Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	42 months

Deliverable 6.8:

The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive

Authors:	Elspeth Guild and Sergio Carrera (CEPS)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 January 2014
Submission date:	27 May 2014

Abstract

This policy brief examines the challenges facing the EU regarding data retention, particularly in the aftermath of the Court of Justice of the European Union (CJEU) judgment Digital Rights Ireland of April 2014, which found the Data Retention Directive 2002/58 to be invalid. The paper first offers a brief historical account of the Data Retention Directive and then moves to a detailed assessment of what the judgment means for determining the lawfulness of data retention from the perspective of the EU Charter of Fundamental Rights: what is wrong with the Data Retention Directive and how would it need to be changed to comply with the right to respect for privacy? The policy brief also looks at the responses to the judgment from the European institutions and elsewhere, and presents a set of policy suggestions to the European institutions on the way forward. It is argued here that one of the main issues underlying the Digital Rights Ireland judgment has been the role of fundamental rights in the EU legal order, and in particular the extent to which the retention of metadata for law enforcement purposes is consistent with EU citizens' right to respect for privacy and to data protection. The paper offers three main recommendations to EU policy makers: first, to give priority to a full and independent evaluation of the value of the data retention directive; second, to assess the judgment's implications for other EU large information systems and proposals which provide for the mass collection of metadata from unsuspected persons, in the EU; and third, to adopt without delay the proposal for Directive COM(2012)10 dealing with data protection in the fields of police and judicial cooperation in criminal matters.

Document history

Version	Date	Changes
1.0	27 May 2014	

Introduction

Since the Snowden revelations on PRISM and USA surveillance programmes began in June 2013,[1] the public in Europe has become accustomed to a whole new vocabulary around data, including such terms as metadata, bulk data collection, data retention and storage, and many other technical terms. While this language was formerly reserved for internet experts, an increasing number of us presume to know what these terms actually mean. This new literacy comes at a price for the European Union – one which is both political and also judicial,[2] as we discovered in the second week of April 2014. In this policy brief, we examine the EU challenge regarding data retention and the fall-out from *Digital Rights Ireland*, the 8 April 2014 landmark judgment of the Court of Justice of the European Union (CJEU), which found the Data Retention Directive to be invalid.[3] We will first give a short history of the Data Retention Directive; secondly, we will examine what the judgment means for future data retention; we will then look at the responses of the European institutions to the judgment, and the current turbulence concerning data retention. Finally the policy brief offers some policy suggestions on the way forward.

Section 1 – What is the Data Retention Directive?

Providers of publicly available electronic communications services, and of public communications networks, process substantial amounts of personal data to do with communications, billing, interconnection payments, marketing, and other activities. Along with this information, there are data concerning details of sources, destinations, dates, times, and types of communication, as well location information in respect of mobile phone use. This information is normally called 'metadata'. While the actual content of communications remains private and is therefore protected by the right to privacy, metadata has been seen as a fairly nebulous concept and not so obviously jeopardizing the EU Charter of Fundamental Rights. This premise has been at the heart of the discussion surrounding the Data Retention Directive.

[1] Refer to D. Bigo et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", CEPS Liberty and Security Series, No. 62, November, Brussels.

[2] C-293/12 & C-594/12, *Digital Rights Ireland*, April 2014, Court of Justice of the European Union.

[3] Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15.3.2006, L 105/54, 13.4.2006.

Over ten years ago, the EU adopted the Directive 2002/58 on privacy and electronic communications (ePrivacy Directive)[4] which required that metadata ('traffic data' for the purposes of the Directive) must in principle be deleted or made anonymous as soon as it is no longer needed for billing purposes, unless the subscriber agrees to its retention.[5] By as early as 1997, a number of people and organisations within the EU, primarily in the law enforcement world, had sought an exemption from the obligatory deletion of metadata so that operators would be required to retain metadata for law enforcement purposes. The result was Directive 97/66 which did no more than permit member states to adopt such legislation for the protection of public security, defence, or public order, including the economic well-being of the state.[6] This exception was then incorporated into the ePrivacy Directive allowing for a number of derogations from the principle of deletion which could be employed by member states. Variations in the ways in which different member states used these derogations caused some operators to cry foul as they were subject to very different rules depending on the member state.

While this debate was going on, the bombings of the railway station in Madrid occurred on 11 March 2004, heightening anxiety in the EU about potential terrorist attacks. This was followed a year later by the attacks on the London Underground on 7 July 2005. These outrages strengthened the argument that more surveillance was needed in the EU, including on telecommunications metadata, to protect against acts of political violence. The result of this convergence of security concerns and private sector lobbying was the European Commission's proposal for a Data Retention Directive. Adopted in 2006, the original objective of the Data Retention Directive (2006/24), as set out in its preamble, was primarily to prevent and detect criminal offences, in particular organised crime and terrorism. The internal market objective of harmonising retention periods across the member states became of secondary concern.

The Directive requires service providers to retain details of all telephone, mobile, and internet communications (i.e. metadata) for periods of between no less than six months and no more than two years from the date of the communication.[7] The choice of the exact period of time has been left in hands of member states' national legislatures. Data retention is however different from data preservation (or 'quick freeze'). The latter occurs 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. Data preservation is a specific targeted law

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[5] The ePrivacy Directive was revamped somewhat in 2009, and in 2013 the institutions adopted a new Regulation (611/2013) beefing up the sanctions on those who fail to comply with the privacy obligations contained in the Directive.

[6] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 024, 30.1.1998.

[7] Article 6 of the Data Retention Directive.

enforcement measure managed by judicial authorities across the EU member states and often used as a less intrusive alternative to data retention. In the case of preservation, a judge must be convinced that it is necessary in a specific case of law enforcement to quick-freeze someone's data.[8] Thus the criminal justice systems control the issuing of data preservation orders, and these institutions are familiar with the necessity of acting within the confines of due process and fair trial.

Data retention, on the other hand, is the collection of bulk metadata. Everyone's data is collected without the requirement of any suspicion or the intercession of a judge. It is the job of individuals and organisations in the private sector to retain the metadata (tapping into a whole new industry of data warehousing).[9] While the preamble to the Data Retention Directive refers to law enforcement authorities in three places (twice in Preamble 9 and once in Preamble 14) and declares itself compliant with the European Convention of Human Rights (ECHR), in the text Article 4 permits member states to allow access to data retained by whatever competent law enforcement agency it chooses. Thus there is no necessary monopoly of criminal justice authorities over access to the data. Member states could allow their intelligence services to have access to the data (as the US authorities have done in respect of PRISM).[10] Access to data is not confined to specific criminal investigations, and there is no need for states to make access subject to judicial scrutiny. These are among the aspects of data retention which have caused the most concern, as it is hard to escape the conclusion that retention of the data is arbitrary and access to it is unlimited.

The transposition of the Data Retention Directive did not run smoothly. Although it had a deadline of 15 September 2007, by the time the Commission issued its first report on the Directive in 2011 (COM(2011)225), only 25 out of 27 Member States

[8] There is also the possibility of what is called Quick Freeze Plus – which is where a judge orders the retention of all data still held by operators either before or after the date of the freezing order. These tools are used by EU law enforcement authorities which provide assistance to one another in the context of the Council of Europe's Convention on Cybercrime.

[9] For instance, IBM offers potential customers "IBM DB2® [which] delivers data warehousing capabilities that help organizations extract insight from all types of data, delivering the information on time and in context so that business leaders can derive actionable insights for faster, more efficient decision making" (www14.software.ibm.com/webapp/iwm/web/signup.do?source=sw-infomgt&S_PKG=ov12031&S_CMP=DB2_accelerate_analytics_wp&csr=wwus_imbluawfastlane-20130912&cm=k&cr=google&ct=109HF38W&S_TACT=109HF38W&ck=data_warehouse_technologies&cmp=109HF&mkwid=sWDa2R7An_3372041974 2_43246d30503); Oracle claims: "Oracle Database is the industry foundation for high performance scalable, optimized data warehousing. Oracle Exadata Database Machine is a complete, optimized, hardware and software solution that delivers extreme performance and database consolidation for data warehousing" (www.oracle.com/us/products/database/datawarehousing/overview/index.html?sckw=srch:data_warehousing&SC=srch:data_warehousing&mkwid=solCaMUx8|pcrid|28179689698|pkw|data%20warehousing|pmt|e|pdv|c). With such enticing opportunities available to the private sector via metadata it is not surprising perhaps that the law enforcement world also wanted to benefit from these new insights.

[10] D. Bigo et al. (2013), "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU", CEPS Policy Brief No. 293, Centre for European Policy Studies, Brussels, June.

had transposed it in national law.[11] Austria and Sweden, which had no laws on data retention, still only had draft legislation on the table. Belgium had partially transposed the directive. Constitutional courts in Romania (2009), Germany (2010), Bulgaria (2010), the Czech Republic (2011) and Cyprus (2011) had found legislation to implement the directive to be unconstitutional, unjustifiably intrusive, or both. In some cases it was found that the Directive itself was unconstitutional.[12] The Commission began infringement proceedings against a number of member states. On 30 May 2013, the CJEU found against Sweden in one of these proceedings and it was ordered to pay €3 million for its failure to transpose the Directive.[13] The Commissioner for the Directorate General for Home Affairs Cecilia Malmström confirmed to the European Parliament on 16 April 2014 following the CJEU judgment against the directive, that it would be reimbursing the Swedish government the full €3 million, although nothing was mentioned about interest.[14] The Commissioner also confirmed that the outstanding infringement proceedings against Germany would be withdrawn, although she did not mention whether the Commission would be paying Germany's legal costs. In 2006 a new political party was established in Sweden, the Pirate Party, committed to freedom on the internet and bitterly opposed to the data retention directive. In 2009 it gained its first seat in the European Parliament.[15] So the Directive was not only causing judicial trouble in some member states, but also seemed to be assisting the creation of a new political party in one of them, on the basis of implacable opposition to it.

As regards use of metadata by police (though little is known about access by intelligence services), the Commission, in something of a push back, published figures on law enforcement requests in 2008, the most recent data available.[16] Notwithstanding substantial problems with quality of the information, which the Commission openly acknowledges, as far as it was able to determine there had been a total of about 1.5 million requests by law enforcement agencies to retained data. About one third (480, 000 requests) of these was for data which had been stored for less than three months. Thereafter the drop-off rate in relation to number of requests is dramatic.[17] Similarly the differences among the member states' practices are startling. German law enforcement agencies made a total of

[11] European Commission, "Evaluation Report on the Data Retention Directive (2006/24)", COM(2011) 225 final, Brussels, 18.4.2011.

[12] See Statewatch (www.statewatch.org) and FP7 Project SECILE documents (http://eulawanalysis.blogspot.fr/2014/04/national-legal-challenges-to-data.html).

[13] http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-05/cp130066en.pdf

[14] www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN

[15] www.theguardian.com/technology/blog/2009/jun/08/elections-pirate-party-sweden

[16] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf

[17] According to the same Commission statistics the total requests for retained traffic data between 21 and 24 months of age were only 1.634 in 2008 (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf).

12,684 requests in 2008 while their French counterparts made 503,437. After the French, the UK agencies were the next most devoted users, making 470,222 requests.

At the plenary debate on the subject in the European Parliament on 16 April 2014, concerns were raised over the lack of evidence proving the effectiveness of the Data Retention Directive in the fight against crime and terrorism.[18] The problem of efficiency of metadata collection, retention, and access as a tool for law enforcement remains. The US government's Privacy and Civil Liberties Oversight Board issued its report on NSA mass surveillance on 23 January 2014. This sets out much detail about the legal challenges and other issues around the NSA bulk metadata collection and access programmes.[19] Among the curious aspects of the report is a similar problem to the one inherent in the Data Retention Directive: the difficulty of properly substantiating the effectiveness of using metadata in the fight against serious crime and terrorism.

Notwithstanding the political debates and challenges around bulk metadata retention and access, the issue did not emerge as a legal challenge at the EU level until 2012 (after six years of the Directive's life) when national courts in Austria and Ireland referred specific questions to the Court of Justice of the European Union (CJEU) in Luxembourg. During that period one particularly significant event for the validity of the Directive took place: the Lisbon Treaty came into force on 1 December 2009, making the EU Charter on Fundamental Rights (EU Charter) legally binding. Although this EU Charter had been in existence since 2000, it was only incorporated into the EU treaties in 2009 when it was given the same status as the treaties themselves.[20] This proved important in the judicial events which followed and which we now discuss below.

Section 2 – Why did the CJEU find the Data Retention Directive invalid?

The first time the CJEU was required to think about the Data Retention Directive was in 2006 when the Irish Government took an action against both the European Parliament and the Council over the legal basis of the directive in the case C-301/06 *Ireland v. The European Parliament*.[21] The Irish Government argued that the fundamental purpose of the Directive was law enforcement, not the completion

[18] www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN

[19] www.pclob.gov/meetings-and-events/2014meetingsevents/23-january-2014-public-meeting

[20] Article 6.1 Treaty on European Union.

[21] C-301/06, *Ireland v European Parliament and Council*, 10 February 2009.

of the internal market, and so it should not be adopted under the provisions relating to the latter (as had been done). The CJEU decided this case in 2009 and found that the Directive regulated operations which are independent of the implementation of any police and judicial cooperation in criminal matters. According to the Court, it harmonised neither the issue of access to data by the competent national authorities nor that relating to the use and exchange of those data between those authorities so it could correctly be adopted as an internal market measure. But it is striking in light of the same court's subsequent judgment on the validity of the Directive that it was complacent about the legal basis on which it had been adopted. Bearing in mind the importance of the fight against serious crime and terrorism in the preamble and origins of the Directive[22] there seems to be a certain inconsistency with the CJEU's finding, which might perhaps relate to the lack (by then) of a sound fundamental rights treaty. The decision was published on 10 February 2009, almost 10 months before the Lisbon Treaty would change the relation of EU law to fundamental rights with the 'lisbonisation' of the EU Charter into a legally binding component of primary law.[23]

But this judgment predates the controversy which broke out in the EU member states' constitutional courts over the implementation of the Directive, which commenced only in 2009. This revolt of the national courts is perhaps important in considering what some might call the CJEU's more strict approach to the Data Retention Directive in the case C-293/12 & C-594/12 *Digital Rights Ireland* of April 2014. The issue became one about the role of fundamental rights in the EU legal order. In particular: is the retention of our metadata for law enforcement purposes consistent with EU citizens' right to respect for privacy (Article 7 EU Charter) and to data protection (Article 8 EU Charter)?

The CJEU handed down its decision on 8 April 2014 and simply found that "Directive 2006/24… [was] invalid". The Court did not limit the temporal effect of the judgment. Therefore, it can be assumed that the invalidity of the Directive took effect from the date of its entry into force back in 2006. The CJEU expressly stated: "Directive 2006/24 entails a wide-ranging and particularly serious interference with [the right to respect for privacy and data protection] in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".

[22] Refer to Justice and Home Affairs Council 2626 Council Meeting, 2 December 2004, 14894/04, Brussels. See also the European Council Declaration on Combating Terrorism, Brussels, 25 March 2004.

[23] The reservation by the CJEU to examine in *Ireland v. Parliament and Council* any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24 was interpreted by Advocate General Villalón in two ways: first, the CJEU was not called to interpret the Data Retention Directive in light of the EU Charter and particularly the right to privacy; and second, despite the validation of the legal basis of the Directive, the CJEU did not examine its proportionality in relation to the interference with fundamental rights. Refer to paragraphs 81 to 86 of the Opinion. Opinion of Advocate General Cruz Villalón, Case C-293/12, 12 December 2013.

Needless to say, this came as something of a shock to the EU institutions which participated in drafting and passing the Directive. It seems a majority of them were asleep on the job when it came to protecting EU citizens' privacy while addressing the pressures emerging from the Madrid and London bombings. Only the European Data Protection Supervisor (EDPS) comes out of this affair looking good, as that office had consistently warned that the Directive was not compliant with the EU Charter.[24] In addition to the two countries from which the references were made (Ireland and Austria), a number of other member states intervened in the case before the EU's highest court: Spain, France, Italy, Poland, and the UK in support of the Directive, and Portugal against it. The European Parliament, Council, and Commission all intervened in support of the Directive, while the Irish Human Rights Commission, which was also a party to the case, opposed it. What was the reasoning of the CJEU?

First, the Court confirmed that the amount and precision of the data covered by the Data Retention Directive allowed very precise conclusions to be drawn concerning people's private lives: everyday habits, permanent and temporary residences, where people go, who they meet and places they visit. It permitted state authorities to access all this data directly and specifically and thus it affected the private lives of everyone in the EU. This conflicted with the right to respect for private life which is protected by Article 7 of the EU Charter[25] and it therefore must be considered to be considered to be particularly serious interference.[26] This finding was a one of the strongest feature of the argument that access to and collection of metadata is not an interference with privacy simply because the authorities do not have access to the content of communications such as e-mails and phone conversations. For the EU now, access to or collection of 'metadata' is by definition an invasion with privacy. Whether or not the authorities then have access to the content of the communications is another matter and does not influence the finding that metadata collection and access is, in itself, an interference with privacy.[27] The CJEU held that "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[28] This corresponds with the Advocate General Cruz Villalón's opinion when he argued that "the vague feeling of surveillance" as a consequence of data

[24] http://europa.eu/rapid/press-release_EDPS-11-6_en.htm

[25] Refer to paragraphs 34 and 35 of the judgment.

[26] Paragraph 37 of the ruling.

[27] The CJEU here makes reference to the jurisprudence of the European Court of Human Rights on the subject. As the court in Strasbourg has yet to decide on the specific issue of metadata collection and access (though a case is pending before it on the subject) it will be interesting to follow whether there is an influence from one European supranational court on another. Refer to *Big Brother Watch and Others v. the United Kingdom* (no. 58170/13), which deals with a challenge against the surveillance on electronic communications programmes by UK secret services (GCHQ) following the Snowden revelations and their incompatibility with Article 8 of the ECHR.

[28] Paragraph 53 of the judgment.

retention can have a decisive influence on the exercise by EU citizens of their freedom of expression and information,[29] and additionally emphasised that

> ...the collection and, above all, the retention, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period.[30]

Yet, according to the CJEU, the interference is not so enormous as to negate the essence of the right to privacy as such.[31] What this means is that the interference does not result in the Data Retention Directive being thrown out altogether as destroying the essence of privacy. Instead, what is required is that the interference be justified in each case. There are two stages to the justification requirement, or legality test. The first is the determination whether there are adequate grounds for the interference. The second is to determine whether the justification is proportionate in light of its objective and the severity of the interference with the fundamental right to privacy.

As regards the first stage, any interference with a person's private life (which does not destroy the essence of the right) has to be justified if it is to be lawful. The EU institutions justified the Directive's interference on the grounds of its value in the fight against serious and organised crime, and against terrorism. The Court accepted these grounds as satisfying the test.[32] This is interesting when compared

---

[29] See paragraphs 52 of the opinion.

[30] Paragraph 72 of the opinion.

[31] Paragraph 39 of the judgment stresses that "... even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such". Also, in paragraph 40 the CJEU added that "Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data."

[32] See paragraph 41 which stipulates that "As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in

with the position of the CJEU in the earlier case *Ireland v European Parliament and Council* where the legal basis was at issue. There it was the Directive's place in the internal market project which justified its existence. The law enforcement aspect, according to the CJEU at that time, was a side effect. In the 2014 judicial consideration of the Directive, law enforcement becomes the central question, and the only ground for justifying an interference with the right to respect for privacy on the basis of public policy and security. This acceptance by the Court is also remarkable given that the European Commission 2011 evaluation report on the Directive COM(2011) 225, cited above, did not provide convincing evidence for the value of data retention for law enforcement purposes. Indeed, the necessity of data retention as a law enforcement technique has been contested since its inception.[33] In his opinion on the Commission proposal of 2005, the EDPS said he was not convinced by the assumption of its necessity and called for further evidence.[34] In the opinion published in May 2011 on the Commission evaluation report,[35] the EDPS concluded that on the basis of the available quantitative and qualitative findings it remained doubtful whether the European Commission could conclude that data retention was considered necessary for law enforcement by most member states, and there is still a problematic lack of evidence substantiating its value.[36]

The second part of the test which the Directive must pass is whether it is proportionate to attain the legitimate objective pursued or whether it exceeds the limits of what is appropriate and necessary to achieve the objective. According to the CJEU, because the interference is substantial and particularly serious, the EU legislature's discretion is reduced and the review of that discretion should be strict[37], but that since retained data may be a valuable tool for criminal

---

its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security." The CJEU continues by arguing in paragraph 43 that "In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime."

[33] See for instance the letter addressed to Commissioner for Home Affairs by a group of civil society organisations and individuals the 22 June 2010 and considering the intrusive nature of the directive unacceptable (www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf).

[34] European Data Protection Supervisor, opinion on the proposal for a data retention directive, of 26 September 2005, OJ 2005, C298/1.

[35] European Data Protection Supervisor opinion on the evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), May 2011, Brussels.

[36] Ibid. Refer to paragraphs 40 and 41 of the opinion. The EDPS concluded in paragraph 44 that "After careful analysis, the EDPS takes the view that, although the Commission has clearly put much effort into collecting information from the Member States' governments, the quantitative and qualitative information provided by the Member States is not sufficient to confirm the necessity of data retention as it is developed in the Data Retention Directive. Interesting examples of its use have been provided, however, there are simply too many shortcomings in the information presented in the report to allow general conclusions on the necessity of the instrument. Moreover, further investigation into alternative means should still be done. These two points will now be further elaborated."

[37] Paragraph 48 of the ruling.

investigations the objective is appropriate. The CJEU found, though, that while the fight against serious and organised crime and terrorism is of great importance for public security it does not justify the Directive. The right to privacy means that all exceptions must be interpreted narrowly.[38] The Directive itself is an exception to the right. At this point, the CJEU clarifies that the duty of data protection in Article 8 of the EU Charter is especially important for the right to respect for private life in Article 7 EU Charter. The principal right is that to respect for private life which is found in Article 7.[39] The state's obligation to ensure data protection is a corollary obligation, the purpose of which is to ensure the respect for private life in those situations where people consent to the collection and use of their data, or there are exceptions to the consent rule.

So, what is wrong with the Data Retention Directive and how would it need to be changed to comply with the right to respect for privacy? According to the CJEU it should respect the following set of ten standards for it to pass the legality test:

1. the Directive should lay down clear and precise rules governing its scope and application.
2. it must provide minimum safeguards to protect personal data against abuse, and set out clear safeguards against any unlawful access to the data.
3. where personal data is subject to automated processing the rules must be even stricter than where it is not so subject.
4. there needs to be differentiation among electronic communication and traffic data in light of the objective of fighting serious crime.
5. there need to be limits on the personal data collected – e.g. a particular period of time, geographic zone, or circle of specific people. The current blanket collection of everyone's data which includes even communications subject to the obligation of professional secrecy is unacceptable.
6. the limits need to be informed by objective criteria related to the purposes – prevention, detection, or criminal prosecutions concerning offences ('serious crime' by reference to national law is not acceptable).
7. there must be substantive and procedural conditions set out in the Directive which control national authorities' access to the data and its use (the current rules in the Directive are insufficient); the procedures must be strictly tied to the purpose of the interference.
8. there need to be objective criteria regarding who is authorised to access the data, and those criteria must be strictly necessary to achieve the objective.
9. competent national authorities or an independent administrative body should carry out a review prior to any request to access the data, to ensure that this is limited to what is strictly necessary for the objective. The prior review body should consider every request for access to the

[38] Refer to paragraph 52 of the judgement.

[39] Paragraph 53.

data following a reasoned request from the law enforcement authorities seeking access in order to ensure that the access, if permitted, is strictly necessary to achieve only the identified legitimate objectives.

10. different categories of data must be subject to different periods of retention which are clearly explained and justified on the basis of objective criteria in pursuit exclusively of the legitimate aim.

This is the first package of criteria which a Data Retention Directive would need to have to be in conformity with Article 7 Charter, the right to respect for private life. The CJEU then considered a second set of criteria, the data protection requirements (Article 8 Charter), which relate to the rules for private sector organisations storing the data. For a Directive on Data Retention to be compatible with the EU Charter, this must also be addressed. What is needed, according to the CJEU would be:

- First, clear rules to protect the retained data, which take into account the vast quantity of data, its sensitivity, and the risk of unlawful access; these rules must ensure the integrity and confidentiality of the data's retention;
- Second, a high level of security to be accorded by the providers by means of technical and organisational measures, notwithstanding the possible costs of implementing security;
- Third, the irreversible destruction of the data at the end of the data retention period;
- Fourth, the retention of the data exclusively in the EU as otherwise the independent compliance authority might not be able to provide protection to individuals with regard to processing of personal data.[40] This criterion is of particular importance to the legal protection and political dilemmas raised by the Snowden PRISM revelations as well as cloud computing.[41]

Not surprisingly, this list of essential elements and legal standards for any future revision of the Data Retention Directive poses a number of challenges for the EU institutions. In the next section we will examine the first reactions to the judgment.

[40] This standard is laid down in paragraph 68 of the judgment which states that "... it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 *Commission* v *Austria* EU:C:2012:631, paragraph 37)."

[41] Cloud computing has been defined as "the distributed processing of data on remotely located computers accessed through the Internet" and the data transfers taking place in its context engage a multiplicity of data centres dispersed across various legal jurisdictions and a multiplicity of private actors. Cloud computing has been developed as "a new business model for the private sector to commoditise the extraneous capacities of their data centres". For a more developed analysis of this definition and the political and legal challenges of cloud computing refer to D. Bigo et al. (2012), "Fighting Cybercrime and Protecting Privacy in the Cloud", European Parliament Study, DG Internal Policies, Brussels.

Section 3 – What were the reactions to the *Digital Rights Ireland* decision?

After 8 April, there was something of a hush across those institutions which had been following the case closely. The enormity of the calamity which had befallen the Directive took a little while to sink in. The only EU institution to welcome the judgment was the European Data Protection Supervisor (EDPS) who said in a press release that he considered it a landmark judgment that limited the blanket government surveillance of communications data.[42] The EDPS was particularly satisfied that the CJEU had underlined that the Directive constituted a serious and unjustified interference with the fundamental right to privacy in the EU Charter. He said the finding that retention of communications data must be duly specified and used only in very specific contexts was very important. The purposes must be precisely defined and clearly limited and responsibility cannot be left to member states in this regard. The EDPS added that the judgment means that "the EU should take a firm position in discussions with third countries, particularly the USA, on the access and use of communications data of EU residents." With one sentence the EDPS put his finger on one of the most sensitive aspects of the judgment.

By contrast, DG Home Affairs of the Commission issued only one press release over the following days, on 10 April, congratulating law enforcement agencies across the world and EUROPOL for joining forces with airline, travel, and credit card industries on 8 and 9 April for coming together

> to combat the purchase of airline tickets with stolen credit cards. This initiative - the second of its kind - took place at 68 airports in 32 countries worldwide, including 24 EU Member States, Iceland, Norway, Switzerland, the USA, Colombia, Brazil, Peru and Ukraine. In an unprecedented move, representatives from 35 airlines and major credit card companies Visa Europe, MasterCard and American Express worked with staff from Europol's EC3, law enforcement officers from across the EU, the US Secret Service, the US Immigration and Customs Enforcement and the Colombian national police at Europol's operational centre to identify suspicious airline ticket transactions resulting from the use of fake or stolen credit cards via the Internet.[43]

While it is doubtless important to address the use of stolen credit cards, the timing of the press release, which presupposes that substantial amounts of personal data were exchanged across the public and private sectors in many countries, seems unfortunate. DG Justice of the Commission issued a press release a few days later on 14 April on the growing importance of the EU Charter to protect the fundamental rights of EU citizens, but with reference only to new moves on gender equality. The 4th Annual Report on Application of the EU Charter of Fundamental Rights, published by the Commission the same day has no mention of privacy and only two on data protection, one regarding its effort to negotiate a new data protection

[42] https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Pressnews/pressreleases/PR2014

[43] http://ec.europa.eu/dgs/home-affairs/what-is-new/news/index_en.htm

standard,[44] and the other regarding the independence of the Austrian data protection authority.

The Council over those days was occupied with the situation in Ukraine and issued no press release mentioning the judgment. The Council Legal Service issued a confidential opinion on the relevance and implications of the judgment which is analysed below.[45] The European Parliament (EP) issued several parliamentary questions to the Commission[46] and discussed the judgement in its final plenary session on 16 April 2014. It invited the Commissioner of DG Home Affairs to attend and give some initial feedback. Commissioner Malmström advised the EP that "we have already started the reflection on whether there is a need or not for a new legislative proposal. This, in that case, would be for the next Commission to take up. The judgment of course underlines the need for a swift adoption of the proposed data protection reform and, in particular, the draft directive which applies to the law enforcement sector."

The possibility that the Commission would make no further proposal on the subject undoubtedly took some by surprise. Should the Commission follow this approach, the matter would then be one for the member states and the consistency of national rules on data retention would be uncertain - precisely the complaint of the private sector before the adoption of the Directive. No doubt the member states could reach agreement on data retention periods without a directive and indeed the Council of Europe could be a forum where discussion could take place on this. But, as Commissioner Malmström indicated during her intervention, there is still a need for a directive on data protection in the context of law enforcement activities (police and judicial cooperation in criminal matters) which fall outside the material scope of the Data Protection Directive 95/46/EC.[47]

Indeed, and in order to address this gap, early in 2012 the European Commission launched the 'data protection reform legislative package', which is composed of two main legislative proposals, the general data protection Regulation (COM(2012)11)[48] and the Directive (COM(2012)10) dealing with data protection in the fields of police

[44] "The aim of the reform is to put individuals back in control of their data by updating their rights (Article 8). Explicit consent, the right to be forgotten, the right to data portability and the right to be informed of personal data breaches are key elements. They will help to close the growing rift between citizens and the companies with which they share their data, willingly or otherwise" paragraph 3.1.2 COM(2014)224.

[45] Refer to Council of the European Union, Judgment of the Court of 8 April 2014 and invalidation of the Directive 2006/24, 9009/14, 5 May 2014, Brussels. Retrievable from statewatch.org

[46] See www.europarl.europa.eu/plenary/en/parliamentary-questions.html#sidesForm

[47] Directive 95/46/EC of the European Parliament and 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 L 281, 23.11.1995.

[48] European Commission, proposal for a regulation 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), COM(2012) 11 final, 25.1.2012.

and judicial cooperation in criminal matters.[49] The negotiation processes of both initiatives are still ongoing and have proved to be extremely controversial, with certain EU member states and representatives from the private sector expressing concerns about the economic implications of a stronger EU data protection regulatory framework. Of particular concern has been the lack of progress in the negotiations on the proposal for a directive covering law enforcement, which appears to be still in a stalemate,[50] as the processing of personal data for the purposes of crime prevention constitutes a domain where certain national governments are still reluctant to transfer greater powers of scrutiny to the EU. Indeed, some of the current provisions suggested by the proposal would be of direct relevance to data retention.[51] It may therefore be that the Commission is only using the threat of no further action as a bargaining position to help the Council reach agreement on the directive in a form which would fulfil the terms laid down by the CJEU in the *Digital Rights Ireland* judgement.

The implications of the judgment, however, are much wider than the one directive. As Commissioner Malmström admitted to the EP, the clarification of the right to respect for privacy and data protection in the Charter also has implications for at least two agreements already in force in collaboration with the USA: the Passenger Name Record Agreement (PNR) and the Terrorist Finance Tracking Programme (TFTP). In 2011 the EU and the US agreed on a new PNR Agreement regulating the transfer of passenger name records by air carriers to the US for use by US authorities in the prevention, detection, investigation, and prosecution of terrorism and certain transnational crimes. While the Commission robustly defends the data

[49] See European Commission, proposal for directive 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, COM(2012) 10 final, 25.1.2012, Brussels. See D. Bigo et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament", European Parliament, DG Internal Policies, Brussels (www.ceps.be/book/towards-new-eu-legal-framework-data-protection-and-privacy-challenges-principles-and-role-europ).

[50] Refer to European Parliament legislative resolution of 12 March 2014 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 (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)) (Ordinary legislative procedure: first reading) (www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0219&language=EN&ring=A7-2013-0403).

[51] Refer for instance to Article 9, which deals with measures based on profiling and automated processing, or the new Article 9a introduced by the European Parliament, which covers general principles for the rights of the data subject. Article 9 as amended by the Parliament states in section 2a that "Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed or will be committing a criminal offence shall only be lawful if and to the extent that it is strictly necessary for the investigation of a serious criminal offence or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the State, or the life of persons." See also Articles 4, which deals with principles which member states would have to respect in relation to data processing, and the new Articles 4a and 4b introduced by the European Parliament. See www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0219&language=EN&ring=A7-2013-0403

protection provisions which have been included in the agreement, there has been little improvement since the last agreement, which has been heavily criticised for its data protection failures.[52] Furthermore, the Commission itself has put on the table a proposal for an EU PNR Directive which is still in the legislative process.[53] The Commissioner was adamant that this proposal was compliant with the CJEU judgment, although her justification was based exclusively on the limitations on processing data and the effectiveness of safeguards. This may not be sufficient to satisfy the CJEU.

When assessing the proportionality of the EU PNR proposal and the systematic flagging of passengers which would be inherent to the system, the European Union Agency for Fundamental Rights (FRA) in Vienna made a direct parallel with the Data Retention Directive and the questions over its lack of proportionality raised by the constitutional courts of various EU member states. The FRA concluded that "The same reasoning could also be applied to the proposed EU PNR system for it, too, foresees data collection and analysis for all passengers on international flights, rather than restricting the collection and analysis of PNR data in a more targeted manner".[54] Notwithstanding this, it is regrettable that when addressing the proportionality of the EU PNR proposal the FRA merely stated that "for proportionality reasons to include an explicit obligation in the proposal to make every reasonable effort to define assessment criteria in a manner which ensures that as few innocent people as possible are flagged by the system".[55] In light of *Digital Rights Ireland*, one may well conclude that the FRA was perhaps too cautious here.[56]

TFTP is an international agreement which permits financial messaging data transfers from the EU to the US Treasury Department. A new TFTP agreement between the EU and the US came into force on 1 August 2010 after the EP had thrown out an earlier attempt because it did not sufficiently protect EU citizens'

---

[52] For an analysis of the Commission proposal on EU PNR, see E. Brouwer (2009), "The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?", CEPS Working Document No. 320, Centre for European Policy Studies, Brussels, September, p. 339; and E. Brouwer (2011), "Ignoring Dissent and Legality: The EU's Proposal to Share the Personal Information of all Passengers", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

[53] Proposal for directive 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, 2.2.2011.

[54] Pp. 17 and 18.

[55] Ibid.

[56] It is now clear that Brouwer was right when arguing that "The failure to justify the necessity or proportionality, but also the efficiency or added value of the EU PNR system is unlikely to be solved by sunset or review clauses, allowing the legislator to adopt amendments or improvements to the instruments involved at a later stage. Nor can the intrusive effects of data systems be taken away by a general reference to applicable data protection rules, or by granting the data subject limited rights such as the right to apply for access or correction". See E. Brouwer (2009), "The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?", CEPS Working Document No. 320, Centre for European Policy Studies, Brussels, September, p. 25.

privacy.[57] Many MEPs at the time of the approval of the second attempt at a TFTP agreement were still unconvinced that there were sufficient guarantees for EU citizens' privacy. It is likely that they will come back to this aspect of the agreement if re-elected. However few political voices have been heard on the implications of the CJEU judgement on the Safe Harbor scheme, the third EU-USA framework under which companies can self-certify that they are data protection compliant in order to shift (or 'free transfer') large amounts of personal data back and forth from EU member states to companies across the Atlantic.[58] The European Commission, in an evaluation of the functioning of Safe Harbor carried in November 2013,[59] has already pointed out that there has been growing concern among EU data protection authorities about data transfers under the Safe Harbor scheme. They have argued that the data protection principles are loosely formulated and insufficiently enforced and that the Safe Harbor scheme relies too much on self-regulation. The Commission also raised concerns about the possibility of personal data transferred under Safe Harbor being accessed and further processed by US authorities "beyond what is strictly necessary and proportionate to the protection of national security".[60] These are the core issues in EU-US relations to which the EDPS was referring in his press release of 8 April, and which are now very much at stake after the CJEU intervention. However, there is also the sensitive matter of the USA (PRISM) mass surveillance programmes run by the NSA, which affect everyone in the EU and remain outstanding.

The profound implications of *Digital Rights Ireland* over EU legal instruments and policy tools engaged in mass data collection have been confirmed by the above-mentioned confidential opinion issued by the Council Legal Service of 5 May 2014 on the judgement invalidating the Directive. According to the opinion, existing EU measures and proposals which provide for "mass data collection, storage of the data of a very large number of unsuspected persons, and access to and use of such data by law enforcement authorities do not stand a serious chance of passing the legality test" unless they go hand-in-hand with a high level of data protection and "adequate safeguards... to ensure that any serious restriction of fundamental rights is circumscribed to what is strictly necessary and is decided in the framework of guarantees forming part of Union legislation instead of being left to the legislation

[57] A. Amicelle (2011), "The great (data) bank robbery: terrorist finance tracking program and the 'Swift affair'", *Research Questions, CERI* 36, pp. 1-27; S. Carrera et al. (2013), "The 'Lisbonisation' of the European Parliament: Assessing progress, shortcomings and challenges for democratic accountability in the area of freedom, security and justice", CEPS Liberty and Security in Europe Series, No. 58, September, Centre for European Policy Studies, Brussels.

[58] Refer to Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000. See also http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm. See also http://export.gov/safeharbor/eu/eg_main_018365.asp

[59] Commission Communication, p. 5.

[60] Ibid., p. 17.

of Member States".[61] Such currently existing measures would include the Visa Information System (VIS) and EURODAC (the EU data base of asylum seekers), and initiatives like the above-mentioned proposed EU PNR Directive, or the Commission proposals for an EU Entry/Exit System for third country nationals crossing EU external borders.[62]

There are many points of difference between the EU and the US on the data programmes but the one which is particularly relevant here is the question of data retention. On 17 January 2014, the US President announced that his government would take a variety of measures to re-establish public confidence regarding privacy. Among the things he promised was an end to the bulk collection of telephony metadata records, with an assurance that the government would have access to the information it needed to meet its national security requirements. A new programme would be created whose key attributes would be: (a) that the government would not collect telephone records in bulk but that the records would remain at the telephone companies; (b) that except in the case of emergency, the government would obtain the records only pursuant to individual orders from its specialist court approving the use of specific numbers for such queries, if a judge agreed based on national security concerns; (c) that the companies would be compelled by court order to provide technical assistance to ensure that the records be queried and that results be transmitted to the government in a usable format and in a timely manner.[63] This sounds very similar to the Data Retention Directive and so would be problematic for the EU in its proposed use of the data of EU residents. The UN Human Rights Committee, in its concluding observations on the fourth period report of the USA issued on 23 April under the International Covenant on Civil and Political Rights 1966, warned the US government, in the context of its comments on the NSA surveillance programmes, that "the State party should refrain from imposing mandatory retention of data by third parties."[64] Clearly it is not only the EU who are concerned about bulk metadata retention.

[61] Refer to Council of the European Union, judgment of the Court of 8 April 2014 and invalidation of the Directive 2006/24, 9009/14, 5 May 2014, Brussels. Retrievable from statewatch.org

[62] European Commission, proposal for a regulation establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the member states of the European Union, COM(2013) 95 final, 28.2.2013.

[63] www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[64] CCPR/C/USA/CO/4, 23 April 2014.

Section 4 – What should the EU do? Policy Suggestions for Ensuring *Digital Rights Ireland* Compliance

The European institutions are now in that silent period when the EP has adjourned for the elections, a new Commission will follow, and a number of member states will have national elections. It is likely that there will be little more from them on the future of privacy and data retention until autumn 2014. There are a number of options open to the EU institutions arising out of the *Digital Rights Ireland* affair and the invalidation of the Data Retention Directive. The first, which Commissioner Malmström threatened, is that the Commission do nothing, but this is probably not viable. Assuming this, what should be done? There are a number of steps which could be taken.

First, on data retention itself, while one can understand the frustration of the Commissioner for Home Affairs with the outcome, it is not a realistic solution for the European Commission to just walk away. Instead a full and independent re-assessment of the need for a Data Retention Directive must be undertaken as soon as possible. If the Council wants a directive, then it must show that it is necessary. If not, any new proposal will fail the subsidiarity and proportionality principles applicable to every piece of EU legislation. This means that member states will need to show that access to retained data for the purposes of law enforcement actually helps to address and solve serious crimes. From the information publicly available at the moment, there seems to be little reason to require companies and service providers to retain metadata for more than three months, as it is mainly within that time period that law enforcement authorities seek access to it.[65] But even that period may not be justified unless there is evidence that it is necessary and proportionate to achieve the purported public policy objective. In order to strengthen security and law enforcement in the EU, the European Commission could propose a measure on enhanced data preservation which would be *Digital Rights Ireland* compliant. Also, there needs to be more legal certainty and a commonly accepted definition of what constitutes 'serious crime' for the purposes of data retention and processing in the EU, otherwise the real purpose of any further steps will remain unclear.[66]

---

[65] Refer to http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf

[66] This has been pointed out for instance in the above-mentioned FRA opinion on the EU PNR proposal which stated that "...proportionality is mandatory under Article 52 of the Charter and the exclusion of minor offences could be considered to be equally mandatory. The FRA suggests to limit the list of crimes covered by Article 2 of the proposal to ensure that they are sufficiently serious and to guarantee the proportionality of the EU PNR system", page 16. This was also a point raised by the EDPS on the same proposal which highlighted that "Instead of leaving the faculty of narrowing the scope of application to Member States, the EDPS considers that the Proposal should explicitly list offences which should be included in its scope and those which should be excluded as they should be considered as minor and do not meet the proportionality test". See the European Data Protection Supervisor (EDPS) opinion on the proposal for a directive of the European Parliament and of the

Second, as regards the private sector, further discussion is needed on a European 'privacy cloud' where the data of EU residents is stored so that EU data protection supervisors can be sure it will be treated in accordance with European standards and legal principles.[67] The EU needs to develop its own capacities in cloud computing, which would ensure that data processing practices were in compliance with EU law. This has been recently underlined by the European Parliament Moraes Report on the US NSA surveillance programme, the impact of surveillance bodies in various member states on EU citizens' fundamental rights, and transatlantic cooperation in Justice and Home Affairs.[68] This report called on the European Commission and EU member states to "to speed up the work of establishing a European Cloud Partnership". This suggestion has been put into doubt by recent judicial activity in the US where in a number of first instance decisions, US judges have held that companies based in the US which have ring-fenced their EU databases to fulfil EU requirements must bring personal data back to the US if requested by US authorities.[69] A number of US technology companies, including Microsoft and Google, have indicated that they will appeal these decisions. One can only hope that they are successful, or EU personal data will have to be held only by companies with no links to the USA.

Thirdly, there is no point in EU institutions pretending that all is well with the PNR and TFTP agreements, and the Safe Harbor scheme with the USA. There needs to be a careful and thorough independent evaluation of all three instruments in light of the legal standards established by the CJEU and more generally the EU data protection framework. It may be painful to have to go back to the negotiating table with the US authorities on any of them, but surely this would be better than to have the agreements fall like ninepins one after the other as they are challenged before the CJEU.

Fourthly, the EU PNR proposal needs to be revamped as well, and its value and necessity critically reconsidered. The CJEU has made it clear that privacy protections need to be intrinsic to any measure which seeks to create exceptions and interferences with the EU Charter of Fundamental Rights. Now is the time to make sure that this proposal is properly designed to be *Digital Rights Ireland* compliant. In cases where this is not possible, the initiative should be abandoned altogether. It would be certainly counter-productive to push ahead with the

---

Council on the use of passenger name record data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime, 25 March 2011, paragraph 27, p. 7.

[67] Refer to Recommendation 3 of D. Bigo et al. (2013), "Mass Surveillance of Personal Data by EU member states and its compatibility with EU Law", CEPS Liberty and Security in Europe Series, No. 62, Centre for European Policy Studies, Brussels, November.

[68] European Parliament, report 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, 2013/2188, Rapporteur: Claude Moraes, paragraph 67. The report also calls for "A European Digital Habeas Corpus – Protecting Fundamental Rights in a Digital Age", which suggests eight specific policy actions. See paragraphs 130-133.

[69] www.bbc.co.uk/news/technology-27191500

proposal, simply for the sake of getting it through, if there is a risk that it will not be able to withstand an EU privacy test.

Finally, the Council needs to stop placing obstacles in the way of the proposal for Directive COM(2012)10 which deals with data protection in the fields of police and judicial cooperation in criminal matters. This proposal has been on the table for far too long and its adoption could be central to addressing gaps of legal protection of privacy in law enforcement. Now is a good moment to take stock, ensure that the proposal fulfils the *Digital Rights Ireland* tests, and adopt it as soon as possible.

This is a substantial list of policy suggestions but it is also a necessary one. We who live in the EU are entitled to respect for our privacy. Those responsible for protecting it, and for ensuring our security, now have clear instructions from the highest EU judicial authority on the way forward.

References

Amicelle, A. (2011) "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", *Research Questions* 36, Sciences Po CERI, May.

Bigo, D. et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy", European Parliament study, DG IPOL, Brussels.

Bigo, D. et al. (2012), "Fighting cyber crime and protecting privacy in the cloud", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 462.509, Brussels.

Bigo, D. et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", CEPS Liberty and Security in Europe Series, No. 62, Centre for European Policy Studies, Brussels, November.

Bigo, D. et al. (2013), "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU", CEPS Policy Brief No. 293, Centre for European Policy Studies, Brussels, June.

Brouwer, E. (2009), "The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?", CEPS Working Document No. 320, Centre for European Policy Studies, Brussels, September.

Brouwer, E. (2011), "Ignoring Dissent and Legality: The EU's Proposal to Share the Personal Information of all Passengers", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

Carrera, S. et al. (2013), "The 'Lisbonisation' of the European Parliament: Assessing progress, shortcomings and challenges for democratic accountability in the

area of freedom, security and justice", CEPS Liberty and Security in Europe Series, No. 58, Centre for European Policy Studies, Brussels, September.

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de