr Sim Kallas, Vice-President of the European Commission*, 17 October 2011.

European Economic and Social Committee (EESC) (2011a), *Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, SOC 414, 5 May 2011.

EESC (2011b), *Report of the Public Hearing on the use of security scanners at EU airports,* Brussels, 11 January 2011.

European Parliament (2011a), *Legislative resolution on the draft Council decision on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service,* P7_TA-PROV(2011)0470, 27 October 2011.

European Parliament (2011b), 'SWIFT implementation report: MEPs raise serious data protection concerns', Press release, 16 March 2011.

European Union, United States of America (2010), *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program,* OJ 2010 L 195/5.

Europol Joint Supervisory Body (2011), *US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles*, Press release, Brussels, 2 March 2011.

France, Boulogne-Billancourt Industrial Tribunal, 19 November 2010, *Mme. B. v. SAS Alten Sir.*

France, Boulogne-Billancourt Industrial Tribunal, 19 November 2010, *Mme. S. v. SAS Alten Sir.*

France, Data Protection Agency (*Commission nationale de l'informatique et des libertés*, CNIL) (2011), *Délibération n° 2011-048 du 17 février 2011 portant avis sur un projet d'arrêté modifiant l'arrêté du 28 janvier 2009 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 et visant à proroger l'expérimentation du « fichier des passagers aériens » (FPA) jusqu'au 31 décembre 2011 (demande d'avis n° 1183168V2)* CNIX1108803X, 31 March 2011.

France, Le Fur (2010), *Written question No. 91193 from M. Marc Le Fur to the Minister of the Interior, Overseas Departments and local authorities, 19 October 2010, answer of the Minister of the Interior, Overseas Departments and local authorities*, available at: http://questions.assemblee-nationale.fr/q13/13-91193QE.htm.

Germany, Data Protection Commissioner Schleswig-Holstein (*Landesdatenschutzbeauftragte Schleswig-Holstein*) (2010), *Sicherheits- und Datenschutzziele miteinander in Einklang bringen*, Interview, 17 September 2010.

Germany, German Constitutional Court (*Bundesverfassungsgericht*), BVerfG, *1 BvR 256/08 vom 2.3.2010*, 2 March 2010.

Germany, German Federal Commissioner on Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) (2011), Annual Report 2009/10.

Germany, Ministry of the Interior (*Bundesministerium des Innern*) (2011a), *Studie des BKA bekräftigt Notwendigkeit von Mindestspeicherfristen.*

Germany, Ministry of the Interior (*Bundesministerium des Innern*) (2011b), 'Körperscanner im Test: Leistungsfähig, aber noch nicht flächendeckend einsetzbar', Press release, 31 August 2011.

International Conference of Data Protection and Privacy Commissioners (2010), Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data, 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27–29 October 2010.

Italy, National Body for Civil Aviation (*Autorità per l'Aviazione Civile*) (2010), 'In ENAC riunione cisa sui security scanner (body scanner): terminate prima fase sperimentazione senza risultati attesi', Press release, 19 December 2010.

Italy, National Body for Civil Aviation (*Autorità per l'Aviazione Civile*) (2011), 'Messa a punto dei security scanner L3 provision sugli aeroporti di Roma Fiumicino e Milano Malpensa', Press release, 9 May 2011.

Le Monde (2011a), 'Can you insult your boss on Facebook?', 10 March 2011.

Le Monde (2011b), 'Facebook proposes to organise lists of friends', 14 September 2011.

Lithuania, Committee on European Affairs of the Seimas (*Lietuvos Respublikos Seimo Europos reikalų komitetas*) (2011), *Komiteto Išvados*, 2011.

Max-Planck-Institut für Ausländisches und Internationales Strafrecht (2012), *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO*, Forschungsbericht im Auftrag des Bundesministeriums der Justiz, 27 January 2012.

Netherlands, Senate (*Eerste Kamer der Staten-Generaal*) (2011a), *E110022 - Evaluatierapport over de dataretentierichtlijn.*

Netherlands, Senate (*Eerste Kamer der Staten-Generaal*) (2011b), *Korte aantekeningen*, 5 July 2011.

Norway, Data Inspection Board (2011), *Facebook's Response to Questions from the Data Inspectorate of Norway, September 2011.*

Organisation of Economic Co-operation and Development (OECD) (2011a), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers No. 176, 6 April 2011.

OECD (2011b), Christopher Kuner, *Regulation of transborder data flows under data protection and privacy laws*, OECD Digital Economy Paper No. 187, 8 December 2011.

Portugal, Data Protection Authority (*Comissão Nacional de Protecção de Dados*) (2011), Parecer No. 39, 9 May 2011.

Regulation (EC) No. 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency, OJ 2004 L 77.

Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) OJ 2008 L 218.

Regulation (EU) No. 1077/2011 of the European Parliament and of the Council establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2011 L 286.

Romania, Constitutional Court of Romania, decision No. 1258, 8 October 2009.

Romania, Senate of the Romanian Parliament (2011), *Reasoned Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)*, 6 April 2011.

Slovenia, Ministry of the Interior (*Ministrstvo za notranje zadeve*) (2010), 'State Secretary Goran Klemenčič Attends Informal Meeting of Justice and Home Affairs Council in Toledo', Press release, 21 January 2010.

Slovenia, Information Commissioner (*Informacijski pooblaščenec*) (2011), Interview with a representative, 7 October 2011.

Spain, Spanish Data Protection Agency (*Agencia Española de Protección de Datos*) (2011), *Memoria 2010*, AEPD, 2011.

Sweden, Committee of Justice, Swedish parliament (2010), *Proposals for parliamentary resolution on the use of body scanners at EU airports* (2010/11:JuU4), 23 November 2010.

Sweden, Government Offices of Sweden (*Regeringskansliet*) (2010), *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv*, Prop. 2010/11:46 2006/24/EG.

Sweden, Data Inspection Board (*Datainspektion*) (2011), *Facebook svarar de nordiska länderna*, 20 September 2011.

United Kingdom, House of Lords (2011), *The United Kingdom Opt-in to the Passenger Name Record Directive,* European Union Committee, 11th Report of Session 2010–11, HL Paper 113, The Stationery Office, London, 11 March 2011.

United Kingdom, Home Office (2011a), *The UK's Opt-in to Council Decision to Sign and Conclude the EU-Australia PNR Agreement*, Written Ministerial Statement, 5 September 2011.

United Kingdom, Home Office (2011b), 'EU Directive on Passenger Name Records', Press release, London, 10 May 2011.

United Kingdom, European Scrutiny Committee (2011c), *Terrorist Finance Tracking Systems*, London, 20 September 2011.

UN & CoE

January

February

March

April

May

21 June – The Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe issues a report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data

June

July

August

September

October

November

December

EU

January

2 February – European Commission adopts a proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

February

16 March – European Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program

March

18 April – Evaluation report from the European Commission to the Council and the European Parliament on the Data Retention Directive

April

May

16 June – Publication of Special Eurobarometer survey 359 on attitudes on data protection and electronic identity in the European Union

June

13 July – European Commission adopts a Communication on a European terrorist finance tracking system: available options

July

August

26 September – The Council of Ministers of the European Union gives its consent to the European Commission's proposals regarding the use of body scanners at EU airports

29 September – Signature of the EU-Australia agreement on Passenger Name Records (PNR)

September

25 October – Regulation of the European Parliament and of the Council establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

27 October – European Parliament adopts a legislative Resolution on the draft Council decision on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service

October

10 November – European Commission adopts a Regulation amending the regulation supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports

11 November – European Commission adopts an implementing Regulation concerning the common basic standards on civil aviation security as regards the use of security scanners at EU airports

24 November – The Court of Justice of the European Union issues judgments in two cases relevant to data protection and information society: *ASNEF and FECEMD v. Administración del Estado* and *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs*

November

13 December – European Council gives the green light for the EU-US PNR agreement

December