Gavin Robinson

Data protection reform, passenger name record and telecommunications data retention

– Mass Surveillance Measures in the E.U. and the Need for a Comprehensive Legal Framework –

Résumé

Dans l'article, l'auteur s'interroge sur l'impact d'une reforme proposée du cadre légal européen règlementant la protection des données au niveau européen qui n'assurerait qu'une protection réduite des données à caractère personnel utilisées dans les domaines policier et judiciaire. L'article conclue sur une brève réflexion quant à la valeur sociale et politique des droits à la protection des données et à la vie privée, pour enfin aborder les potentiels effets néfastes du profilage à grande échelle et plaider ainsi pour le développement progressif d'un cadre juridique européen en matière de protection des données qui soit transparent, équilibré et complet couvrant toutes les manipulations des données par les acteurs de sécurité intérieure.

Zusammenfassung

Der Artikel untersucht den Einfluss einer Reform des Europäischen Rechtsrahmens zum Schutz persönlicher Daten, der bislang einen nur verkürzten Schutz persönlicher Daten in den Bereichen Polizei und Justiz sicherstellte. Der Artikel betont am Ende den politischen und sozialen Wert der Rechte auf Datenschutz und auf den Schutz der Privatsphäre. Der Autor fordert einen Europäischen Rechtsrahmen im Bereich des Datenschutzes der transparent und fair ist und der jegliche mögliche Manipulation persönlicher Daten durch die Akteure innerer Sicherheit abdeckt.

I. Introduction: data protection: EU legal framework

On 1st December 2009, the Lisbon Treaty entered into force looking set to breathe new life into data protection in the European Union. A new horizontal legal basis for data protection provisions in Article 16 TFEU, the elevation of data protection to the status of fundamental right enshrined in Article 8 of the Charter and a stronger role for the European Parliament in the post-pillar Union were welcomed as vital tools.[1] Enthusiasm

1 See for example the contribution of Peter Hustinx, European Data Protection Supervisor, 'Data Protection for Law Enforcement after Lisbon', ERA Conference: *Data Protection in the Age of SWIFT, PNR, Prüm and E-Justice*, 31 May 2010. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-05-31_Speech_ERA_EN.pdf.

for data protection and privacy are also evident in the European Council's Stockholm Programme, which commits to ensuring the respect of core data protection principles,[2] both by evaluating the functioning of existing instruments[3] and by building "a comprehensive protection scheme."[4] Anchored in a new Information Management Strategy for EU internal security,[5] the new EU approach to personal data promises to be mindful both of law enforcement "business needs" and data protection.

Article 8 of the ECHR provides that "everyone has the right to respect for his private and family life, his home and his correspondence". Data protection has been developed by the ECtHR as an aspect of privacy protection in its considerable jurisprudence on Article 8. For example in *M.S. v. Sweden*, the Strasbourg court stated that "the protection of personal data […] is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention".[6]

Another Article 8, that of the EU Charter of Fundamental Rights, establishes data protection as a fundamental right, providing that personal data may however "be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". [7]

Yet European legislation on data protection in the Area of Freedom, Security and Justice is fragmented, presenting a complex patchwork of regulation. Police and judicial cooperation in criminal matters are excluded from the scope of the 1995 Data Protection Directive.[8] A Framework Decision, adopted in 2008, does not apply to domestic processing of data for law enforcement and security matters and features wide exemptions to the main principles of data protection consolidated in the 1995 Directive.[9] Additio-

2 "[B]asic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured[…]": Section 2.5, Stockholm Programme.

3 Section 2.5, Stockholm Programme.

4 Ibid.

5 See Chapter 4, Stockholm Programme.

6 M.S. v. Sweden, judgment of 27 August 1997, para 41.

7 Article 8. Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

8 See Article 3(2), first indent, of 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**,** *Official Journal L 281, 23/11/1995 P. 0031 – 0050.*

9 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal L 350, 30/12/2008 P. 0060 – 0071.*

nally, sector- or agency-specific rules exist in relation to the Schengen Information System (SIS), Europol, Eurojust and the Prüm Decision.[10]

The Lisbon Treaty extended the ordinary legislative procedure to Justice and Home Affairs, laid down a new single legal basis for data protection rules at EU level[11] and endowed the Charter of Fundamental Rights with the same legal value as the Treaties, thereby formally elevating data protection to fundamental right status.[12] The Stockholm Programme and the Commission's Internal Security Strategy reiterated the political will to protect fundamental rights as a vital premise of the AFSJ, marking a departure from a former tendency to treat fundamental rights as brakes on efficiency, requiring to be balanced against security. Taken together, these developments would seem to provide fertile ground for insisting on the rigorous (re-)evaluation of the necessity and proportionality of both existing and envisaged measures touching on the use of personal data in law enforcement.

II. A comprehensive new data protection package?

A package for reforming the EU rules on data protection was adopted by the Commission on 25 January 2012. The package contains a proposal for a Regulation[13] containing general rules on data protection and a proposal for a standalone Directive on data pro-

10 These rules generally refer to national legislation or to international legal instruments such as the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

11 Article 16 TFEU (ex Article 286 TEC)
1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

12 See Article 8. Protection of personal data:
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

13 European Commission, 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), Brussels, 25.1.2012, COM(2012) 11 final.

tection in the law enforcement sector,[14] preserving in a sense the old First/Third Pillar division in post-Lisbon European data protection law.

1. The decision to opt for a package

The European Data Protection Supervisor, in his 7th March 2012 Opinion on the package, welcomed the Regulation as a "huge step forward" but expressed "serious disappointment" that the legal framework at EU level looks set to remain fragmented despite the availability of a single legal basis in Article 16 TFEU.[15]

At a conference in November 2012, the Director of the Internal Security unit at the European Commission DG Home Affairs, Reinhard Priebe, insisted that a single-measure outcome had proved unattainable in practice, and that the dual-instrument package proposed represented the best that the Commission was able to secure. First, according to Priebe, the rather general terms of Article 16 TFEU limit what can be done with the provision. The substance of Article 16 TFEU, calling for the introduction of "rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law", undoubtedly contrasts with the greater depth, detail and programmatic nature of the core Treaty provisions on judicial cooperation in criminal matters (Articles 82 and 83 TFEU), calibrating the mutual recognition principle and the approximation of criminal laws and regulations. Moreover, Declaration 21 annexed to the Lisbon Treaty envisages the creation of specific rules on data protection and the free movement of such data in the fields of police and judicial cooperation in criminal matters should separate regulation prove necessary due to the specific nature of these fields.[16] Priebe stressed that the goal of the proposed Directive is not to harmonise data protection in the law enforcement sector, and that the terseness of the legislative building blocks reflected the Member States' divergences on the matter. Across the Member States, there exist a number of different data protection cultures, and the same or perhaps an even greater number of different law enforcement cultures (going down to basic structural differences such as which body is a police body, and which is a judicial body). Priebe emphasised that, at the negotiating table, a number of Member States start from the position that data gathering, processing and exchange

14 European Commission, 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, Brussels, 25.1.2012, COM(2012) 10 final.

15 European Data Protection Supervisor, Opinion on the data protection reform package, Brussels, 7 March 2012, para 11.

16 Declaration 21, *Declarations Annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon:* "The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.".

in the law enforcement sector should not be subject to any legal constraints, let alone to rules enshrined in a directly-applicable Union-wide Regulation.[17]

Important stakeholders at Member State level have divergent views on the matter. The Association of Chief Police Officers ("ACPO", United Kingdom) told the House of Commons Justice Committee in November 2012 that it was "rather surprised that the [2008 Framework Decision on data protection in the former Third Pillar] is going to be changed so soon after implementation", considering that the processes in place following the Third Pillar measure work "relatively well".[18] In contrast, Intellect, the UK trade association for the IT, telecoms and electronics industries, stated its preference for a single piece of regulation to facilitate implementation at a business level, and also voiced fears that the differing levels of data protection provided by the Regulation and the Directive[19] could lead to a staggered implementation of separate aspects of the Regulation in separate pieces of legislation, creating confusion for market actors.[20] The Justice Committee itself was clear that there should be "consistency between the two instruments from the outset".[21]

Would this entail a scaling up of protection levels found in the proposed Directive, or a scaling down of those found in the proposed Regulation? In oral evidence given to the UK House of Commons Justice Committee in September 2012, Françoise Le Bail (Director General, DG Justice at the European Commission) argued that the same principles were reflected by both instruments, and that the package applied both Article 16 of the TFEU and Declaration 21 to the Lisbon Treaty, "which says that for this particular field, which is police and judicial co-operation in criminal matters, of course specific provision should be taken".[22]

2. Scope and level of protection

a) Level of protection

Whilst the new draft Directive does, unlike the 2008 Framework Decision, apply to domestic processing of data, it will essentially provide for a lower standard of protection for data used for law enforcement purposes. The EDPS, in his 7th March 2012 Opinion on the package took the view that "compared to the proposed Regulation, many provisions in the proposed Directive are weak, without any evident justification,"[23] and recommended changes *inter alia* to tighten up derogations to the purpose limitation prin-

17 Presentation at ERA Conference, 'Data Protection in the Area of European Criminal Justice Today', 5th November 2012, Trier, Germany.

18 See House of Commons Justice Committee – Third Report – *The Committee's opinion on the European Union Data Protection framework proposals*, 1st November 2012, available at http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/57202.htm, para 109.

19 See *infra* "Scope and level of protection".

20 See Justice Committee Report on the EU Data Protection framework proposals, para 12.

21 Ibid, para 13.

22 Justice Committee Report on the EU Data Protection framework proposals, Oral Evidence, response to Question 71.

23 EDPS Opinion, para 19.

ciple, to include non-suspected persons as a separate data category, to strengthen data subject rights to notification and rectification of personal data, as well as to bolster the powers of supervisory authorities, limited by the terms of the proposed Directive.[24] Interestingly, the UK's Justice Committee, reporting to the European Scrutiny Committee, recently accepted that the Directive "does not sufficiently protect personal data",[25] yet also cited subsidiarity concerns in order to argue in favour of an exemption for domestic processing from even these – admittedly sub-standard – provisions.[26]

b) Scope: activities covered

Representatives from the UK Ministry of Justice, in evidence to the Justice Committee, recently reaffirmed the UK government's intention to attempt to remove domestic processing from the face of the Directive.[27] The Justice Committee's report agreed, considering that the "huge costs and burdens" connected to such a scheme would be unwarranted in the absence of any evidence that a lack of EU-level rules is obstructing inter-Member State cooperation or harming data protection,[28] and that a "carve-out for policing and security" is necessary in order to meet the specific needs of law enforcement authorities.[29] If the United Kingdom succeeds on this count at the negotiating table, what has often been criticised as a key flaw in the 2008 Framework Decision may well remain in the new generation of EU data protection legislation: a common framework of standards would only be applicable to data transferred between Member States, with variable levels of national data protection applicable to domestic processing despite the unavoidable twists and vagaries of investigations making it difficult in practice to operate a strict division between "domestic data" and data which may at some point require transfer to another Member State.

An innovative aspect of the draft Directive concerns its approach to the automated processing of personal data, including for the creation of personal profiles. Chapter II of the proposal ('Principles') lays down, alongside a general ban on the processing of

24 See EDPS Opinion, 'Recommendations', pp.73-75.

25 Justice Committee report, para 151: "As currently drafted, the Directive does not sufficiently protect personal data. In particular, the level of data protection is not to the same standard as that contained in the draft Regulation which covers data protection matters.".

26 Ibid, para 151: "We are concerned that it should be clear that domestic processing of data within the UK by law enforcement agencies will not be covered or restricted by the Directive, and it should also be clear that Member States have the flexibility to implement the Directive in ways which achieve its purposes through processes which are appropriate and proportionate in their national context.".

27 See Justice Committee Report, Oral Evidence of Rt Hon Lord McNally, Minister of State at the Ministry of Justice, answer to Question 104: "We believe – and we believe we have allies among other countries in the negotiations – that that is precisely the best outcome for the Directive as a whole. It is almost a belt-and-braces approach. We are securing our own position but we want to argue the case for keeping these matters to domestic control across the Community or the Union".

28 See Justice Committee Report, paras 138-139.

29 See Justice Committee Report, Oral Evidence of Rt Hon Lord McNally, answer to Question 106.

so-called "sensitive" personal data[30] in article 8(1), quite novel provisions in article 9 ('Measures based on profiling and automated processing'). Article 9(1) reads: "Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests". Article 9(2), meanwhile, provides that " [a]utomated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8". The Meijers Standing Committee of experts on international immigration, refugee and criminal law did recently take issue with the draft Directive's wording, insisting that the risk of discrimination would only be effectively reduced by adapting the provisions in order to forbid automated processing based "*solely or decisively* on the special categories of personal data referred to in Article 8,"[31] but the overall balanced tone must be welcomed.

c) Horizontal scope

Moving on from the substance of the draft Directive's data protection provisions, more broadly the EDPS bemoaned the envisaged package's lack of "horizontal" comprehensiveness, leaving as it does unaffected the data protection rules for EU institutions and bodies, but also all specific instruments adopted in the area of police and judicial cooperation in criminal matters such as the Prüm Decision and the rules applying to Europol, Eurojust and the Schengen Information System.[32] More specifically, the EDPS saw the choice for a self-standing instrument as "a missed opportunity to clarify and ensure the consistent application of rules applicable to situations in which activities of the private sector and of the law enforcement sector interact with each other and borderlines are becoming increasingly blurred".[33]

The transfer of PNR data, telecommunications and financial data to law enforcement bodies provide prime examples of such interplay. As a British data protection consultancy points out, lower standards in law enforcement matters create an "inverse data protection effect": the more controversial the processing (eg. for law enforcement), the weaker the protection; the less controversial the processing (eg. processing for a seat booking), the stronger the level of protection.[34] Yet even the tentative first few steps

30 Defined as data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health of sex life; see article 8(1).

31 Letter from Meijers Committee to the European Parliament, *Note on the proposal for a General Data Protection Regulation and the protection of personal data in the area of judicial co-operation in criminal matters and police co-operation*, 23rd November 2012, available at http://statewatch.org/news/2012/nov/eu-meijers-committee-dp.pdf.

32 EDPS Opinion, para 443.

33 EDPS Opinion, para 443.

34 See Pounder, C. N. M. (2011), 'A data protection critique of the proposed Passenger Name Record Directive (COM(2011) 32 text)', Amberhawk Training Ltd.

towards regulating profiling at the EU level taken by the draft Directive[35] would, as the text stands, not apply to a future EU-PNR system were the latter system to be finalised before the new data protection framework.[36] As we shall see, the proposed EU-PNR Directive is itself completely silent on the matter of data mining and profiling. Once more, the comprehensiveness of the new EU data protection framework appears open to question.

III. Passenger name record: Jumping the data protection gun?

PNR is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by air carriers, including name, dates of travel and travel itinerary, ticket information, address and phone numbers, means of payment used, credit card number, travel agent, seat number and baggage information. PNR data are supposed to constitute an effective tool in order to "identify and track criminal and terrorist activity",[37] warranting its systematic transmission by air carriers to law enforcement bodies. PNR is not to be confused with Advanced Passenger Information (API) limited to biographical information from the machine-readable part of a passport, for which a scheme, providing not for systematic access by law enforcement but for access by request, is already live in relation to flights inside the Union.[38]

Negotiations with the USA on a fourth EU-US PNR agreement continued throughout 2011. The latest agreement, intended to have a higher degree of permanency than previous deals, was concluded in early December 2011. In a plenary vote on the 19th April 2012, the European Parliament adopted the latest EU-US PNR agreement with 409 votes in favour, 226 against and 33 abstentions, reflecting the contentious nature of the issue. The Opinion of the European Data Protection Supervisor, published on 13 December 2011, welcomed safeguards on data security and oversight.[39] However, the Union overseer repeated doubts as to the necessity and proportionality of the scheme. Indeed, if one takes the successive EU-US PNR agreements from 2004, 2007 and 2011, one can observe a "slackening" evolution in terms of purpose limitation, retention period (from 4 years to 15 years including "anonymised" time), the transmission of sensitive information (medical and religious data), push/pull systems, onward transfer, and judicial

35 See above discussion of articles 8 and 9, draft Directive on data protection in the law enforcement sector.

36 See Article 59, Proposal for a Directive: "The specific provisions for the protection of personal data 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 in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive *remain unaffected*." [Emphasis added].

37 Explanatory Statement to Timothy Kirkhope Draft Report on EU-PNR, p.30.

38 Directive 2004/82/EC of 29 August 2004 on the obligation of air carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

39 Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-12-09_US_PNR_EN.pdf.

redress.[40] The EDPS also voiced serious reservations as to the real enforceability of US concessions such as the right to redress.[41] A central problem in the international context is that intended 'guarantees' negotiated for EU citizens (eg. ban on processing of sensitive data, right to redress), as hard-won as they may have been, may be practically unenforceable in third states, particularly the United States. This state of affairs leads some observers to consider that in order to prevent established levels of protection from being "hollowed out by global security networks", in the long-term a transnational data protection authority may be necessary.[42] However, this idea will not be developed further in this contribution, which will focus rather on the ongoing project of creating an internal EU-PNR surveillance system.

A Commission proposal for a Directive establishing an internal EU-PNR scheme was made in February 2011.[43] Subsequently, the United Kingdom gained support from 15 other Member States to extend the scope of the instrument to include the option of covering selected flights inside the European Union. The EU scheme, for a time, was passing through the European Parliament in parallel with the EU-US scheme until the latter was finally adopted in April 2012. The Parliament's Rapporteur on the internal measure (Timothy Kirkhope MEP) showed greater support for the necessity of travel surveillance generally than the Rapporteur on the transatlantic set-up (Sophie In'T Veld MEP), and in his draft report of 14th February 2012 advocated no major changes to the Commission's proposal, voicing support for an extension to intra-EU flights and the use of PNR data in the context of terrorism and "serious crime".[44] On the 23rd April 2012, the Presidency presented a compromise text, providing for the optional coverage of intra-EU flights, to the Council with a view to opening negotiations with the European Parliament.[45]

40 See Hornung, G. and Boehm, F. (2012), 'Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security', Study for the Greens / European Free Alliance in the European Parliament. Available at http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/PNR_Study_final.pdf.

41 Op cit. n.39, paras 23-24.

42 Nickel, R. (2010), 'Data Mining and "Renegade" Aircrafts: The States as Agents of a Global Militant Security Governance Network – The German Example', *Emory International Law Review,* 24: p.650.

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

44 European Parliament, Draft Report on the proposal of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Timothy Kirkhope, 14th February 2012, see Explanatory Statement pp.30-32.

45 Council of the European Union, Note from Presidency to Council, 'Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', Interinstitutional File: 2011/0023 (COD) (Brussels, 23 April 2012).

Highly critical opinions from the European Data Protection Supervisor,[46] the Article 29 Working Party[47] and the Fundamental Rights Agency[48] followed publication of the draft EU-PNR Directive. Citing violations of the rights to protection of personal data,[49] respect for private and family life[50] and to be free from discrimination,[51] each opinion concluded that the necessity and proportionality of the scheme have not been sufficiently established.

Article 52(1) of the EU Charter provides that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be *provided for by law* and respect the essence of those rights and freedoms. Subject to the principle of *proportionality*, limitations may be made only if they are *necessary* and *genuinely meet objectives of general interest recognised by the Union* or *the need to protect the rights and freedoms of others*."[52]

Article 52(1): 'Objectives of general interest/to protect rights and freedoms of others'

National security and/or the prevention of crime have been accepted as a "legitimate aim" (the ECHR wording) by the European Court of Human Rights in Convention Article 8 case law,[53] and the Fundamental Rights Agency seems to be in no doubt that EU-PNR clears this hurdle. It may be useful, however, to reflect on whether the workings of the PNR set-up fit the scenario of crime prevention. Now, PNR is raw data fed into security practices related to profiling and data mining, marked by a trend towards prevention that in some cases "appears to slide towards anticipation", playing less a pre-emptive role than a preparatory one, collecting, processing and sharing data "just in case" a crime is committed.[54] It is possible to argue that, on a strict reading of "objectives of general interest", interferences with fundamental rights such as those made inevitable by EU-PNR require clear demonstrable links to crime prevention in order to be considered Charter-compliant.

46 European Data Protection Supervisor ('EDPS'), *Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime* (Brussels, 25 March 2011), available at www.edps.europa.eu.

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

48 European Union Agency for Fundamental Rights ('FRA'), *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 (COM(2011) 32 final)*, FRA Opinion – 1/2011, 14 June 2011.

49 Article 8, CFREU.

50 Article 7, CFREU.

51 Article 21, CFREU.

52 Emphasis added.

53 Notably in ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

54 *IN:EX – Converging and conflicting ethical values in the internal/external security continuum in Europe*, European Commission, 7th Framework Programme (FP7), *D.2.5. Recommendation Report: Situating Privacy and Data Protection in a Moving European Security Continuum*, March 2011, pp.7-8. Available at www.inexproject.eu.

Article 52(1): 'Provided for by law' (ECHR wording: 'in accordance with the law')

In its reading of the EU-PNR Proposal, the FRA points up concerns over the "quality" of the law, meaning essentially its accessibility and foreseeability. Firstly, the Annex to the Proposal provides air carriers with a "general remarks" category of information, potentially opening the door to unlimited information gathering.[55] The Proposal also purports to limit the use of PNR data to fighting "serious crime",[56] yet the definition of "serious crime" in article 2(h) of the Proposal is not watertight. Indeed, that sub-article refers to the offences listed in article 2(2) of the Framework Decision on the European Arrest Warrant – a provision which incidentally does not itself feature the term "serious crime". Article 2(h) of the Proposal further allows Member States to exclude from the scope of the scheme "those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality", thereby impliedly acknowledging that the term "serious crime" encompasses *minor* offences. This creative manner of legislating may remind the reader of the much-maligned purpose (un)limitation provisions in the 2008 Framework Decision on 3rd pillar data protection,[57] and sits uneasily with the Commission's claim that an EU-PNR system would increase legal certainty for passengers.[58] For this to be so, as the FRA points out, surely the margin of discretion on such a central factor of the proposal should not be left to the Member States.[59]

Finally, article 4(2)(b) permits Passenger Information Units to compare PNR data against "relevant databases, including international or national databases or national mirrors of Union databases, where they are established on the basis of Union law, on persons or objects sought or under alert".[60] Both the EDPS and the Article 29 Working Party criticised the low level of foreseeability afforded by this provision.[61]

---

55 FRA Report, p.13.

56 EU-PNR Proposal, Article 1(2).

57 2008 Framework Decision, Article 3 (emphasis added)
1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. […]
2. *Further processing for another purpose shall be permitted in so far as:*
(a) it is not incompatible with the purposes for which the data were collected;
(b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and
(c) processing is necessary and proportionate to that other purpose.
See also Article 11 (emphasis added)
Processing of personal data received from or made available by another Member State Personal data received from or made available by the competent authority of another Member State may, in accordance with the requirements of Article 3(2), be further processed only for the following purposes other than those for which they were transmitted or made available:
[…]
(d) *any other purpose* only with the prior consent of the transmitting Member State *or* with the consent of the data subject, given in accordance with national law.

58 COM(2011) 32 final, p.4.

59 FRA Report, p.14.

60 EU-PNR Proposal, article 4(2)(b).

61 EDPS Opinion on EU-PNR Proposal, p.5; Article 29 Working Party Opinion, p.5.

Article 52(1): 'Necessity and proportionality'

The Strasbourg Court established in the *Handyside* case[62] that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[63] A "pressing social need" was the term preferred by the Court in the *Olsson* case.[64] Proportionality, meanwhile, "puts the reason for the limitation and the scope of the limitation into relation with each other."[65]

In the Explanatory Memorandum attached to the EU-PNR Proposal, the Commission forwards evidence of the necessity of PNR in combating serious transnational crime, particularly drugs and human trafficking.[66] Also in the Commission's 2010 Communication on information management in the AFSJ, numerous examples demonstrated the necessity of PNR to the investigation of child trafficking, trafficking in human beings, credit card fraud and drug trafficking, but the source of this evidence was not disclosed.[67] In relation to PNR agreements with the USA, the UK House of Lords European Union Select Committee, initially unsure,[68] subsequently received confidential evidence from the Home Office which convinced the Lords that PNR data, when used in conjunction with data from other sources, could significantly assist in the identification of terrorists.[69] In 2011, the Committee gave its blessing to the UK's opt-in to the latest agreement.[70] Thus, it remains the case that there has been no evidence made publicly available of the necessity of PNR in the fight against terrorism or the other "serious crimes" covered in art 2(h) of the Proposal.[71]

In other words, the Commission has only ever provided examples demonstrating the necessity of PNR data in the context of combating "serious transnational crime" whereas the proposed Directive refers in numerous contexts to "serious crime"[72] – defined as the offences listed by Article 2(2) of the Council Framework Decision 2002/584/JHA on the European Arrest Warrant.[73]

62 ECtHR, *Handyside v. UK,* No. 5493/72, 7 December 1976.
63 Ibid, paragraph 48.
64 ECtHR, *Olsson v. Sweden*, No. 10465/83, 24 March 1988.
65 FRA Report, p.14.
66 European Commission, *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February 2011, pp. 5-6.
67 European Commission (2010), *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, Brussels, 2010.
68 The EU/US Passenger Name Record (PNR) Agreement, 21st Report, Session 2006-07, HL Paper 108, paragraph 22.
69 The Passenger Name Record (PNR) Framework Decision, 15th Report, Session 2007-08, HL Paper 106, paragraph 49.
70 The United Kingdom's opt-in to the Passenger Name Record Directive, 11th Report, Session 2010-2011, HL Paper 113, paragraph 6.
71 FRA REPORT, pp.15-16.
72 See EU-PNR Proposal, articles 1(2)(a), 4(2)(b), and 4(2)(c).
73 EU-PNR Proposal, article 2(h).

The necessity and proportionality of systems such as EU-PNR are particularly sensitive not only because systematic surveillance seems contrary to the essence of Treaty aspirations to a single Area of Freedom, Security and Justice without internal border controls,[74] but especially since data collection and analysis are foreseen for all air passengers, instead of being applied in a more targeted manner.[75] From a technical point of view, one might maintain that blanket data collection simply comes with the territory of proactive risk profiling, a technique involving tests performed on the basis of "constantly evolving and non-transparent criteria".[76] Nonetheless, in accepting this reality the Fundamental Rights Agency argues for the addition to the proposal of an "explicit obligation […] 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".[77]

The need for specific safeguards in the EU-PNR instrument itself becomes clearer when one recalls that the future Directive on data protection in the law enforcement sector, as currently drafted, will not apply to previous acts.[78] The tentative provisions therein regulating profiling[79] will therefore not apply to what is set to be one of the most significant developments yet in the profiling of European citizens, should the EU-PNR Directive enter into force before the new data protection instrument. Negotiations are ongoing at the time of writing, yet the relative urgency of the EU-PNR does seem doubtful considering that a number of the Member States in favour of an internal EU-PNR scheme have already begun using their own PNR systems, tempering somewhat the immediate need for rolling out the European set-up. Speaking at a November 2012 conference, Emilio de Capitani (former head of Civil Liberties, Justice and Home Affairs Secretariat at the European Parliament) also questioned the need to move quickly on this issue given that this time, and in contrast to the negotiations which led to the EU-US agreements, there is no external diplomatic pressure on the Union.[80]

That being said, proportionality testing of the future EU-PNR system may in the medium to long-term find other outlets than the legislative process. The reactions of a series of national Constitutional Courts to the Data Retention Directive could be interpreted as preparing the ground for future judicial control of the proportionality of initiatives such as the EU-PNR system. Indeed, as the Fundamental Rights Agency underlines, the same reasoning – the condemnation of data retention as unconstitutional *inter alia* since the scheme affects all citizens who are in principle to be considered as innocent – could also be applied to the proposed EU PNR system.[81] Accordingly, it is to the current state of play regarding the Data Retention Directive that we now turn.

74 Article 67(2), TFEU.
75 For discussion, see FRA Report, pp.17-18.
76 EDPS, Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 25 March 2011, pp. 4-5.
77 FRA Report on EU-PNR Proposal, p.18.
78 Article 59, Proposal for a Directive.
79 See above discussion of proposal for a Directive on data protection in the law enforcement sector, p.5.
80 Presentation at ERA Conference, 'Data Protection in the Area of European Criminal Justice Today', 5th November 2012, Trier, Germany.
81 FRA Report on EU-PNR Proposal, p.17.

IV. Data retention: Judicial control post-Lisbon

The European Parliament and the Court of Justice look set to have pivotal roles to play in the relationship between personal data and law enforcement over the next few years, not only concerning new measures such as the EU-PNR scheme, but also in respect of the evaluation and judicial control of existing measures – most notably, from a data protection point of view, the fabled Data Retention Directive.[82] Briefly revisiting the background to the agreement of such a measure in the pre-Lisbon EU set-up may prove instructive in this regard.

1. Directive 2006/24: origins

Four years prior to the introduction of the Directive, in 2002 the e-privacy Directive had applied data protection principles found in the 1995 Data Protection Directive to the telecommunications sector, mandating the erasure of traffic data once no longer needed in order to transmit a communication.[83] Although at that time the JHA Council expressed a desire to carve an "appropriate and proportionate" exception to the e-privacy Directive's erasure provisions, ensuring the retention of electronic communications data for "a limited time" for law enforcement purposes,[84] high-level calls for legislative action did not resurface until after the Madrid bombings on 11th March 2004. Within a fortnight, the European Council presented a slew of proposed measures intended to combat terrorism including the transfer of Passenger Name Record data, the introduction of bio-

82 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal *L 105, 13/4/2006 P. 0054 – 0063.*

83 Article 6(1) of the e-privacy Directive: 'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication […].'.

84 See paragraph 7, Conclusions on Information technologies and the investigation and prosecution of organised crime, Justice and Home Affairs Council Meeting, Brussels, 19 December 2002, doc 15691/02 (Presse 404): [The Council of the European Union] AGREES that the adoption of rules on the approximation of Member States' legislation on the obligation of electronic communication services providers to retain specific traffic data concerning electronic communications for a limited time should take into account the dialogue between interested parties. If it is found necessary to establish such rules, they should at any rate ensure that such traffic data is available insofar as it is necessary according to the standards of a democratic society and existing provisions of a constitutional nature of each Member State, appropriate and proportionate for the prevention, detection, investigation and prosecution of criminal offences.".

metric IDs and the retention of telecommunications data.[85] Just over a month later, a group of four Member States tabled a joint proposal for a third pillar Framework Decision taking up this last policy recommendation,[86] but the requirement of unanimity hindered negotiations. The London bombings on 7th July 2005 spurred the JHA Council, presided over by the then-UK Home Secretary Charles Clarke, to state that a Framework Decision would be agreed by October that same year.[87]

On a domestic level, the law enforcement community in the UK had been pushing for more extensive data retention for some years. The Anti-Terrorism, Crime and Security Act, which entered into force less than two months after the September 11th attacks, had indeed already lain down a legislative basis for an extensive data retention scheme, but on a voluntary basis (in the form of a 'Code of Practice').[88] However, besides the 7/7 attacks, by the time the UK Presidency of the EU came around in the second half of 2005, technical developments and political opportunity also seem to have contributed to making the Directive the most hastily-passed piece of legislation in the history of the EU.

Internet Service Providers (ISPs) resisted most strongly the pressure to divulge customer data. As previously mentioned, provisions in the 2002 e-privacy Directive forced Communications Service Providers ('CSPs') to delete user data as soon as such data was no longer required for commercial purposes. For telephone service providers, call data remained essential to accurate billing, however due to the rapid proliferation of "always-on" broadband services available at a flat monthly rate, the same no longer held for ISPs. Unwilling to pay for any such scheme, and concerned that widespread retention might expose market actors to subsequent legal action for breaches of UK data protection law, many ISPs intimated to the UK government their preparedness to relocate abroad.[89] Faced not only with possible damage to the British economy but with the prospect of further reduced data flows to the law enforcement community, the UK government privileged the EU law route. Efforts were perhaps further focused on speedy progress due to the fact that the rotating EU presidency was set to pass from the UK at the turn

85 European Council, Declaration on Combating Terrorism, Brussels, 24 March 2004, available at http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf, p 4: "The European Council, with a view to the further development of the legislative framework set out above, instructs the Council to examine measures in the following areas:
- proposals for establishing rules on the retention of communications traffic data by service providers; […]".

86 The Member States were France, the United Kingdom, Ireland and Sweden. See Council of the European Union, Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism, Council doc. 8958/04, Brussels, 28 April 2004.

87 Extraordinary Justice and Home Affairs Council meeting of 13 July 2005, Council Declaration on the EU Response to the London Bombings (Council doc 11116/05, Presse 187), para 4.

88 For a detailed discussion of the UK law before the Directive, see Milford, P. (2008), 'The Data Retention Directive: too fast, too furious a response?', Southampton Business School. Available at http://www.petermilford.com/downloads/Data_Retention_PMilford.pdf, pp. 19-35.

89 Ibid, p.35.

of the year to Austria, known opponents of the proposed data retention scheme. The initial proposal for a third pillar Framework Decision was re-worked as a first pillar Directive and presented by the Commission on the 21st September 2005.[90] This meant qualified majority voting instead of unanimity, but also engaged the European Parliament's co-decision powers.

After the UK Presidency had failed to reach an agreement with the LIBE Committee at the European Parliament, the British delegation directly approached the leaders of the two largest Parliamentary Groupings, the PSE and the PPE. Those leaders, both German MEPs, agreed privately to support the Council's position on the Directive in an apparent "demonstration of power" by members of the new "grand coalition" between Germany's two largest domestic political parties.[91] Victory for the UK Presidency in the face of opposition from industry, civil rights organisations and fellow Member States was assured when the Parliament voted through the Council's compromise text on 14th December 2005, performing a considerable climb-down from its repeated stance that any form of mass surveillance is unjustified.[92]

2. Directive 2006/24: a difficult transposition

The Data Retention Directive finally came into force on 3rd May 2006, mandating the collection of traffic and location data, as well as data necessary to identify subscribers, on the part of the providers of publicly available electronic communications networks or of public communications networks in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime.[93] Article 6 of the Directive provides for a minimum retention period of six months, and a maximum period of two years from the date of the communication, giving some leeway to Member States in this respect.

Indeed, the Directive offers less scope for detailed critical analysis than the other measures mentioned since, as its title indicates, it mandates the retention of telecommunications data and does not regulate the access, processing or transfer of those data by law enforcement at Member State level. This regulatory division invariably makes it difficult to assess the justifiability of the data retention obligation alone – conditions of access and use are simply crucial to any such appraisal.[94] In leaving such matters to the national level, one commentator argues that "the Directive has placed a bomb in the privacy of European citizens and has allowed the Member States alone to take measures to prevent it from exploding."[95]

90 COM (2005) 438 final, 21 September 2005.

91 Rauhofer, J. (2006), 'Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union', *SCRIPT-ed* 3:4: 322-343, at 338.

92 See, for example European Parliament resolution on the First Report on the implementation of the Data Protection Directive (95/46/EG), dated 09/03/2004, document reference P5-0104/2004.

93 Ibid, article 1(1).

94 Markou, C. (2012), 'The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb', *Computer Law & Security Review* 28: 468-475 at 471.

95 Ibid, p.475.

Whilst the relative social value of privacy is eminently debateable, it is surely worth reflecting on the real impact of EU legislation "harmonising the exception" to e-privacy and possible implications for the citizen-State relationship. In a number of Member States, constitutional arrangements have been directly affected. Cyprus, for instance, revised its constitution in order to accommodate data retention, extending to all citizens permitted derogations to the right to privacy that had previously applied only to prisoners.[96]

Moreover, certain national provisions have tended to mirror the separation of communications data retention and the use and processing of those data in domestic legislation. In the United Kingdom, for example, whilst the retention of data is regulated by secondary legislation,[97] access is regulated by the Regulation of Investigatory Powers Act 2000 ('RIPA'), the convoluted drafting of which has resulted in access to communications data for more than 800 public bodies, including all councils.[98] The British media has for a number of years been awash with reports of councils using RIPA in order to monitor citizens for comparatively trivial matters such as ensuring parents reside in school catchment areas or to detect littering, with the expression "dustbin Stasi" even making it as far as Parliament.[99]

At Member State level, implementing laws have been successfully challenged as unconstitutional in Germany,[100] Cyprus,[101] Bulgaria[102] and the Czech Republic.[103] In Austria and Sweden, resistance from civil society ensured that transposition took over six years.[104] Most recently, in October 2012 a group of Slovak MPs filed a complaint against the Slovakian transposition at that country's Constitutional Court. Prepared by

96 Ibid, p.472.

97 The Data Retention (EC Directive) Regulations SI 2007/2199.

98 See Cattanaci, J.A. and Mifsud Bonnici, J.P. (2010), 'The end of the purpose-specification principle in data protection?', *International Review of Law, Computers & Technology* 24(1): 101-117.

99 http://www.parliament.uk/business/publications/research/key-issues-for-the-new-parliament/security-and-liberty/surveillance-society/.

100 Judgment of the German Constitutional Court ("*Bundesverfassungsgericht"*) of 2nd March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, English press release at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (27th May 2010 17:17).

101 Judgment of the Cyprus Supreme Court, *Civil Applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010*, 1st February 2011; see further Markou, C. (2012), 'The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb', *Computer Law & Security Review* 28: 468-475.

102 Decision of the Bulgarian Supreme Administrative Court, 11 December 2008, reported on 17 December 2008 by EDRi at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention (accessed 24 October 2012).

103 Judgment of the Czech Republic Constitutional Court, 31 March 2011, unofficial English translation available at: http://www.edri.org/files/DataRetention_Judgment_ConstitutionalCourt_CzechRepublic.pdf (accessed 24 October 2012).

104 See Press Release from the European Commission, 31st May 2012: "Today, the Commission also formally decided to end the proceedings against Austria, which has notified all the measures fully transposing the Directive, and to make a partial withdrawal of the case against Sweden. 2 While Sweden has now fully transposed the Directive, the Court is still expected to rule on the case following last year's second referral, when the Commission requested both a lump sum and a penalty payment (IP/11/409).".

the European Information Society Institute ('EISi', which is based in Slovakia), the complaint argues that national laws both implementing the provisions of the Directive and arranging for access by police[105] are incompatible with constitutional provisions on proportionality as well as the rights to privacy, data protection and freedom of expression as enshrined in Slovakian human rights law, the ECHR and the CFREU.[106]

Amongst the decisions of national jurisdictions, that of the Romanian Constitutional Court features perhaps the most virulent rejection in principle of data retention.[107] The Court judged not only the Romanian implementing law unconstitutional due to violations of the rights to secrecy of communication, to move freely, to freedom of speech and the right to privacy, but also ruled that blanket data retention as embodied by Directive 2006/24 was a disproportionate intrusion into private lives. Such intrusion could only be justified, said the Court, were it "made in a clear, predictable and unambiguous manner, so that the possibility of the arbitrariness or abuse from authorities in this field may be avoided, as much as possible".[108] Yet it is the judgment of the German Constitutional Court (*Bundesverfassungsgericht*) which may prove the most influential of all. The Karlsruhe judges annulled the German implementing law as a disproportionate intrusion into constitutional rights to privacy and "informational self-determination,"[109] as well as the right to the integrity of telecommunications.[110] The criteria of purpose limitation, data security, transparency and safeguards against abuse of data were judged not to have been met by the implementing law, but importantly – and in contrast to the approach of the Romanian judges – the Court clearly stated that data retention in principle is not "absolutely incompatible with article 10 of the German Constitution,"[111] paving the way for revamped domestic legislation respecting these criteria to eventually surface. Following the *Bundesverfassungsgericht* judgment on 2nd March 2010 annulling the domestic German implementing law, over two years passed before the Commission announced on 31st May 2012 that it was referring Germany to the CJEU, requesting that the Court impose financial penalties.[112]

105 The Slovak provisions in question are § 58(5), (6), (7)(a), § 63(6) Act No. 351/2011 Coll. on Electronic Communications (*data retention*); § 116 Penal Procedure Act (Act No. 301/2005 Coll.) (*access to retention data*); and § 76(a)(3) Police Corps Act (Act No. 171/1993 Coll.) (*access to retention data*).

106 http://www.eisionline.org/index.php/projekty-m/data-retention-m/49-sl; see coverage in English by the NGO Statewatch available at http://statewatch.org/news/2012/oct/04slovakian-dret-challenge.htm, both last accessed 16th October 2012.

107 Decision no. 1258 of the Romanian Constitutional Court, 8 October 2009, Romanian Official Monitor No. 789, 23 November 2009. Unofficial English translation available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html [accessed 24th October 2012).

108 Ibid, (no paragraphs in English translation of judgment). For a discussion of the Romanian Constitutional Court's decision, see Bannon, A. (2010), 'Romania retrenches on data retention', *International Review of Law, Computers & Technology* 24(2): 145-152.

109 As developed in domestic jurisprudence from the right to human dignity found in article 1 of the German Constitution (*Grundgesetz*).

110 Protected by article 10, *Grundgesetz.*

111 Para 205.

112 Commission Press Release available at http://europa.eu/rapid/press-release_IP-12-530_en.htm?locale=en, last accessed 16th October 2012.

It seems that more interesting times are ahead, since wrangling over (non)transposition has continued in parallel with a new direct challenge to Directive 2006/24, currently working its way through the Court's systems. The Court of Justice of the EU has already passed judgment once on the Directive, rejecting an action for annulment in early 2009 brought by the Republic of Ireland (with the support of Slovakia), who argued that the Directive should have been adopted on a Third Pillar legal basis, as opposed to its Article 95 EC internal market foundation.[113] Over three years on, a fresh challenge is pending at the Luxembourg court, this time on a reference for a preliminary ruling from the High Court of Ireland.[114] Digital Rights Ireland, a member of the European digital civil rights group EDRi, was granted standing by the domestic court which in turn referred its questions as to whether the Directive is "disproportionate, unnecessary or inappropriate to achieve the legitimate aims of: Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime? and/or Ensuring the proper functioning of the internal market of the European Union," as well as its compatibility with Convention/Charter rights to free movement, privacy, the protection of personal data, freedom of expression and good administration".[115]

It remains, however, difficult to see how the CJEU would be able to assess the compatibility of Directive 2006/24 with Charter rights *inter alia* to data protection and privacy since the instrument itself deals only with retention, and not with access to and use of the data in question. Ultimately, it may be that a future revision of the legislation itself will provide the opportunity to rein in some of its most problematic excesses.

What is the added-value of the Directive from a criminal justice perspective? It is instructive to note from the outset that circumvention of the provisions is quite possible (for example by anonymisation) and, notably, German police statistics in 2011 showed that Data Retention had not reduced crime rates.[116] The Commission's own 2011 evaluation of the Directive failed to enlighten, with the Commission extolling the virtues of the measure[117] and laying any blame for the evaluation's lack of empirical clout at the door of reticent Member States.[118] NGOs such as European Digital Rights, AK

113 Case C-301/06 *Ireland v European Parliament*, *Council of the European Union* [2009] ECR I-00593.

114 Case C-293/12, Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 – *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*;
OJ C 258 from 25.8.2012, p.11.

115 Ibid.

116 http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/.

117 European Commission, Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24 EC), Brussels, 18.4.2011, COM(2011) 225 final.

118 Ibid, p.19: "Reliable quantitative and qualitative data are crucial in demonstrating the necessity and value of security measures such as data retention. This was recognised in the 2006 action plan on measuring crime and criminal justice95 which included an objective for developing methods for regular data collection in line with the Directive and to include the statistics in the Eurostat database (providing they meet quality standards). It has not been possible to meet this objective, given that most Member States only fully transposed the Directive in the last two years and used different interpretations for the source of statistics.".

Vorrat and Panoptykon highlight the potential for abuse of data, data loss, false positives and false negatives (especially where commercial databases are used) as well as the possible generation of new forms of cyber-criminality.[119]

Further to the British controversy over access to retained telecommunications data by local councils, other possible uses of information gathered pursuant to Directive 2006/24 have led to litigation before the CJEU. In the recent *Bonnier*[120] case, article 8 of Directive 2004/48/EC (concerning the enforcement of intellectual property rights) formed the basis for a Swedish law providing the possibility to order an ISP in civil proceedings to disclose the name and address of subscribers alleged to have violated copyright to private parties intent on enforcing their IP rights. The ISP, ePhone, appealed to the Stockholm Court of Appeal, arguing *inter alia* that the injunction sought was contrary to Directive 2006/24/EC since it would entail "disclosure *to persons other than the authorities referred to in the directive* of information relating to a subscriber to whom an IP address has been allocated."[121]

The Court begins its judgment by establishing that Directive 2006/24 deals exclusively with the handling and retention of data generated or processed by the providers of publicly available electronic communications services or public communications networks for the purpose of the investigation, detection and prosecution of serious crime and their communication to the competent national authorities.[122] Indeed, Article 11 of the 2006 Directive amends the e-privacy Directive, effectively disapplying Article 15 (1)[123] of the latter instrument in respect of data specifically requiring retention for the purposes of Article 1(1) of the 2006 Directive.

Thus the possible exceptions to erasure included in the e-privacy Directive, naturally open to interpretation by courts, were transformed into an obligation, or "harmonised" across the Union by the very terms of the 2006 Directive in respect of that instrument's purposes.[124] However, Recital 12 of Directive 2006/24/EC states that "Article 15(1) of Directive 2002/58/EC continues to apply […] *to retention for purposes, including judicial purposes, other than those covered by this Directive*."[125] Taking these provisions

119 For an enlightening overview of possible (mis)uses of personal data including those covered by Directive 2006/24, see AK Vorrat, 'There is no such thing as secure data: Refuting the myths of secure IT systems' (2011), available at http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

120 C-461/10 *Bonnier Audio and Others v Perfect Communication Sweden AB* [2012], judgment of April 12, 2012 (not yet published).

121 Para 31 (emphasis added).

122 Para 40.

123 Article 15(1) of Directive 2002/58/EC (the "e-privacy Directive") lays down exceptions to the Directive's general obligation to erase subscribers' communications data on selected grounds including national security and "unauthorised use of the electronic communication system".

124 Directive 2006/24, Article 11: "The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC: '1 a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1(1) of that Directive.'.

125 Emphasis added.

into account, the Court concludes that Directive 2006/24 "constitutes a special and restricted set of rules",[126] the material scope of which does not cover the Swedish copyright legislation at issue since the latter pursues an objective different from that pursued by Directive 2006/24.[127] No provision of the 2006 Directive could therefore preclude the application of national legislation of the sort in question in the form of an order served on the ISP to identify suspected copyright violators to copyright holders.[128]

In Member States such as Sweden, where communications data were already being retained under national provisions, the 2006 Directive may merely have enshrined data retention in the form of an obligation. Indeed, in *Bonnier* at the time the reference for a preliminary ruling was made, Directive 2006/24 had still not been implemented in Sweden. However, for other Member States which had chosen not to take advantage of Article 15(1) of the e-privacy Directive, the 2006 instrument harmonised the retention of data ostensibly to be used for investigating, detecting and prosecuting serious crime, and the *Bonnier* judgment indicated how such data may be used in civil proceedings relating to intellectual property rights. It is for the Member States "to ensure that they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the European Union legal order",[129] whilst it is for the national court to ascertain that the data at issue have been retained in accordance with national legislation, in compliance with the conditions laid down in Article 15(1) of Directive 2002/58.[130] The potentially serious questions of proportionality raised by this interpretation must however be read in conjunction with the earlier decision of the CJEU in *Scarlet Extended*.[131] Here, the Court decided that the ordering of an injunction forcing an ISP to install a general filtering system infringes the ISP's freedom to conduct business, but also internet users' right to data protection[132] and freedom to receive and impart information.

The anticipated revision of Directive 2006/24 may provide the opportunity to close the *Bonnier* loophole described above, however the reform timetable is less than clear. In December 2011 a Commission communication to the EU Council Working Party on Information Exchange and Data Protection ("DAPIX") indicated that a further Impact Assessment on the Data Retention Directive was due to be completed in May 2012, leading to a new Commission proposal in July 2012. However, in July 2012 the Commission sent an email to the members of EuroISPA, a pan European association of European Internet Services Providers Associations (ISPAs), intimating that the Directive would not be revised in 2012. This was so that the revision of Directive 2006/24 could be handled in parallel with that of the closely-related e-Privacy Directive, the nature of that revision being dependent in turn on progress made on the general Data

126 *Bonnier* judgment, para 43.
127 Ibid, para 34.
128 Ibid, para 61.
129 Ibid, para 56.
130 Ibid, para 37.
131 Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgment of the Court (Third Chamber) of 24 November 2011 (not yet published).
132 Ibid, para 50.

Protection Regulation.[133] The reasoning behind this delay was recently criticised at a November 2012 conference by representatives of the European Data Protection Supervisor, who insisted that the despite a strong opposition of views between stakeholders, it would be preferable to revise the Directive as soon as possible.[134]

V. Conclusion: The need for a comprehensive data handling framework

Whilst the identification of citizens is a crucial part of the state's basic function – private legal interactions would not be juridically possible without a regulation of individuals' identity[135] – mass surveillance is perceived as more worrisome due to its potential "chilling effect" and grave implications for data protection and privacy, anchored in human dignity. Privacy also has instrumental social value in protecting other, more obviously political rights such as freedom of expression, freedom of association, or freedom of religion: "[b]y ensuring that there is a limit on what the state can reasonably expect to know about us, privacy not only helps to protect individual autonomy, but also censures that we are free to use that autonomy in the exercise of other fundamental rights".[136]

Data mining and profiling techniques allow essentially banal data, whether those data be telecommunications, airline bookings or financial records, to be processed in order to reveal sensitive information and build detailed profiles of individuals. The process might be likened to alchemy, transforming the potential of information in such a way as to nullify certain prohibitive data protection rules, since those rules are formulated in terms of types of individual pieces of data. Beyond privacy and data protection, profiling – defined as an attempt to give specific content to what particular persons or classes of persons are like: their preferences, their practices, their personal histories, and so on, in order to anticipate future behaviour[137] – would also appear to risk undermining the normative foundations of the presumption of innocence. This last principle is born of a deeper assumption built into our legal systems that each of us is free to choose to act differently in the future than we did in the past.[138] A high price should be exacted in return for its weakening, in the form of demonstrable crime prevention benefits, proportionate restrictions to fundamental rights, and legal certainty for individuals. For this to be so, the European Parliament and the Court of Justice will have increasingly important roles to play in the development of a truly comprehensive EU-level framework for the handling of personal data in the law enforcement sector, addressing not only the

133 Email from Commission to EuroISPA available at https://publicaffairs.linx.net/news/?p=8453 l, last accessed 16th October 2012.

134 Presentation of Herke Kranenborg, 'Revising the data retention Directive: Just do it and do it now', ERA Conference, *Data Protection in the Area of European Criminal Justice Today*, 6th November 2012, Trier, Germany.

135 Thorburn, M. (2012), 'Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data', in Sullivan, G. R. and Dennis, I., eds. (2012) *Seeking Security: Pre-Empting the Commission of Criminal Harms* (Hart Publishing), p.17.

136 Goold, B. (2009), 'The Political Value of Privacy', *Amsterdam Law Forum,* VU University Amsterdam, pp.2-3.

137 Thorburn, M., op cit. n.133, p17.

138 Ibid, p.33.

collection of information, but access to the databases, sharing of data, security, retention, transparent system architecture and processing, as well as independent oversight.