UN & CoE

January

February

March

9 April – CoE Parliamentary Assembly adopts Resolution 1986 (2014) on improving user protection and security in cyberspace, as well as Resolution 1987 (2014) on the right to internet access

16 April – CoE Committee of Ministers adopts a recommendation on a 'Guide to human rights for internet users', to help them better understand their human rights online and what they can do when these rights are challenged

April

2 May – CoE Committee of Ministers adopts a recommendation urging member states to protect whistleblowers and journalists

May

26 June – UN Human Rights Council adopts a resolution on the promotion, protection and enjoyment of human rights on the internet

30 June – UN High Commissioner for Human Rights submits a report to the UN General Assembly on the right to privacy in the digital age

June

July

August

18 September – In *Brunet v. France* (No. 13327/04), the ECtHR rules that keeping details recorded in a crime database after the discontinuance of criminal proceedings without the real possibility of deletion violates the right to respect for private and family life (Article 8) of the ECHR

23 September – Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism submits a report to the UN General Assembly on the *Promotion and protection of human rights and fundamental freedoms while countering terrorism*

24 September – UN Security Council adopts Resolution 2178 (2014), dealing with measures to prevent movement and recruitment of foreign fighters and calling in particular on member states to exchange travel information

September

October

November

18 December – UN General Assembly adopts Resolution 69/166 on the right to privacy in the digital age

December

EU

January

12 February – European Commission issues a communication on *Internet policy and governance. Europe's role in shaping the future of internet governance*

20 February – European Data Protection Supervisor adopts an opinion on the European Commission communications *Rebuilding trust in EU–US data flows* and the *Functioning of the safe harbour from the perspective of EU citizens and companies established in the EU*

February

12 March – European Parliament adopts a resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights

12 March – European Parliament approves MEPs' reports endorsing the data protection reform

March

8 April – In *Digital Rights Ireland and Seitlinger and Others* (Joined cases C-293/12 and C-594/12), the CJEU invalidates the Data Retention Directive (2006/24/EC)

8 April – In *European Commission v. Hungary* (C-288/12), the CJEU rules that the government's premature termination of the Hungarian Data Protection Commissioner's term in office breaches EU law

10 April – Article 29 Working Party adopts an opinion on surveillance of electronic communications for intelligence and national security purposes

April

12 May – Council of the EU adopts Guidelines on freedom of expression online and offline

13 May – In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos* (C-131/12), the CJEU declares that an internet search engine operator is responsible for its processing of personal data that appear on web pages published by third parties

May

June

July

August

September

October

25 November – European Parliament decides to request CJEU to deliver an opinion on the EU–Canada agreement on transfer of passenger name records (PNR)

26 November – Article 29 Working Party adopts guidelines on the implementation of the CJEU judgment in *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/121)

November

5 December – Article 29 Working Party adopts a working document on surveillance of electronic communications for intelligence and national security purposes

December

5 Information society, privacy and data protection

EU internal security concerns, including the threat of terrorist attacks, have affected the data protection debate, while mass surveillance and government secrecy have continued to be widely discussed. Examples of this shift in attention are renewed calls for an EU directive on passenger name records (PNR) and the discussion of whether there is a need to collect and store considerable data on all air passengers. At the same time, privacy remained top of the agenda; the Court of Justice of the European Union annulled the Data Retention Directive, and, in the Google case, clarified important aspects of EU data protection law.

5.1. Mass surveillance continues to spark global concern

"The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether."

United Nations (UN), Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), Fourth annual report submitted to the General Assembly, *A/69/397, 23 September 2014*

Following 2013 revelations that the United States and **United Kingdom** intelligence services have been conducting surveillance of global telecommunication and data flows on a previously unimaginable scale,[1] expectations were high that 2014 would bring both better understanding of the actual mass surveillance practices and greater compliance with fundamental rights by those involved.

In April 2014, the Council of Europe Parliamentary Assembly (PACE) Committee on Legal Affairs and Human Rights organised a hearing in which Edward Snowden gave evidence via video link. The hearing took place in the context of a report on mass surveillance that PACE is to adopt in 2015. The Council of Europe Commissioner for Human Rights reiterated his concerns about the internet rule of law at the end of 2014 and made several recommendations, including on the equal application of human rights online and offline, data protection, cybercrime and national security activities.[2]

5.1.1. United Nations

Among international organisations, the United Nations (UN) was by far the most vocal, and its forthright condemnations were particularly noticeable given the relative silence of regional organisations.

The UN made its stance clear, declaring that mass surveillance infringes on the rights to privacy, freedom of expression and association. Mass surveillance cannot be condoned, it found, without proper justification, safeguards to protect those affected and adequate oversight of those carrying it out. These statements were enshrined in several relevant documents that Table 5.1 summarises.

The UN General Assembly expressed its concerns in a second resolution on the right to privacy in the digital age,[3] backed by 65 of the 193 UN member states, 10 more than in 2013. The increased support indicates rising global awareness over the previous year. Supporters did not include the countries that make up the intelligence alliance between Australia, Canada, New Zealand, the **United Kingdom** and the United States.[4]

Table 5.1: Key 2014 UN documents linked to privacy and mass surveillance

Body	Title	Date
Human Rights Committee	Concluding observations on the fourth periodic report of the United States of America, Doc. CCPR/C/USA/CO/4	23 April 2014
Human Rights Council	Resolution on the promotion, protection and enjoyment of human rights on the internet, Doc. A/HRC/26/L.24	20 June 2014
High Commissioner for Human Rights	Report on the right to privacy in the digital age, Doc. A/HRC/27/37	30 June 2014
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism	Fourth Annual Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Doc. A/69/397	23 September 2014
General Assembly	Resolution on the right to privacy in the digital age, Doc. A/RES/69/166	18 December 2014

Source: FRA, 2014

Warning that mass surveillance is "emerging as a dangerous habit rather than an exceptional measure", the UN High Commissioner for Human Rights called for a more robust protection of the human rights enshrined in key international texts. These rights include Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR, ratified by all EU Member States), which both guarantee privacy, as well as regional and national laws.[5]

The Human Rights Committee also raised the principle of extraterritoriality when it required, among other things, that the United States respect its obligations under the ICCPR even for actions abroad when carrying out the collection of signals intelligence.[6] Critics of the principle rejected the requirement, arguing that states that carry out extraterritorial surveillance are only obliged to extend safeguards to their own citizens.[7] Advocates, however, say that the ICCPR establishes an extraterritorial right to privacy, whose jurisdiction extends beyond physical borders. They also note that a failure to adhere to this principle would violate the right of non-discrimination. As the Special Rapporteur put it, when states "exercise regulatory authority over the telecommunications or Internet service providers (ISP) that physically control the data", even when these are overseas, they are also engaging the principle of territorial jurisdiction.[8]

The UN High Commissioner for Human Rights found that there is currently little transparency and that the inadequate oversight in place allows a lack of accountability for arbitrary or unlawful intrusions on the right to privacy. The High Commissioner stated that "the very existence of a mass surveillance programme creates an interference with privacy".[9] These findings were echoed by various UN bodies, which promoted mixed forms of strong, independent and effective oversight (i.e. via the involvement of executive, parliamentary, judiciary and expert bodies) as viable solutions. They also urged states to establish authorities capable of providing binding remedies to those whose rights have been violated.

That states engaging in mass surveillance should prove the effectiveness of their programmes was also a recurrent statement. According to the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity, and almost no States have enacted explicit domestic legislation to authorize its use."[10] The Special Rapporteur therefore reasoned that, while terrorism might provide a justification for the exercise of mass surveillance, the systematic interference that intelligence services and law enforcement bodies are carrying out must comply with Article 17 of the ICCPR and other international human rights standards. Since these include the principles of necessity and proportionality, the Special Rapporteur implies that states engaging in mass surveillance are thereby violating human rights. Not only does he argue that "it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately", but his analysis makes clear that the right to privacy may be interfered with only on an exceptional, case-by-case basis.

To become more privacy-friendly, the Human Rights Council urged states to address the security concerns

that have the potential to infringe upon the right to privacy.[11] Further recommendations included that states ensure that their practices are not arbitrary or unlawful by enacting accessible, specific and foreseeable laws (including information-sharing agreements). Since data retention schemes involve the cooperation of telecommunication and internet providers, the private sector was urged to avoid becoming compliant with human rights infringements by omission, that is to say, by failing to require that governmental demands of accessing such data are done in accordance with the right to privacy.

5.1.2. European Union institutions

After the political turmoil that followed the 2013 revelations of the mass surveillance operations by the United States and the United Kingdom, the Council of the European Union did not revisit the issue in 2014.

The European Commission pursued discussions with United States (US) authorities as it assessed Decision 2000/520/EC, the so-called Safe Harbour Decision,[12] which provides the legal basis for the transfer of personal data from the EU to US companies. Simultaneously, theycontinued the negotiations for a data protection umbrella agreement between the EU and the United States.[13]

The European Parliament (EP) also took further action, adopting a resolution based on a report prepared by the Committee on Civil Liberties, Justice and Home Affairs (LIBE).[14] It said that mass surveillance by public authorities is incompatible with the fundamental rights enshrined in the EU Charter of Fundamental Rights (the Charter), and called for a full investigation into the matter. It also urged national governments and parliaments not to remain silent in the face of the revelations.[15] The resolution called for a large number of follow-up actions, including one asking FRA to conduct in-depth research into the effects of mass surveillance on EU citizens' fundamental rights.[16] Furthermore, the EP addressed other EU institutions about their inaction, reminding them that it is the "duty of the European institutions to ensure that EU law is fully implemented for the benefit of European citizens and that the legal force of the EU Treaties is not undermined by a dismissive acceptance of extraterritorial effects of third countries' standards or actions". The newly elected EP did not formally reopen the discussion after the beginning of the legislature in July but work is planned to resume in 2015.

5.1.3. Member States

Member States continued to react to the Snowden revelations in 2014.[17] **Germany** and the **United Kingdom**, for example, held parliamentary inquiries. The German Federal Parliament established a committee of inquiry, which is still collecting information to analyse the US National Security Agency situation.[18] Similarly, the public evidence sessions held by the United Kingdom's Intelligence and Security Committee as part of its Privacy and Security Inquiry heard from a large array of witnesses, from civil society representatives to the Home and Foreign Secretaries, who are responsible for issuing warrants for surveillance within and outside the United Kingdom.[19] The committee had not yet published its findings by the end of 2014. The **French** National Assembly also held a public hearing dealing with surveillance and privacy, touching on the French secret services' current work, the oversight mechanism, data protection safeguards and the planned reforms.[20] This general reflection was supported by a Council of State report on the digital age and fundamental rights, which suggested concrete legal reforms to enhance the fundamental rights compliance of surveillance activities.[21]

In other EU Member States, non-parliamentarian bodies also raised concerns. In **Estonia**, for instance, it was the Chancellor of Justice (the ombudsperson) who reacted, by initiating a legislative amendment to clarify his oversight powers over the intelligence services.[22] The government opposed his proposal, introducing several amendments to the bill to curb the chancellor's oversight powers in this area.[23] The parliament adopted the amendments in December, explicitly recognising that the Chancellor of Justice has the power to investigate complaints made against the intelligence services. However, as the government requested, he does not have the power to access certain types of state secrets and classified foreign information.[24] This exemplifies the difficulties and hurdles in organising oversight mechanisms meant to control intelligence services within the EU. In **Belgium**, the Standing Intelligence Agencies Review Committee started four investigations linked to the Snowden revelations, two of which were discussed in 2014 in the competent senatorial commission; the other two are still pending.[25]

National security concerns, however, continue to be used as a justification for restricting the right to privacy in several countries. Some, such as **France**, have asked for an increase in the human and technical resources of their intelligence services to cope with new challenges. The Parliamentary Delegation on Intelligence tried to balance this by calling for better protection of individual freedoms and better internal control within the intelligence services, and by stating that the work that French intelligence services carry out is drastically different in nature from that of US intelligence services.[26] Others, such as the **United Kingdom**, have called for broader surveillance powers and a ban on the use of encryption in communication, to facilitate the intelligence services' work.[27]

In 2014, only a few cases were brought before national courts. One of these, brought before the UK's

Investigatory Powers Tribunal (IPT) by various NGOs, was dismissed.[28] The claimants alleged that the use of the TEMPORA programme[29] by the British intelligence services, including Government Communications Headquarters (GCHQ), is unlawful. Since the intelligence services adhered to their policy of 'neither confirm nor deny', the tribunal was only able to hypothetically assess whether the legal framework would allow GCHQ to conduct mass surveillance. In its ruling, the tribunal found that the programme is legal in principle, though it did not study the proportionality of its use.

The tribunal also studied the legality of British intelligence services receiving data from, for example, the United States, when those data are based on communications intercepted by controversial mass surveillance programmes such as Prism or Upstream. It concluded that the "sufficient safeguards in place" in the United Kingdom afford individuals suitable protection. Privacy International and its co-claimant, Bytes For All, plan to contest the ruling before the European Court of Human Rights.[30]

A similar case was brought before the District Court of The Hague in the **Netherlands**.[31] The court also ruled that the country's intelligence services may receive data from foreign intelligence and security services, even if their powers are wider than those allowed within the country.

Promising practice

Publishing an annual activity report

Croatia's Security and Intelligence Agency (*Sigurnosno-obavještajna agencija*, SOA) has published an activity report explaining its role, duties, responsibilities and some of its current activities to the public for the first time. Prior to this, information related to SOA was considered classified. The agency launched a series of meetings with various target groups (civil society organisations, students and media) to bring its work closer to the public in 2014.

For more information, see: www.soa.hr

In **Hungary**, before the Constitutional Court, the Commissioner for Fundamental Rights challenged two legal provisions on surveillance.[32] Although Hungarian legislation does not provide for mass surveillance, the court ruling is an example of judicial scrutiny of whether surveillance measures are proportionate and take factors other than security into consideration. The commissioner contested two provisions: one allowing the continuous surveillance of "persons under national security check", the other excluding judicial review of the minister's decision on a complaint against the national security check's final findings. The court ruled that continuous surveillance, especially by secret means, of "persons under national security check" is disproportionate. In so doing, it upheld the commissioner's reasoning, arguing that it is disproportionate because the surveillance covers all those who come into contact with the person under surveillance, such as family members. It also declared unconstitutional and void the exclusion of judicial review of the minister's decision.[33]

5.1.4. Role of data protection authorities

Previous FRA research, and particularly the 2014 report on *Access to data protection remedies in EU Member States*, has stressed the role of data protection authorities (DPAs) as supervisors[34] and as the non-judicial remedial mechanism preferred by individuals who have experienced a data protection violation.[35] FRA has identified the need for improvements, namely further harmonisation and strengthening of the DPAs' powers, as well as the removal of obstacles that affect in practice the exercise of the fundamental right to a remedy.

The revelations on mass surveillance triggered wide-reaching discussion by DPAs globally[36] and at European level.[37] The Article 29 Working Party (A29 WP), which assembles all EU DPAs, analysed the current EU and international legal framework and provided recommendations.[38] It considers that effective oversight of national intelligence services should be carried out by the DPAs or in close collaboration with them. The A29 WP also stressed the need for more transparency of national intelligence services' activities. It called on Member States to respect their obligations under the right to privacy (Article 8 of the European Convention on Human Rights (ECHR)) and to further improve their data protection rules, including in the context of data exchange between national intelligence services. The A29 WP also stressed the full applicability of the EU data protection law when data are processed by private entities, such as electronic communications providers, and subsequently accessed by national intelligence services, or data are transferred by private entities to third countries and accessed by the national intelligence services of those countries.

Given the important role played by DPAs in safeguarding data protection, an assessment of DPAs' power vis-à-vis national intelligence services seemed important. FRA's comparative analysis aims to complement the work DPAs performed in 2014.[39] Table 5.2 on the DPAs' powers over national intelligence services (NIS) provides an overview of the national legal frameworks in place.

According to FRA's findings, in only seven EU Member States do DPAs have the same powers over

Table 5.2: DPAs' powers over national intelligence services, by EU Member State

EU Member State	No powers	Same powers	Limited powers
AT		X	
BE			X
BG		X	
CY			X
CZ	X		
DE			X
DK	X		
EE	X		
EL			X
ES	X		
FI		X	
FR			X
HR		X	
HU		X	
IE			X
IT			X
LT			X
LU	X		
LV	X		
MT	X		
NL	X		
PL			X
PT	X		
RO	X		
SE		X	
SI		X	
SK	X		
UK	X		
TOTAL	**12**	**7**	**9**

Notes: *'No powers' refers to DPAs that have no competence to supervise NIS.*

'Same powers' refers to DPAs that have the exact same powers over NIS as over any other data controller.

'Limited powers' refers to a reduced set of powers (these usually comprise investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.

Source: *FRA, 2014*

national intelligence services as they do over any other data controller.

In 12 Member States, the DPAs have no powers over NIS. They are excluded either expressly by the general data protection law or by specific laws on the functioning of the national intelligence services. In **Latvia**, for instance, the DPA, according to the general data protection law, is not competent to supervise files classified as 'official secrets'. Personal data processed by the national intelligence services fall entirely within that scope, as the investigatory operations law stipulates.[40]

In nine Member States, DPAs have limited powers over NIS. While DPAs retain the power to issue non-binding recommendations on general matters relating to NIS surveillance, limitations observed vary considerably by Member State. Some limitations are formal and do not really affect the DPAs' powers; others are more substantive.

Formal requirements in **Cyprus** or **Greece**, for example, state that an on-site inspection can take place only if the head of the DPA is present.[41] In **Germany,** the law stipulates that, instead of the head, an officer duly authorised in writing may carry out this task.[42] Similarly, only a DPA commissioner who has been a member of the Council of State, the Court of Cassation or the Court of Auditors may carry out an investigation in **France**.[43] In **Belgium**, **France** or **Italy,** for instance, when vested with exercising individuals' right to access their own data, DPAs are permitted to inform the individual only that the necessary checks have been made, but not which data have been processed if such information affects the security of the state.

Other limitations are more substantive. Data-processing activities by NIS may be wholly or partially excluded from the notification requirement to the DPAs (**Belgium**, **France**).[44] Investigatory powers, especially the powers to request and/or access data relating to the data-processing activities and premises relevant for the data-processing activities, are also limited (**France**, **Germany**, **Ireland** and **Poland**).[45] Some DPAs are not endowed with the power to handle complaints by individuals and issue binding decisions (**Belgium**, **Poland**).[46] In **Germany**, regarding postal and electronic communications data, the DPA's power is limited to giving an opinion only if requested to do so by the oversight body (the G-10 Commission, composed of four independent experts elected by parliament).[47] However, even the G-10 Commission cannot initiate an investigation, as the federal and state data protection commissioners pointed out.[48] Finally, according to FRA data, the **Lithuanian** DPA's powers cannot be clearly defined because the wording of the data protection law is debatable in conjunction with the specific law on the national intelligence services.[49] In the absence of legal reform, a judicial interpretation of these acts would clarify the situation.

In some countries, the involvement of DPAs may occur indirectly. In **Luxembourg**, for example, the DPA is not competent to supervise NIS. However, the supervisory authority competent to supervise data processing related to state security, defence and public safety is composed of the Chief State Prosecutor and two members of the DPA.[50]

In this context, various DPAs called for legislative reforms and the implementation of data security measures in 2014, especially of easy-to-use secure encryption tools. In **Germany**, the federal and state data protection commissioners adopted two resolutions suggesting measures for better protection of personal data and privacy. The first resolution related to data security measures for electronic communication service providers. Special attention is paid to the role of secure encryption and easy-to-use tools for the end users, the transfer of personal data only to cloud providers that operate in a trustworthy legal framework and raising citizens' awareness of the potential of new technologies.[51] The second resolution asked parliament to remove the deficiencies of the current oversight system.[52] The initiation of an investigation, for instance, is a necessary power of any DPA and should be provided for by law. It also asked to embed the DPAs in the oversight system, thus taking advantage of their expertise. These calls build on a 2013 Federal Constitutional Court judgment on a standardised national anti-terrorism data file. The court held that, in a surveillance system which is not open to scrutiny by individuals subject to surveillance, there must be an effective oversight system in place, and when there is a data exchange between various intelligence services there must be enhanced cooperation of the supervisory DPAs too.[53]

The **United Kingdom** Information Commissioner's Office (ICO), in its written submissions to the Intelligence and Security Committee of Parliament, points out that the legal framework is fragmented and needs reviewing to ensure effective oversight and redress mechanisms.[54] The ICO also stresses its need to be involved prior to the enactment of legislative measures and during the conduct of privacy impact assessments before and after a legislative measure is taken. The ICO draws a difference between electronic communications surveillance and other surveillance methods, such as closed circuit television (CCTV); the former is easy, intrusive and covert, it emphasises. The ICO strongly recommends the use of encryption and other technological measures by electronic communication providers. Finally, in an effort to clarify the responsibilities of the various oversight bodies and enable their effective cooperation, the ICO began to draw up a roadmap.[55]

Promising practice

Offering open source encryption programmes

The **Portuguese** data protection authority has developed a website proposing both information and software to enhance the online privacy of internet users. The project, called *Pen C3Priv*, consists of a USB memory stick including several open source programs, configured with the maximum levels of privacy, as well as an encryption program that allows the users to save encrypted documents. This memory stick also contains a portable internet browser with many extras to ensure more privacy of personal information. One of the advantages of using these programs is that they are created in open source, which allows scrutiny and eventual detection and correction of security flaws on a transparent basis.

For more information, see: http://c3p.up.pt

5.2. Towards an enhanced data protection regime

5.2.1. Data protection reform package still not adopted

The Council of Europe is finalising its modernisation of the convention on data protection (Convention 108).[56] This was mainly driven by the ever-increasing challenges of information and communication technologies (ICT) and the globalisation of data flows. In December 2014, the intergovernmental Ad Hoc Committee on Data Protection finalised the modernisation proposals. It will submit them to the Council of Europe Committee of Ministers for examination and adoption early in 2015.[57] Convention 108 is the sole legally binding international instrument in the field of data protection and is also open to states that are not members of the Council of Europe. The European Commission obtained a mandate to negotiate, on behalf of the EU, its accession to the Convention and to ensure that the proposed text is compatible with the EU data protection package.[58] The proposed modernisation strengthens the data protection system, including the DPAs' powers. The European Conference of DPAs made specific proposals for enhancement.[59]

Turning to the developments in the EU system, the European Parliament adopted its position on the data protection reform package in March 2014, maintaining the main building blocks of the 2012 European Commission's proposals.[60] It also improved the safeguards in some points, such as the conditions for lawful data transfers to third countries, the DPAs' power to impose dissuasive fines, and cooperation amongst national DPAs in cross-border cases to bring individuals concerned closer to their national DPAs. The European Council, as co-legislator, has not yet completed its work, but it reiterated the need for the adoption of the data protection reform package in 2015.[61] Sixteen national parliamentary delegations also sent a strong call for the adoption of the reform in 2015.[62]

5.2.2. CJEU interpretation strengthens EU data protection regime

The Court of Justice of the European Union (CJEU) has handed down three important judgments in the area of data protection, delivering two on 8 April 2014.

The first elaborates on the notion of DPAs' complete independence. The CJEU has already stressed in a series of judgments that DPAs' full independence is essential to safeguarding the fundamental right to personal data protection. This new case confirms and develops case law covered by previous annual reports.[63] In *Commission v. Hungary*,[64] the CJEU considered that prematurely ending the DPA head's term as a result of a reform of the national data protection system infringes the requirement of full independence, since it can be considered an external political influence.[65]

The second judgment on the validity of the Data Retention Directive (see Section 5.2.3) also addressed the DPAs' oversight powers in the context of data retention for surveillance. In *Digital Rights Ireland and Seitlinger and Others*, the CJEU held that the directive should have made sure that data falling under the scope of the directive is retained within the European Union's territory to enable DPAs to perform their monitoring role.[66] This lack of a safeguard contributed to the annulment of the directive.

The third important case, Google Spain against the Spanish DPA, deals with the so-called 'right to be forgotten', which the CJEU reinforced in its landmark ruling in May 2014.[67] It recognises that individuals have the right to decide whether information linked to their name, and therefore available to anyone who uses a search engine such as Google, should be available to the public; it thus strengthens the right of citizens to have control over their personal data. However, as stated by the court, this right is not absolute. Information may be removed only on the basis that the information is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of time that has elapsed".

The CJEU established that the operators of search engines are data controllers, within the meaning of the Data Protection Directive, because of the way they collect and process data.[68] Search engine operators are thus more than mediators that simply make

information available on the internet. They must therefore comply with the requirements set out in the directive, including the right to the erasure of inaccurate data – even when published by a third party – and the right to object to the data processing under the conditions set out in the directive.

The CJEU stated, moreover, that these obligations apply to the subsidiaries or "establishments" of the search engines too, when the main undertaking is located in a third country, as long as they have an establishment within the EU which sells advertising space to that Member State "in order to make the service offered by the engine profitable".[69]

Google began complying with the judgment by removing some of the requested information one month later. As newspapers saw links to their articles removed, criticism of the judgment followed. Other search engines such as Yahoo and Bing stated in November that they would also comply with the ruling.[70]

The CJEU is expected to provide further interpretation of DPA powers, since the High Court of **Ireland** referred a case to it in July 2014.[71] The case was reported in last year's annual report. It questions whether DPAs can launch their own investigations, based on developments (such as the mass surveillance revelation and particularly the PRISM programme), or whether they should be bound by a European Commission decision on the adequacy of the data protection level in a third country (presently the adequate level of protection provided by the US companies which have signed up to the Safe Harbour Privacy Principles).[72]

5.2.3. EU Member States react to the invalidation of the 2006 Data Retention Directive

As mentioned in Section 5.2.2, on 8 April 2014 the CJEU handed down a judgment in *Digital Rights Ireland and Seitlinger and Others*. The CJEU ruled that Directive 2006/24/EC on data retention had been null and void from the moment it entered into force on 3 May 2006. As reported in previous annual reports,[73] the transposition of the directive into national law had been delayed and challenged before the highest courts in various Member States.[74]

According to the CJEU, the Data Retention Directive pursued a legitimate aim in the fight against serious crime and therefore contributed to national security. Thus, for the CJEU "the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest".[75] The Data Retention Directive was, however, declared incompatible with Articles 7, 8 and 52 (1) of the Charter and hence declared invalid because of the following shortcomings regarding the principle of proportionality, namely that it did not:

- define the concept of serious crime, which made it difficult to weigh the general interest in combating serious crime against the individual's right to privacy;
- prescribe the exact conditions on which the data can be accessed by the national security authorities;
- include an obligation to distinguish between the data of suspects and those of users without any criminal background or indeed links with the suspects;
- grant the data subjects sufficient remedies or safeguards against misuse of the collected data;
- prescribe the procedural requirements for storing or justify the specified retention period of 6 to 24 months.

The CJEU also considered that, due to improved automated analysis tools, metadata and content data could no longer be strictly distinguished. It stated that:

> *"those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[76]

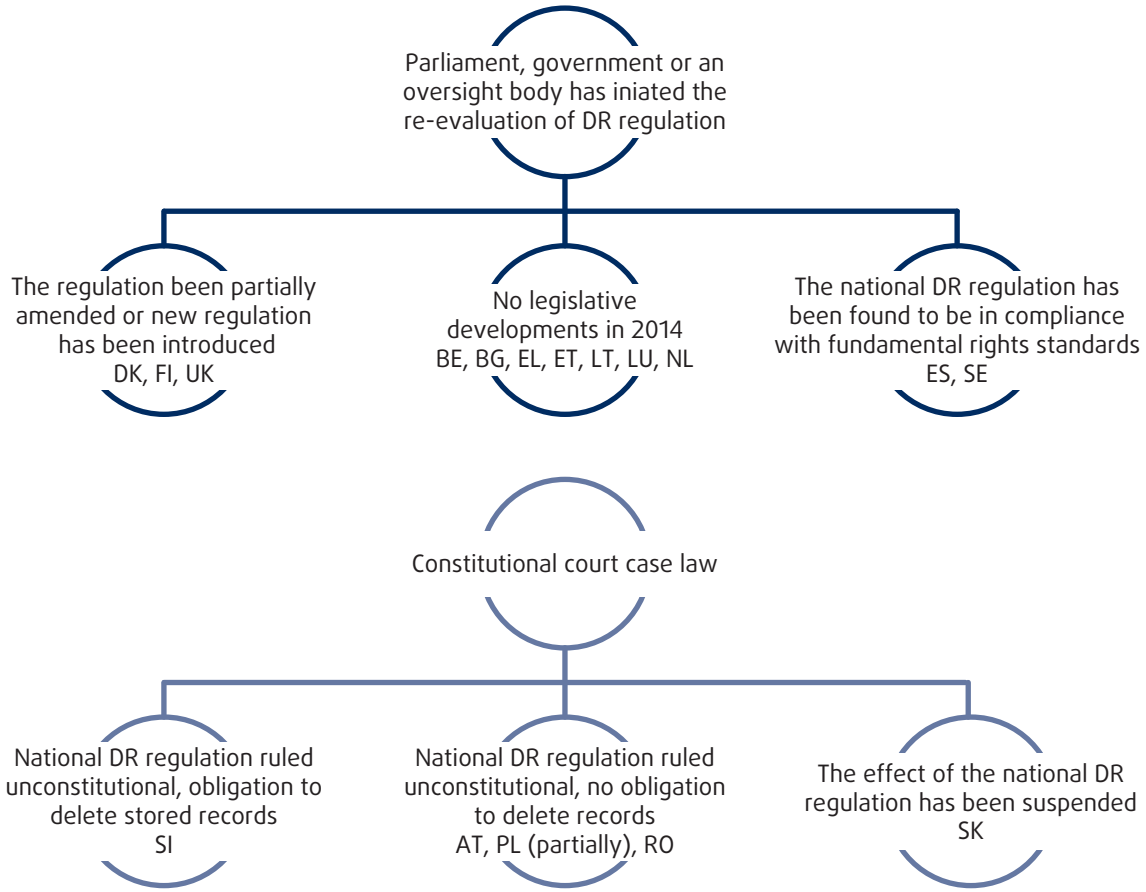
The CJEU also reiterated that the general population was not to be given the impression that it was under constant surveillance.

Although the *Digital Rights Ireland* ruling did not oblige Member States to abolish their national data retention regulations, it nevertheless set forth criteria for assessing their compatibility with fundamental rights standards. As a consequence, Member States are bound to re-evaluate their data retention regulations, and diverse judicial, legislative and private sector developments took place in 2014 after the CJEU's judgment.

Broadly, the impact of the data retention judgment on national data retention legislation and policy can be summarised as follows, showing a diverse pattern of responses at national level (Figure 5.1).

At the time of the CJEU judgment, several higher national courts already had cases pending. The *Digital*

Figure 5.1: Impact of the data retention judgment at national level



Note: *DR = data retention.*
Source: *FRA, 2014*

Rights Ireland case accelerated proceedings in many Member States and established the assessment criteria, which helped guide rulings.

The **Austrian** Constitutional Court was the first, on 27 June 2014,[77] to declare the national data retention laws to be invalid on the ground of inconsistency with the national constitution and Articles 7 and 8 of the Charter and Article 8 of the ECHR. The **Romanian** Constitutional Court followed on 8 July 2014.[78] Just three days later, on 11 July 2014, the **Slovenian** Constitutional Court[79] repealed mandatory data retention and took steps to compel ICT operators to delete stored metadata. All three courts followed the CJEU's argument and reasoning. On 30 July 2014, the **Polish** Constitutional Court ruled that the national provisions concerning the rules of access to and use of telecommunications data by the national security authorities were invalid and contrary to the Polish constitutional law on the right to privacy, and that data retention regulation was invalid principally because it did not lay down any judicial or other external control mechanism over the legality of the requests for electronic metadata made by the intelligence authorities. On 23 April, the **Slovak** Constitutional Court suspended the national data retention regulation until it is amended and brought into conformity with the CJEU judgment.[80] Cases are pending in **Belgium**[81] and **Bulgaria**.[82]

In addition to the constitutional debate, the CJEU judgment also has a direct impact on criminal procedure law. The question arises of whether criminal proceedings have to be invalidated where data obtained via mass storage have been used as evidence. The retroactive effect of the CJEU ruling has been discussed by lawyers in the media and also in courtrooms. In **Cyprus**,[83] **Spain**[84] and the **Netherlands**,[85] defence lawyers have attempted to use the CJEU ruling to overturn convictions in cases where necessary evidence has been collected via mass storage. National courts have, however, found that data retention is a proportionate measure for combating crime. Even when the applied measures have been viewed as excessive in the light of the *Digital Rights Ireland* criteria, the Court of Appeal of the Netherlands explicitly stated that the invalidation of the directive does not automatically make the national legislation unconstitutional.[86]

The CJEU's approach has not entirely determined how Member State authorities have reacted. Some have

drafted regulations widening law enforcement and intelligence institutions' access to telecommunication data. In **Cyprus**[87] the government proposed to parliament draft legislation that obliges telecom companies to register the users of prepaid cards. In **Germany** and **Romania**, draft laws were proposed that, according to the critics, implicitly allowed the reintroduction of data retention. In December 2014, the German government adopted the bill on information technology security, taking these criticisms into account.[88] In Romania, the draft act was also criticised and in December a group of parliamentarians referred it to the Constitutional Court for review.[89] In **Croatia**, a new bill was introduced according to which the intelligence services may ask a network provider to grant them direct access to communication data and which allows the removal of encryption for secret surveillance purposes.[90]

The **United Kingdom** delivered the most notable legislative response to the CJEU judgment, adopting emergency legislation.[91] On 27 July 2014, the Data Retention and Investigatory Powers Act (DRIP) and its annex Data Retention Regulation entered into force. One of the main triggers for adopting DRIP was the fact that many electronic communications service providers were considering deleting the data they had at their disposal. Under DRIP, public telecommunications operators notified by the Secretary of State are required to retain certain data that have been generated or processed in the United Kingdom relating to telephony and internet communications for up to 12 months.

Critics say that, rather than promoting privacy and limiting data retention, DRIP mainly aims to maintain or even expand the measures of blanket surveillance allowed in the Regulation of Investigatory Powers Act of 2000.[92] The foremost concern, expressed by British academics in an open letter to the full House of Commons, is that the new bill expands the investigatory powers of the British intelligence services from national to global level.

The CJEU judgment has also triggered enhanced fundamental rights guarantees. In **Finland**, for example, the new Information Society Act was amended to determine the retention periods of different communications data.[93] In **Denmark**, ISP companies are no longer obliged to store information on users' source and destination internet protocol addresses, port numbers and session types (a practice known as session logging).[94] The **Dutch** Minister of Justice and Security announced that alterations to the Act on Obligatory Retention of Data and the Criminal Procedure Code, entailing more stringent procedures for accessing the stored data, will be presented to parliament.[95]

The legislators in many Member States have suggested defining more precisely the scope of offences that allow the use of retained data for investigatory purposes. The new **Finnish** Information Society Act stipulates that retained data be used in the investigation and prosecution of serious crimes and refers to an exhaustive list provided in the Act of Coercive Measures.[96] In addition, the **Luxembourg** Ministry of Justice recommended that the current penalty threshold of one year should be replaced by an exhaustive list of offences.[97] In **Lithuania**, the discussions relate to the scope of the legislation and in particular the definition of 'serious and very serious crimes'.[98] In some Member States, such as **Bulgaria**,[99] **Estonia**,[100] **Greece**[101] and the **Netherlands**,[102] various organisations produced various legal analyses of the national regulation.

In 2011, the **German** Minister of Justice suggested replacing mandatory blanket retention of data with less invasive data preservation, also known as "quick freeze".[103] Privacy and digital rights activists support this alternative solution.[104] Data preservation differs from retention in that it occurs only when a tribunal orders a service provider to retain (from the date of the preservation order) the data of specified individuals who are suspected of criminal activities. There would, therefore, be no option of non-suspicion-based retroactive policing. The former European Commissioner for Home Affairs Cecilia Malmström, however, argued strongly in favour of mandatory retention, stating that:

> *"we need to address the argument that data retention should be replaced by a system of data freeze, or data preservation. I am not convinced that this would be an effective alternative. Data freeze will never bring back deleted data. Only data retention ensures that data which may one day be decisive – to prosecute or to clear a criminal – are available. I am afraid there are no easy choices or shortcuts here."*[105]

The effectiveness of the proposed alternative will be confirmed or denied by the experience of **Romania**, which has, following *Digital Rights Ireland*, resorted to preservation.

Data retention concerns public and private actors equally. Therefore, the ICT sector has a substantial role to play in the aftermath of the judgment. To date, **Slovenia** is the only Member State that has obliged electronic communications service providers to delete stored communications data.[106] Elsewhere, companies are faced with a dilemma: should they continue storing communication data and thereby risk infringing individuals' fundamental rights, or should they delete the data and thereby breach obligations laid down by national law? So far, the first scenario has not lead to any lawsuits. The **Hungarian** Civil Liberties Union (*Társaság a Szabadságjogokért*), an NGO, plans to sue the two largest mobile telecommunications providers to challenge the data retention rules in

the Act on Electronic Telecommunications before the Constitutional Court.[107]

To avoid potential claims, some **Swedish** ICT operators took the most proactive course by announcing that they had stopped retaining customer data and deleted all the stored files.[108] However, in June the obligation to retain data was restored by the Swedish Post and Telecom Authority after an analysis of the Swedish law found it compatible with the EU court decision. The Swedish legislation is currently under further analysis.

NGOs and the media, the third group of actors in the majority of Member States, have published opinions in support of the CJEU *Digital Rights Ireland* judgment and thus contributed to the general debate over digital rights, surveillance and privacy. The **Belgian** Human Rights League (*Liga voor Mensenrechten/Ligue des Droits de l'Homme*), the Net Users' Rights Protection Association and, most notably, Digital Rights Ireland have also taken direct judicial action. Digital Rights Ireland is continuing the case against data retention in the High Court of Dublin.

A major twist in the discourse on the general necessity of indiscriminate data retention came after the January 2015 terrorist attacks in France. In response to the events, data retention and extensive cyber surveillance are once again considered suitable and proportionate means of fighting against terrorism. As an example of this tendency, **Denmark** is considering reintroducing session logging.[109] In the **United Kingdom**, the Prime Minister has pledged to legislate on internet surveillance powers to allow intelligence services to break into the encrypted communication of suspected terrorists. The question of reintroducing data retention has also been raised in **Austria**, **Germany** and **Romania**.

5.2.4. Passenger name records in the framework of the EU internal security agenda

The CJEU's *Digital Rights Ireland* ruling also played an important part in the political debate on EU passenger name record (PNR) legislation, which drew the European Parliament's and the Council of the European Union's renewed attention to the 2011 legislative proposal.[110] The debate intensified as the perceived threat of a terrorist attack rose, gaining a new sense of urgency after the January 2015 terrorist attacks in France.[111]

PNR data are collected by airlines from passengers during reservation and check-in procedures. These include the passengers' contact and travel details, means of payment and other information. In 2011, the European Commission introduced a proposal for a PNR directive that would allow law enforcement agencies to use the data to combat terrorism and serious crime, complementing the various PNR agreements with third countries. The proposal was, however, stalled in the European Parliament in 2013 on grounds of data protection and proportionality concerns.

The CJEU's *Digital Rights Ireland* ruling reinforced the European Parliament's critical view of the principles underlying the use of PNR data for law enforcement purposes. On 25 November 2014, the European Parliament decided to refer the EU–Canada PNR agreement, signed in June, to the CJEU for an opinion.[112] The opinion could have far-reaching legal implications for all other EU PNR agreements with third countries as well as for the EU draft directive. In his speech in the European Parliament on 3 December 2014, Commissioner Avramopoulos nevertheless called upon the co-legislators to work towards the adoption of the 2011 draft directive as "a matter of realistic choice", encouraging the European Parliament to propose additional safeguards that would make the proposal "more robust from the point of view of fundamental rights guarantees".[113]

The European Commission has also supported Member States in developing their own national PNR systems in 2014. Besides providing financial support to these Member States, it requested that FRA provides practical guidance about the processing of PNR data for law enforcement purposes to promote compliance with fundamental rights. As a result, FRA published, in February, 12 fundamental rights considerations for the attention of Member States' technical experts.[114] This was done in informal consultation with European Commission services and the European Data Protection Supervisor (EDPS) and building on earlier opinions on PNR.[115] The considerations are a non-exhaustive list of 'dos and don'ts' on how to operationalise fundamental rights when establishing national PNR systems. They propose, for example, the introduction of clear and strict limitations on purpose, personal data safeguards and a high level of transparency of the PNR schemes for passengers. These practical considerations do not advocate setting up an EU PNR framework, but they outline key fundamental rights considerations where PNR frameworks do exist.

Discussions on the EU PNR directive gained new impetus from the internal security debate that grew in intensity in 2014. This was driven in part by the possible threat posed by 'foreign fighters' – EU nationals involved in armed conflicts outside the EU. A call for the adoption of the instrument appeared in important policy documents such as the European Council's post-Stockholm programme of 26 and 27 June[116] and the conclusions of the special meeting of the European Council of 30 August, which expressly requested the European Parliament to finalise its work on the proposal by the end of the year.[117] At the global level, the UN Security Council, in

its Resolution 2178 (2014) dealing with measures to prevent the movement and recruitment of foreign fighters, encouraged states to "employ evidence-based traveller risk assessment and screening procedures including collection and analysis of travel data."[118]

These documents set the stage for a clear support for a PNR Directive expressed by Member States in the Justice and Home Affairs Council conclusions of 4 December on the development of a renewed EU Internal Security Strategy. In this key document, the EU Council sets out its strategic priorities in the area of internal security for the upcoming five-year period. It presents "a strong Directive on EU PNR" as one of the tools required to "tackle the current threats, including terrorism". At the same time, however, it underlines the role of fundamental rights in internal security policies and encourages EU institutions and Member States to involve FRA in their design.[119]

> *"Respecting fundamental rights in planning and implementing internal security policies and action has to be seen as a means of ensuring proportionality, and as a tool for gaining citizens' trust and participation."*
>
> *Council of the European Union (2014),* Council conclusions on development of a renewed European Union Internal Security Strategy, *Brussels, 4 December 2014, p. 7*

FRA conclusions

- The EU institutions and Member States have been negotiating the data protection package since January 2012. Despite the evidence that challenges to data protection remain part of today's information society, no political agreement has yet been reached on the legislative proposals.

EU Member States should promptly adopt the data protection package to provide the EU with an enhanced data protection framework that could be complemented with specialised legislation in other areas of EU competence.

- Following the Snowden revelations concerning mass surveillance, the role of intelligence services and the implications of surveillance activities were discussed in the political arena, as well as in courts and by the public. Against this background, a number of EU Member States have engaged in a reform of security and intelligence services, as FRA comparative research shows.

EU Member States should take the opportunity to enhance privacy and data protection guarantees when reforming their services. These could include adequate guarantees against abuse, which entails effective supervision by independent bodies and efficient redress mechanisms. Member States should consider such guarantees in any reforms of intelligence systems.

- Data protection authorities play an important role in safeguarding general data protection legislation. Evidence collected by FRA shows their mandates differ widely. In several EU Member States, DPAs have the legal mandate to play a significant role in supervising security and intelligence services.

Where an EU Member State allows its DPA to supervise security and intelligence services, it should further strengthen the authority's independence and role and ensure that it is supported by adequate financial and human resources.

- In 2014, various revelations concerning mass surveillance highlighted the occurrence of data security breaches. The legal obligations of actors, such as electronic communications service providers, thus moved to the forefront.

EU Member States should ensure that data controllers, such as electronic communications service providers, adhere to their legal obligation as laid down in Article 4 of Directive 2002/58/EC and Article 17 of Directive 95/46/EC: taking into account the risks represented by data processing and the nature of the data involved, service providers have to implement appropriate technical security measures,. The use of secure encryption technologies should be considered in this context, as well as the development of user-friendly encryption tools.

- The CJEU's judgment on the Data Retention Directive spelled out crucial fundamental rights principles and suggested specific safeguards related to, for example, the scope of data retention, its aim and limits to law enforcement agencies' access to the data and the retention time. FRA mapped the Member States' reactions to this core CJEU judgment, identifying a variety of approaches in terms of both judicial and legislative reactions.

When assessing the legal implication of this judgment, the European Commission and Member States should carry out research on data retention's positive impact or lack thereof. If no significant advantages are found, less invasive alternatives should be preferred.

- Discussions on creating an EU framework for acquiring and processing passenger name records played a significant part in the internal security debate in 2014.

The EU co-legislators should ensure that the potential setting up of an EU passenger name records system be accompanied by enhanced fundamental rights safeguards, including limitations on purpose, transparency towards passengers and protection of their personal data.

Index of Member State references

Endnotes

All hyperlinks accessed on 30 April 2015.

1 European Union Agency for Fundamental Rights (FRA) (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office of the European Union (Publications Office), Ch. 3.

2 Council of Europe, Commissioner for Human Rights (2014), *The rule of law on the internet and in the wider digital world*, Strasbourg, Council of Europe.

3 United Nations (UN), General Assembly (2014), *The right to privacy in the digital age*, A/RES/69/166, 18 December 2014.

4 The so-called '5 Eyes' agreement.

5 UN, Office of the High Commissioner for Human Rights (OHCHR) (2014), *The right to privacy in the digital age,* A/HRC/27/37, 30 June 2014.

6 UN, Human Rights Committee (2014), *Concluding observations on the fourth periodic report of the United States of America,* CCPR/C/USA/CO/4, 23 April 2014.

7 United States, Department of Justice (2014), 'Remarks by the President on Review of Signals Intelligence', 17 January 2014.

8 UN, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), *Fourth annual report submitted to the General Assembly*, A/69/397, 23 September 2014. See also Council of Europe, Commissioner for Human Rights (2014), *The rule of law on the internet and in the wider digital world*, Strasbourg, Council of Europe.

9 UN, OHCHR (2014), *The right to privacy in the digital age*, A/HRC/27/37, 30 June 2014.

10 UN, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), *Fourth annual report submitted to the General Assembly*, A/69/397, 23 September 2014.

11 UN, Human Rights Council (2014), *The promotion, protection and enjoyment of human rights on the internet*, A/HRC/26/L.24, 20 June 2014.

12 European Commission (2000), Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Brussels, 26 July 2000.

13 European Commission (2014), *Factsheet EU–US, negotiations on data protection*, Brussels, June 2014.

14 FRA (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office, Ch. 3.

15 European Parliament (2014), *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, P7_TA(2014) 0230, Brussels, 12 March 2014.

16 FRA (2014), 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies', project.

17 For the initial reactions in 2013, see FRA (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office, Ch. 3.

18 Germany, Bundestag, 1. Untersuchungsausschuss (2014), 'Sitzungsabbruch nach Eklat im Untersuchungsausschuss', 16 October 2014.

19 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2014), Privacy and Security Inquiry, 14–16 and 23 October 2014.

20 France, Assemblée Nationale (2014), Commission on rights and freedoms in the digital age (*Commission de réflexion sur le droit et les libertés à l'âge du numérique*). See in particular the round table on freedoms and surveillance activities (*Âge du numérique : Table ronde sur les libertés et les activités de renseignement*), 13 November 2014.

21 France, Conseil d'État (2014), *Le numérique et les droits fondamentaux – Étude annuelle 2014 du Conseil d'État*, Paris, La documentation française.

22 Estonia, Parliament (*Riigikogu*) (2014), Explanatory letter to the bill of the Chancellor of Justice Act Amendment Act, No. 663 (*Õiguskantsleri seaduse muutmise seadus 663 SE, eelnõu algteksti seletuskiri*).

23 Estonia, Riigikogu (2014), *Õiguskantsleri seaduse muutmise seadus 663 SEII, eelnõu seletuskiri*, text presented for the second reading.

24 Estonia, Act on Amending the Chancellor of Justice Act of 9 December 2014 (*Õiguskantsleri seaduse muutmise seadus, Vastu võetud 09.12.2014*), RT I, 22.12.2014, 2. See also the Chancellor of Justice Act (*Õiguskantlseri seadus*), para. 11 (1) Access of Chancellor of Justice to state secrets and classified information of foreign states (*Õiguskantsleri juurdepääs riigisaladusele ja salastatud välisteabele*).

25 Belgium, Comité permanent de contrôle des services de renseignements et de sécurité/Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (2014), *Rapport d'activités 2013/Activiteitenverslag 2013*, Antwerp and Cambridge, Intersentia.

26 France, Délégation parlementaire au renseignement (2014), *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*.

27 United Kingdom, Prime Minister David Cameron's speech in Nottingham, 12 January 2015; *The Guardian* (2015), 'David Cameron pledges anti-terror law for internet after Paris attacks'.

28 United Kingdom, Investigatory Powers Tribunal (IPT), *Liberty & Others vs. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014.

29 FRA (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office, Ch. 3, Table 3.1.

30 Privacy International (2014), *Investigatory Powers Tribunal rules GCHQ mass surveillance programme TEMPORA is legal in principle*. See also European Court of Human Rights (ECtHR), *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, No. 62322/14, 5 January 2015.

31 The Netherlands, Rechtbank Den Haag (2014), C/09/455237 / HA ZA 13-1325, 23 July 2014.

32 Hungary, Alkotmánybíróság (2014), 9/2014. (III.20.) AB határozat, Decision.

33 Hungary, Act CIX of 2014 on the modification of the Act CXXV of 1995 on the national security services and the modification of other Acts related to the national security control modified the legislation on national security services according to the ruling of the Constitutional Court (*2014. évi CIX. Törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint egyes törvényeknek a nemzetbiztonsági ellenőrzéssel összefüggő módosításáról*).

34 FRA (2010), *Data protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II*, Luxembourg, Publications Office; FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office.

35 FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office.

36 36th International Conference of Data Protection and Privacy Commissioners (2014), *Resolution: Privacy in the digital age*.

37 European Data Protection Supervisor (2014), *Opinion on the Communication from the Commission to the European Parliament and the Council on 'Rebuilding trust in EU-US data flows' and on the Communication from the Commission to the European Parliament and the Council on 'the functioning of the safe harbour from the perspective of EU citizens and companies established in the EU'*, 20 February 2014.

38 Article 29 Working Party (A29 WP) (2014), *Opinion 04/2014 on surveillance of electronic communications of intelligence and national security purposes,* WP 215, 10 April 2014; A29 WP (2014), *Working Document on surveillance of electronic communications for intelligence and national security purposes*, 5 December 2014; A29 WP (2014), *Joint statement of the European data protection authorities assembled in the Article 29 Working Party*, 26 November 2014.

39 *Ibid*.

40 Latvia, *Operatīvās darbības likums*, 16 December 1993, Art. 24, part 1.

41 Cyprus, Processing of Personal Data Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 (Ν. 138(Ι)/2001)*), Art. 23 (1) (h); Greece, Data Protection Law 2472/1997 (*Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*), Art. 19 (1) (h).

42 Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), Art. 24 (4).

43 France, Law no. 78-17 relating to information technology, files and freedoms of 6 January 1978 (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), Art. 41 (2).

44 Belgium, Data Protection Act (*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*), Art. 3 (4) in conjunction with Art. 17; France, Law no. 78-17 relating to information technology, files and freedoms of 6 January 1978 (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), Art. 26 (3), in conjunction with Decree no. 2007-914 for application of article 30 I of Law no. 78-17 relating to information technology, files and freedoms (*Décret n° 2007-914 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*).

45 France, Law no. 78-17 relating to information technology, files and freedoms of 6 January 1978 (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), Art. 44, in conjunction with Decree no. 2007-914 for application of article 30 I of Law no. 78-17 relating to information technology, files and freedoms (*Décret n° 2007-914 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*); Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), Art. 24 (4); Ireland, Data Protection Act 1988, section 12 (4) (b) and section 24; Poland, Data Protection Act 1997 (*Ustawa o ochronie danych osobowych*), Art. 43 (2) in conjunction with Art. 14 (1) (3) (5).

46 Belgium, Data Protection Act (*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*), Art. 3 (4) in conjunction with Art. 29–31; Poland, Data Protection Act 1997 (*Ustawa o ochronie danych osobowych*), Art. 43 (2) in conjunction with Art. 12, 15–18.

47 Germany, Act restricting the secrecy of correspondence, posts and telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses - Artikel 10-Gesetz - G 10*), Art. 15.

48 Germany, 88th conference of Federal and State Data Protection Commissioners (*88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*) (2014), *Effektive Kontrolle von Nachrichtendiensten herstellen!*, 8–9 October 2014.

49 Lithuania, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, No. X-1444, 1 February 2008, Art. 1 (5) in conjunction with Lietuvos Respublikos žvalgybos įstatymas, No. XI-2289, 17 October 2012, Art. 24.

50 Luxembourg, Act of 2 August 2002 on the protection of persons with regard to the processing of personal data (*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*), Art. 17 (2).

51 Germany, 87th conference of Federal and State Data Protection Commissioners (*87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*) (2014), *Gewährleistung der Menschenrechte bei der elektronischen Kommunikation*, 27–28 March 2014.

52 Germany, 88th conference of Federal and State Data Protection Commissioners (*88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*) (2014), *Effektive Kontrolle von Nachrichtendiensten herstellen*!, 8–9 October 2014.

53 Germany, Bundesverfassungsgericht, BvR 1215/07, 24 April 2013.

54 United Kingdom, Information Commissioner's Office (2014), *The Information Commissioner's submission to the Intelligence and Security Committee of Parliament – Privacy and Security Inquiry*, 31 January 2014.

55 Information Commissioner's Office, *et al.* (2014), *Surveillance road map: A shared approach to the regulation of surveillance in the United Kingdom*, Version 3.2, August 2014.

56 Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 1981.

57 Ad Hoc Committee on Data Protection (2014), *Abridged report*, CAHDATA(2014)RAP03Abr, 1–3 December 2014.

58 European Commission (2012), 'Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU', Memo.

59 European Conference of Data Protection Authorities (2014), *Resolution on the revision of the Convention for the protection of individuals with regard to automatic processing of personal data*, 5 June 2014.

60 European Parliament (2014), Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), P7 TA(2014)0212, 12 March 2014; European Parliament (2014), Legislative resolution on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, P7 TA(2014)0219, 12 March 2014.

61 European Council (2014), *Conclusions*, EUCO 79/14, 27 June 2014; European Council (2014), *Conclusions*, EUCO 169/13, 25 October 2013.

62 France, Assemblée Nationale (2014), Interparliamentary meeting on personal data, Common Declaration (*Réunion interparlementaire sur le Parquet européen – Déclaration commune*), 17 September 2014.

63 FRA (2013), *Fundamental rights: Challenges and achievements in 2012 – Annual report 2012*, Luxembourg, Publications Office, Ch. 3; FRA (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office, Ch. 3.

64 CJEU, C-288/12, *Commission v. Hungary*, 8 April 2014.

65 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.

66 CJEU, Joined cases C-293/12, C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014, para. 68.

67 CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

68 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 (Data Protection Directive).

69 CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014, para. 55.

70 *Wall Street Journal* (2014), 'In Europe, Microsoft and Yahoo have started to forget', 28 November 2014.

71 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

72 European Commission (2000), Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour principles and related frequently asked questions issued by the US Department of commerce, 26 July 2000.

73 FRA (2014), *Fundamental rights: Challenges and achievements in 2013 – Annual report 2013*, Luxembourg, Publications Office, Ch. 3.

74 *Ibid.*

75 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, para. 44.

76 *Ibid.*, para. 27.

77 Austria, Verfassungsgerichtshof, Decision no. G 47/2012, 27 June 2014.

78 Romania, Curtea Constituțională, Press release, 8 July 2014.

79 Slovenia, Ustavno sodišče, Judgement of 3 July 2014.

80 Slovakia, Ústavný súd (2014), Resolution No. PL. ÚS 10/2014-29 of 23 April 2014.

81 Belgium, Human Rights League (*Liga voor Mensenrechten/ Ligue des Droits de l'Homme*) (2014), 'Big Brother Awards 2014 – Dataretentiewet', p. 9; Jespers, R. (2014), 'Europees Hof van Justitie vernietigt de dataretentierichtlijn van de Europese Unie', De Wereld Morgen, 12 April 2014.

82 Bulgaria, Supreme Administrative Court (*Върховен касационен съд*) (2014), Statement by the Supreme Administrative Court of the Republic of Bulgaria on the request of the Ombudsman of the Republic of Bulgaria for declaring unconstitutional the provisions of Article 250a–250d, Article 251 and Article 251a of the Electronic Communications Act (*Становище на Върховния касационен съд на Република България по искането на Омбудсмана на Република България за установяване на противоконституционност на разпоредбите на чл. 250а–250е, чл. 251 и чл. 251а от Закона за електронните съобщения*).

83 Cyprus, Supreme Court, Appeal Jurisdiction, *Attorney General v. Andreas Isaiah et al.*, 7 July 2014.

84 Spain, Judgment of the Spanish High Court (Criminal Division) nº 15/2014, 24 June 2014.

85 Netherlands, Court of Appeal (*Gerechtshof*) (2014), Case no. 23-005230-12, ECLI:NL:GHAMS:2014:2028, 27 May 2014.

86 *Ibid.*

87 Cyprus, Bill regulating the identification of persons in possession and users of pre-paid mobile telephony equipment and services and other related matters (*Πρόταση νόμου που ρυθμίζει την ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας προπληρωμένου χρόνου ομιλίας και άλλα συναφή θέματα*).

88 Germany, Bundesregierung (2014), Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz.

89 Romania, Referral no. 2/6103 of 23 December 2014 to the Constitutional Court, made by 69 Members of Parliament belonging to the National Liberal Party (*Grupil Parlemenrae al Partidului Național Liberal, Sesizare 2/6103*).

90 Croatia (2014), Amendments of Electronic Communications Act (*Zakon o izmjenama i dopunama Zakona o elektroničkim komunikacijama*), Narodne novine No. 71/14.

91 United Kingdom, Data Retention and Investigatory Powers Act, 17 July 2014.

92 *The Guardian (2014),* 'Academics: UK "Drip" data law changes are "serious expansion of surveillance"', 15 July 2014.

93 Finland, *Tietoyhteiskuntakaari/Informationssamhällsbalken*, no. 917/2014.

94 Denmark, Ministry of Justice (*Justitsministeriet*) (2014), 'Justitsministeren ophæver reglerne om sessionslogning', Press release, 2 June 2014.

95 Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2013–2014), Parliamentary Documents (*Handelingen*), No. 72, no. 2.

96 Finland, *Tietoyhteiskuntakaari/Informationssamhällsbalken*, no. 917/2014, and *Pakkokeinolaki/Tvångsmedelslag*, no. 806/2011.

97 Luxembourg, Le Gouvernement du Grand Duché du Luxembourg, Ministère de la Justice (2014), 'Conséquences de l'arrêt de la Cour de Justice de l'Union européenne du 8 avril 2014 dit „digital rights', Press release, 26 September 2014.

98 Lithuania, Order of the Minister of Justice on the formation of Working Group No. 1R-200 (*Lietuvos Respublikos teisingumo ministro įsakymas dėl darbo grupės sudarymo Nr. 1R-200*), 27 June 2014.

99 Bulgaria, Commission for Personal Data Protection (*Комисия за защита на личните данни*) (2014), 'Invalidation of Directive 2006/24/EC on data retention: What comes next?' ('*Отмяна на Директива 2006/24/ЕО за задържане на трафичните данни. Какво следва?*'), Information Bulletin (*Информационен бюлетин*), No. 4(49)/2014, pp. 13–15.

100 Estonia, Chancellor of Justice (*Õiguskantsler*), Notice no. 6-1/140621/1403065, 15 July 2014.

101 Greece, Data Protection Authority (*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*).

102 Netherlands, State Secretary for Security and Justice (*Staatssecretaris van Veiligheid en Justitie*) (2014), *Conceptwetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens*.

103 Germany, Bundesministerium der Justiz, *Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet*.

104 See for example European Digital Rights (EDRI) (2011), *Shadow report on the Data Retention Directive (2006/24/EC)*, Brussels, EDRI, p. 24.

105 European Commission (2010), 'Data retention is here to stay', Press release, 3 December 2010.

106 Slovenia, Constitutional Court (*Ustavno sodišče Republike Slovenije*), Case U-I-65/13-19, 3 July 2014.

107 TASZ (2014), 'A TASZ bepereli a Telenort és a Vodafone-t az adatmegőrzés megszüntetéséért', Press release, 7 October 2014.

108 ZDNet news (2014), 'Four of Sweden's telcos stop storing customer data after EU retention directive overthrown', 11 April 2014.

109 *The Register* (2015), 'Danes mull session logging law despite EU data retention ban', 15 January 2015.

110 European Commission (2011), *Proposal for a Directive of the European Parliament and 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.

111 For instance, the Joint Statement of the ministers of the Interior of twelve Member States of 11 January 2015.

112 European Parliament (2014), 'MEPs refer EU–Canada air passenger data deal to the EU Court of Justice', Press release, Brussels, 25 November 2014.

113 Avramopoulos, D. (2014), Exchange of Views between Commissioner Dimitris Avramopoulos and MEPs at the LIBE Committee in the European Parliament, Speech/14/2351, 3 December 2014.

114 FRA (2014), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*.

115 FRA (2011), *Opinion on the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, FRA Opinion 01/2011, Vienna, FRA.

116 European Council (2014), *Conclusions*, EUCO 79/14, Brussels, 27 June 2014.

117 European Council (2014), *Conclusions*, EUCO 163/14, Brussels, 30 August 2014.

118 UN, Security Council (2014), Resolution 2178 (2014), S/RES/2178 (2014), 24 September 2014.

119 Council of the European Union (2014), Council conclusions on development of a renewed European Union Internal Security Strategy, Brussels, 4 December 2014.