BRILL
NIJHOFF

TILBURG LAW REVIEW 20 (2015) 35-57

Tilburg
Law Review
brill.com/tilr

The Transformation of Privacy in an Era of Pre-emptive Surveillance

Valsamis Mitsilegas
Professor of European Criminal Law, Director of the Criminal Justice Centre
Head of the Department of Law, Queen Mary University, London
v.mitsilegas@qmul.ac.uk

Abstract

The aim of this article is to analyse the main elements of the emergent system of pre-emptive surveillance at a global scale and to assess the consequences of such a system for the protection of privacy. Firstly, the article will provide an analysis of pre-emptive surveillance practices as projected by US and EU law, focusing on the collection and exchange of every day passenger data (PNR), financial data (under the TFTP Programme) and mobile telecommunications data. After this mapping of pre-emptive surveillance practices, a critical overview of the impact of these practices on privacy will follow. Thereafter, the article will critically evaluate the legal responses that have been primarily developed in EU law in order to address the privacy challenges posed by pre-emptive surveillance. The aim is to highlight the transformation of the right to privacy by judiciaries in Europe in order to counter generalised, massive pre-emptive surveillance in the EU, the US and globally.

Keywords

counter-terrorism – privacy – data protection – surveillance – PNR – TFTP – data retention

* This is a revised and updated version of a paper presented at the workshop on Constitutionalism Across Borders in the Struggle Against Terrorism, held at Harvard Law School on 6–7 March 2014. The author would like to thank all workshop participants for their insights and comments.

 | DOI 10.1163/22112596-02001006

1 Introduction

9/11 has proven a catalyst for the transformation of surveillance practices in the United States (US). In the post-9/11 landscape, pre-emption is key: the aim is to predict the future and to prevent potential terrorist attacks from happening. Surveillance thus becomes pre-emptive and generalised. The manner in which the 9/11 attacks have occurred focuses the attention of state authorities to data stemming from private everyday transactions such as issuing an airline ticket or proceeding to a wire transfer. A perceived state of emergency has led to the initiation of a series of operations and pieces of legislation aiming to ensure the maximum reach of US authorities into everyday personal data. The purpose of the collection and analysis of such data is primarily forward-looking, aiming at the identification and prevention of future terrorist threats. The perception of terrorism as a global threat has led to the externalisation of these practices, with the US applying these practices - legally or operationally - extraterritorially. The application of this pressure to European Union (EU) countries has raised a number of persistent questions with regard to the compatibility of this model of pre-emptive surveillance with fundamental rights, and in particular the right to privacy. The aim of this article is to analyse the main elements of this emergent system of pre-emptive surveillance at a global scale and to assess the implication of such a system on privacy. Section 2 is devoted to the analysis of pre-emptive surveillance as projected by US and EU law and to an analysis of the impact of pre-emptive surveillance on privacy. Section 3 evaluates critically the legal responses developed primarily in the EU to address the privacy challenges posed by pre-emptive surveillance. The article will analyse the emphasis on and limits of data protection law and will focus on the transformation of the right to privacy by judiciaries in Europe in order to counter generalised, massive pre-emptive surveillance in the EU, the and globally.

2 Pre-emptive Surveillance, Privacy and Globalisation

The reconfiguration of the security landscape in recent years has resulted in the transformation of the relationship between the individual and the state. A catalyst towards this transformation has been the growing link between securitisation and pre-emptive surveillance, and the focus of security governance on the assessment of risk.[1] Central in this context is the emphasis on the

1 L Amoore and M de Goede (eds), *Risk and the War on Terror* (Routledge 2008).

future, and the aim of pre-emptive surveillance to identify and predict risk and dangerousness.[2] The pre-emptive turn in surveillance has been based largely upon the collection, processing and exchange of personal data, which has in turn been marked by four key features. The first feature concerns the *purpose* of data collection and processing. This is no longer focused solely on data related to address the commission of specific, identified criminal offences, but rather targets the use of personal data to predict risk and pre-empt future activity. The second feature concerns the *nature* of the data in question: Pre-emptive surveillance is increasingly taking the form of the collection of personal data generated by ordinary, everyday life activities. Key examples constitute the collection, processing and transfer of personal data on financial transactions, airline travel and mobile phone telecommunications. The third feature of pre-emptive surveillance concerns the *scope* of data collection, processing and transfer, with the focus on monitoring everyday life resulting in generalised and mass surveillance, marked by the collection and storage of personal data in bulk. The fourth feature concerns the *actors* of surveillance, with the state increasingly co-opting the private sector in surveillance practices. This privatisation of surveillance constitutes another example of the responsibilisation strategy whereby the private sector is co-opted by the state in the fight against crime.[3] The deployment of the responsibilisation strategy based on the imposition of preventive duties on the private sector has been central in the development of new forms of global security governance, including the global and European anti-money laundering regime.[4] While however in the anti-money laundering framework the private sector is called to transfer proactively private financial data to the state on the basis of specific suspicions, the privatisation of surveillance entails the collection and transfer of personal data without any prior internal risk assessment. Massive quantities of every day personal data is thus collected by the private sector for the primary purpose of risk assessment of future threats, constituting what de Goede has termed 'speculative security practices'.[5] This move towards speculative security, under a system of pre-emptive surveillance, poses fundamental challenges to the rights to private life and data protection, but also more broadly to

2 D Bigo, 'Security, Exception, Ban and Surveillance' in D Lyon (ed), *Theorizing Surveillance. The Panopticon and Beyond* (Willan 2006) 46.

3 On the responsibilisation strategy, see D Garland, 'The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society' (1996) 36 British Journal of Criminology 445.

4 V Mitsilegas, *Money Laundering Counter-measures in the EU* (Kluwer Law International 2003).

5 M de Goede, *Speculative Security* (University of Minnesota Press 2012).

the presumption of innocence and concepts of citizenship and trust within the framework of the relationship between the individual and the state.[6] These challenges will be analysed in greater detail after an overview of the main elements of pre-emptive surveillance from a comparative and transatlantic perspective.

2.1 *Pre-emptive Surveillance and Passenger Data – the PNR Case*

One of the key strands of US counter-terrorism policy post-9/11 has been the requirement for airlines to collect detailed personal data from their passengers in advance of travel in order for such data to be available to the Department of Homeland Security. The emphasis on pre-emptive surveillance in this context can be viewed in the light of the way in which the 9/11 attacks occurred. The US Strategy for Homeland Security, which was adopted in response to the 9/11 attacks, stressed the increasing mobility and destructive potential of modern terrorism and the interdependence between US responses and the global transport infrastructure.[7] To achieve the prevention of potentially dangerous mobility to the US on a global scale, the US passed legislation in November 2001 requiring air carriers operating flights to, from or through the US to provide US Customs with electronic access to data contained in their automatic reservation and departure control systems.[8] These data, known as Passenger Name Records (PNR), constitute records of each passenger's travel requirements and contain all the information necessary to enable reservations to be processed and controlled by the booking and participating airlines. Transfer to such information to the US authorities before departure has been a key element of the US border security strategy focusing on identification and prevention. PNR data can include a wide range of details, from the passengers' name and address to their email address, credit card details and on-flight dietary requirements. The transfer of PNR data was deemed to be key to the operation of the US Automated Targeting System (ATS), which uses a wide range of databases, including law enforcement and FBI databases 'to assess and identify (…) travellers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination.'[9] US counter-terrorism

6 V Mitsilegas, 'The Value of Privacy in an Era of Security' (2014) 8 International Political Sociology 104–108 (forthcoming).

7 Office for Homeland Security, 'National Strategy for Homeland Security' (2002) 21.

8 Title 49 US Code section 44909(c)(3) and title 19 Code of Federal Regulations section 122.49b.

9 Department of Homeland Security, Privacy Office, 'A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union' (2008) 38. For further analysis, see V Mitsilegas, 'Immigration Control in an Era of Globalisation:

requirements post-9/11 thus established a generalised system of pre-emptive surveillance of all airline passengers flying to the US.

The imposition of these duties to air carriers has placed them in an uncomfortable position with regard to EU law. Compliance with US requirements to collect and transfer passenger data on such a large scale could result in carriers acting in breach of EU data protection law.[10] In an attempt to reconcile these competing requirements, the European Commission embarked in negotiations with the US authorities with the view of concluding a transatlantic agreement enabling the collection and transfer of PNR records to the US in accordance with EU law. The proposed agreement was criticised heavily by data protection bodies in the EU as well as by the European Parliament for falling short of respecting EU fundamental rights.[11] On the basis of a Decision by the Commission confirming the adequacy of US data protection standards,[12] a transatlantic agreement on the transfer of PNR data to the US Bureau of Customs and Border Protection was signed in 2004. In the Decision authorising the Conclusion of the Agreement (which was accompanied by the iteration of a series of US Undertakings with regard to its operation),[13] the Council evoked the urgency caused by the uncertainty for carriers and passengers.[14] The Agreement was subsequently litigated before the Court of Justice of the EU, where the European Parliament brought an action for annulment of the Decision authorising the conclusion of the Agreement on grounds of legality, proportionality and infringement of the fundamental rights of privacy and data protection. In what can be characterised as a 'pyrrhic victory' for the European Parliament, the Court annulled the measure on legality (competence) grounds, but without examining the substance of the Parliament's allegation

Deflecting Foreigners, Weakening Citizens, Strengthening the State' (2012) 19 Indiana Journal of Global Legal Studies 3.

10 See Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

11 For further details, see V Mitsilegas, 'Contrôle des Étrangers, des Passagers, des Citoyens: Surveillance et Anti-terrorisme' (2005) 58 Cultures et Conflits 155.

12 Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection [2004] OJ L235/11.

13 Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [2004] OJ L183/83

14 Ibid, Preamble Recital 2.

of lack of compliance with fundamental rights.[15] The annulment of the Agreement resulted in the conclusion of an interim Agreement, and eventually in 2007 of an EU-US PNR Agreement.[16] This Agreement has done little to address concerns with regard to the compatibility with EU law of the system of authorisation of the collection and transfer of PNR data to the US established therein.[17]

The entry into force of the Lisbon Treaty meant that the European Parliament, which had a limited role with regard to the conclusion of international agreements under the old third pillar, was called to consent to the 2007 EU-US PNR Agreement. The Parliament expressed concerns about the compatibility of the Agreement with EU privacy and data protection law. The Parliament decided to postpone the vote on the request for consent on the agreements with the US and Australia until it had explored the options for arrangements for the use of PNR that were in line with EU law and meet the concerns expressed by Parliament in earlier resolutions on PNR[18] and called upon the Commission to put forward a single set of principles to serve as a basis for negotiations with third countries.[19] The policy impact of Parliament's calls was the publication of a Commission Communication on a global PNR strategy.[20] In November 2010, the European Parliament welcomed the Commission's PNR strategy and endorsed the opening of new PNR negotiations with the US. The Parliament stressed the need for the inclusion of a number of data protection safeguards including necessity and proportionality and emphasising that PNR data must not be used for data mining or profiling.[21]

15 Joined cases C-317–04 and 318/04 *European Parliament v Council* [2006] ECR I-04721.

16 For details, see V Mitsilegas, 'The External Dimension of EU Action in Criminal Matters' (2007) 12 European Foreign Affairs Review 457.

17 Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) [2007] OJ L204/16, 18.

18 European Parliament Resolution P7_TA (2010)0144 of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada [2011] OJ C81E/70 Point 4.

19 Ibid Point 7.

20 Commission, 'On the Global Approach to Transfers of Passenger Name Record (PNR) data to third countries', (Communication) COM (2010) 492 final.

21 European Parliament Resolution P7_TA-PROV (2010)0397 of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the European Union and Australia, Canada and the United States [2010].

The negotiation of a new transatlantic PNR Agreement was met with scepticism in the US, with a number of voices in the US arguing that the provisions of the 2007 Agreement – which was heavily focused on security and consisted largely of a US Letter to the EU – should be maintained and that a new Agreement was not necessary.[22]

The new EU-US PNR Agreement was eventually approved by the European Parliament in early 2012 and took effect on June 1, 2012.[23] The Agreement will remain in force for a period of seven years after its entry into force and, unless one of the Parties notifies of its intention not to renew further, will be renewable for subsequent seven year periods.[24] Its structure is a significant improvement from a rule of law perspective, as the main provisions and safeguards are set out largely in the text of the EU-US Agreement itself, rather than in a Letter by the US to the EU, as was the case with the 2007 Agreement. The purpose of the Agreement is defined in rather broad terms: 'to ensure security and to protect the life and safety of the public.'[25] This broad wording may challenge calls for the inclusion of strict purpose limitation safeguards under the Agreement. It applies to a wide range of carriers: to carriers operating passenger flights between the EU and the US,[26] as well as to carriers incorporated or storing data in the EU and operating passenger flights to or from the US.[27] The Agreement establishes an obligation for carriers to provide PNR data contained in their reservation systems to the US Department of Homeland Security (DHS) as required by DHS standards and consistent with the Agreement.[28] Data transmission will occur initially 96 hours before departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.[29] As with the previous transatlantic PNR Agreements, the

22 K Archick, 'U.S.-EU Cooperation Against Terrorism' (CRS Report for Congress 7–5700 RS22030, 4 September 2013).

23 Council Decision 2012/471/EU of 13 December 2011 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security [2012] OJ L215/1; Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security [2012] OJ L215/4.

24 Ibid Council Dec 2012/472/EU Arts. 26(1) and (2).

25 Ibid, Art. 1(1).

26 Ibid, Art. 2(2).

27 Ibid, Art. 2(3).

28 Ibid, Art. 3.

29 Ibid, Art. 15(3). But see exceptions in Art. 15(5).

actual categories of PNR data to be transferred to the US Homeland Security Department are listed in an Annex to the Agreement. The Annex contains 19 categories of PNR data. The Agreement thus maintains the paradigm of the privatisation of crime control set out in earlier Agreements and imposes extensive obligations on carriers to transmit a wide range of everyday personal data to the US Homeland Security Department.

The fundamental rights concerns arising from the latest transatlantic PNR agreement are compounded by calls for the EU to internalise the US approach on pre-emptive surveillance by mirroring the US system in creating a system whereby airlines flying into the EU are required to collect and transfer PNR data to European authorities before travel. The EU-US PNR Agreement itself envisages the potential establishment of such an EU PNR system by stating that if and when an EU PNR system is adopted, the Parties will consult to determine whether this Agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations will in particular examine whether any future EU PNR system would apply less stringent data protection safeguards than those provided for in this Agreement and whether, therefore, this Agreement should be amended.[30] The European Commission tabled a proposal for a Framework Decision on an EU PNR system as early as 2007. Agreement on the proposal was not reached before the entry into force of the Lisbon Treaty, a fact which led the Commission to table new legislation post-Lisbon, this time in the form of a Directive.[31] Parallel to such calls for the establishment of an EU PNR system and negotiations by the EU to conclude PNR agreements with other third countries including Australia and Canada, the Commission has also been calling for the development of a global regime for the collection and transfer of PNR data. In its Communication on a Global Approach to Transfers of PNR Data to Third Countries,[32] the Commission called upon the EU to consider initiating discussions with international partners that use PNR data and those that are considering using such data in order to explore whether there is common ground between them for dealing with PNR transfers on a multilateral level. In this manner, a system of generalized pre-emptive surveillance which has been imposed unilaterally by the US as an

30 Ibid Art. 20(2).

31 Commission Proposal COM(2011) 32 final of 2 February 2011for 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 Crimes [2011].

32 Commission, 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries' (Communication) COM (2010) 492 final.

emergency post-9/11 response potentially becomes normalised via EU action on a global scale, notwithstanding the persistent concerns with regard to the compatibility of such a system with European human rights law.

2.2 *Pre-emptive Surveillance and Financial Data- the Case of the TFTP*

Another instance of US authorities initiating generalised pre-emptive surveillance post-9/11 has been the establishment of the Terrorist Financing Tracking Programme (TFTP). Under this Programme, US authorities had access to bulk: everyday personal data generated by financial transactions in Europe and held by SWIFT. SWIFT is a worldwide financial messaging service that facilitates international money transfers. Routine access to SWIFT data by US authorities was revealed in 2006: the TFTP programme was initiated in secret weeks after 9/11 and run out of the CIA and overseen by the Treasury Department and was a significant departure from typical practice in how the US government acquires Americans' financial records. Treasury officials did not seek individual court-approved warrants or subpoenas to examine specific transactions, instead relying on broad administrative subpoenas for millions of records from SWIFT.[33] The revelation caused alarm in Europe, with both data protection supervisors and the European Parliament expressing doubts about the compatibility of US access to SWIFT data with European data protection law.[34] In response to these concerns, the US authorities made Representations to the EU, explaining the legal basis for the collection of SWIFT data under US law[35] and confirming the emergency framing of US executive action.[36]

---

33 E Lichtblau and J Risen, 'Bank Data is Sifted by US in Secret to Block Terror' *New York Times* (New York, 23 June 2006); <http://www.nytimes.com/2006/06/23/washington/23intel.html?_r=0&pagewanted=all&_r=0> accessed 21 September.

34 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' 06/EN/01935 WP128; European Parliament Resolution P6_TA(2006)0317 on the interception of bank transfer data from the SWIFT system by the US secret services [2006] OJ C303E/843; European Parliament Resolution P6_TA(2007)0039 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues [2007] OJ C287E/349.

35 Representations of the United States Department of the Treasury, 'Terrorist Finance Tracking Program' [2007] OJ C166/18.

36 On 23 September 2001 the President issued Executive Order 13224. In that Order, the President declared a national emergency to deal with the 9/11 terrorist attacks and the continuing and immediate threat of further attacks, and blocked the property of, and prohibited transactions with, persons who commit, threaten to commit, or support terrorism.

The legal force of the US Representations and the extent to which they could address EU constitutional concerns are both questionable. At the same time, SWIFT decided to alter the architecture of its databases to avoid mirroring European databases in US territory. This change in SWIFT architecture meant that US authorities no longer had automatic access to SWIFT data generated in Europe.[37] This development rendered necessary the conclusion of a transatlantic agreement allowing access by US authorities to such data. Negotiations began before the entry into force of the Lisbon Treaty, with the European Parliament already reiterating its data protection concerns and calling for the adoption of a series of safeguards.[38] The first EU-US TFTP Agreement was signed by the Council on 30 November 2009, a day before the entry into force of the Lisbon Treaty.[39] The Agreement would be applied on a provisional basis from 1 February 2010 pending its entry into force and would last for a maximum duration of nine months with the view to the conclusion of a further agreement between the EU and the US post-Lisbon under the new procedure on conclusion of international agreements. This would require the active involvement of the European Parliament.[40] Post-Lisbon, the negotiation and conclusion of international agreements such as the TFTP require the consent of the European Parliament. The 2009 EU-US TFTP Agreement thus presented the European Parliament with a *fait accompli*.[41] Member States chose to sign the Agreement before the entry into force of the Lisbon Treaty, in what can be seen as an attempt to force Parliament into approving an agreement that was crystallised under the old negotiation rules, which granted Parliament a minimal scrutiny role. This perceived attack on Parliament's institutional prerogatives post-Lisbon led to the European Parliament, notwithstanding sustained

37 A Amicelle, 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism. From Criticism to Imitation of Dataveillance' (2013) 56 Liberty and Security in Europe 5–6.

38 European Parliament Resolution P7_TA(2009)0016 of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing.

39 Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program [2010] OJ L8/9.

40 Ibid Preamble recitals 3 and 4.

41 See also J Monar, 'Editorial Comment. The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications' (2010) 15 European Foreign Affairs Review 143.

high level pressure from European governments and the US administration,[42] to reject the EU-US TFTP Agreement in February 2010, depriving thus the US authorities from a legal basis of accessing European SWIFT data.[43] Post-Lisbon, the European Parliament has the power to veto the conclusion of international agreements negotiated on behalf of the EU.[44] The European Parliament confirmed that the TFTP 'must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records.'[45]

The rejection of the first EU-US TFTP Agreement did not halt negotiations in the field. Resuming negotiations was deemed a matter of urgency by both the US and European governments on the grounds that non-access by US authorities to European SWIFT data would represent a major security gap. Negotiations, this time fully post-Lisbon, led to the conclusion in the summer of 2012 of the second EU-US TFTP Agreement which is currently in force.[46] According to Article 1, the Agreement serves the dual purpose of providing the US Treasury with financial payment messages for the exclusive purpose of the prevention, investigation, detection or prosecution of terrorism or terrorist financing and of providing relevant information obtained through the TFTP to law enforcement, public security or counter terrorism authorities of Member States, or Europol or Eurojust for the purpose of the prevention, investigation, detection or prosecution of terrorism or terrorist financing. However, the Agreement allows the provision of SWIFT data to a wide range of authorities[47] and the agreement does not preclude onward transmission to third countries.[48] As with the previous Agreement, the new EU-US TFTP Agreement

42 Ibid, 145.

43 European Parliament Resolution P7_TA(2010)0029 of 11 February 2010 on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] (05305/1/2010 REV 1– C7–0004/2010–2009(190(NLE).

44 Ibid Arts. 218(6) and (4) TFEU.

45 Ibid (n 43).

46 Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L195/3.

47 Ibid Art. 3. SWIFT is the only listed entity in the Annex.

48 Ibid Art. 7.

legitimises under EU law the bulk transfer of every day financial data stemming from ordinary financial activities to the US authorities. The legal challenges with regard to the bulk transfer of data were also highlighted by the European Data Protection Supervisor in the Opinion of the draft Agreement, where it was noted that solutions should be found to ensure that bulk transfers are replaced with mechanisms allowing financial transaction data to be filtered in the EU, and ensuring that only relevant and necessary data are sent to US Authorities.[49]

In a manner similar to the evolution of transatlantic co-operation on the transfer of PNR data, the conclusion of a transatlantic agreement has been accompanied by calls for the internalisation of the US approach to TFTP by the EU via the establishment of an EU TFTP Programme. As in the case of PNR, the establishment of this system is viewed as a means of ensuring reciprocity. In the case of the TFTP, it is thought that an EU system will grant EU institutions a greater degree of control over personal data to be transferred. The possibility of establishing an EU TFTP Programme is set out in the EU-US TFTP Agreement itself: during its course the Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data;[50] if the EU decides to establish an EU system, the US will cooperate and provide assistance and advice to contribute to the effective establishment of such a system;[51] if the EU decides to establish such a system, the Parties should consult to determine whether this Agreement would need to be adjusted accordingly.[52] According to the Decision on the conclusion of the Agreement, the Union shall consider whether to renew the Agreement if, five years after the entry into force of the Agreement, the equivalent EU system has not been set up in accordance with Article 21(2) thereof.[53] The Commission's report on the second joint review of the Agreement indicates that close cooperation and consultation with the US on this issue will continue to be[54] and states explicitly that the functioning of reciprocity under the Agreement is an essential factor in assessing the necessity of a possible establishment of an equivalent EU system.[55]

49 Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data of 22 June 2010, para 20.

50 Ibid (n 46) Art. 11(1).

51 Ibid Art. 11(2).

52 Ibid Art. 11(3).

53 Ibid Art. 2 third indent.

54 Ibid Art. 11(3).

55 European Commission Staff Working Document SWD(2012) 454 final of 14 December 2012 Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of

The Commission has published a Communication setting out options for a European TFTP system, which indicates that an EU TFTP system remains an option under consideration by EU institutions.[56] However, the establishment of an EU TFTP system would signal the normalisation and legalisation of a unilateral, emergency executive US initiative by the EU and the introduction in EU law of yet another system of generalised surveillance that significantly challenges fundamental rights in Europe.

2.3 *Pre-emptive Surveillance and Electronic Communications Data – the case of Data Retention*

Another key instance of the state co-opting the private sector to establish a system of generalised pre-emptive surveillance for counter-terrorism purposes involves the imposition to telecom companies of the obligation to retain metadata concerning phone calls or e-mails of their customers and/or to transfer such data to state authorities. Data retention and transfer systems have been established and developed in parallel in the EU and the US. As explained by Arianna Vedaschi and Valerio Lubello elsewhere in this Special Issue, the EU institutions adopted the Data Retention Directive in 2006, under the impetus of the Madrid and London terrorist attacks, and following a long discussion.

The Data Retention Directive aims to harmonise Member States' data retention provisions, 'in order 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 its national law'.[57] Telecommunications providers are placed under an obligation to retain data, by derogation from Directive 2002/58/EC.[58] Data must be retained for periods 'no less than six months and not more than two years from the date of the communication'.[59] Moreover, the

---

Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2012] 14. For further analysis on the use of reciprocity in transatlantic counter-terrorism co-operation see V Mitsilegas, 'Transatlantic Counter-terrorism Cooperation and European Values. The Elusive Quest for Coherence' in D Curtin and E Fahey (eds), *A Transatlantic Community of Law* (Cambridge University Press 2014) 289–315.

56 Commission, 'A European Terrorist Finance Tracking System: Available Options' (Communication) COM (2011) 429 final.

57 Council Directive 2006/24/EC 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 Art. 1(1).

58 Ibid Art. 3(1).

59 Ibid Art. 6.

retention period may be extended by Member States 'facing particular circumstances that warrant an extension'.[60] Access to retained data is limited 'only to the competent national authorities in specific cases and in accordance with national law'.[61] However, the Directive does not define further what constitutes a competent authority in this context, leaving the designation of such authorities to Member States. Access to personal data is governed by national law, in accordance with necessity and proportionality and subject to EU and international law, in particular the ECHR.[62] Specific provisions on data protection[63] (including a provision on the designation of supervisory authorities by Member States[64]) and remedies[65] are also included in the Directive. However, these provisions are specific and limited and their substance, in particular with regard to judicial remedies is left for Member States to define.[66]

Unlike EU law, US law allows the collection of bulk telephone records directly by the NSA under the telephone records programme that the NSA operates under section 215 of the Patriot Act. The programme is operated under an order issued by the FISA court pursuant to Section 215 of the Patriot Act, an order that is renewed approximately every ninety days. This is another post-9/11 emergency measure. According to the recent report of the US Privacy and Civil Liberties Oversight Board in October 2001, US President George W. Bush issued a highly classified presidential authorisation directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the US. Under this authorization, electronic surveillance was permitted within the US for counterterrorism purposes without judicial warrants or court orders for a limited number of days. President Bush authorized the NSA to collect the contents of certain international communications under the Terrorist Surveillance Program (TSP), and collect in bulk non-content information, or 'metadata' about telephone and Internet communications.[67] According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, 'the program became less a

60 Ibid Art. 12(1).

61 Ibid Art. 4.

62 Ibid.

63 Ibid, Arts. 7–9.

64 Ibid, Art. 9.

65 Ibid, Art. 13.

66 Ibid, Art. 13(1).

67 Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted Under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court' (23 January 2014) 37, see: < https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf> accessed 26 August 2014.

temporary response to the September 11 terrorist attacks *and more a permanent surveillance tool'*.[68] The Privacy Board's report indicates that from late 2001 through early 2006, the NSA collected bulk telephony metadata based upon presidential authorizations issued every thirty to forty-five days.[69] In May 2006, the FISC first granted an application by the government to conduct the telephone records program under Section 215. Following the publication by the Guardian in June 2013 of an article concerning the revelations about the programme by Edward Snowden, FISC Judge Claire Eagan issued an opinion in August 2013, in which she explained the court's rationale for approving the Section 215 telephone records programme. This judicial opinion was the first explaining the FISA court's legal reasoning in authorising the bulk records collection.[70] The Privacy Board has explained clearly and in detail the main functions and content of this far-reaching programme by emphasising the collection of 'metadata', which involves the collection of telephone records from the NSA, their storage in a centralised database and the running of queries by NSA analysts involving up to three 'hops' of connection with the data.[71]

2.4 *Pre-emptive Surveillance and the Individual*

The combination of these features of pre-emptive surveillance extends considerably the reach of the state and poses grave challenges to privacy. Surveillance is occurring on a generalised, massive scale, via the proliferation of channels of data collection, processing and exchange as well as the generalisation of the collection of every day personal data by bulk and the use and processing of such data by the state. The collection and use of personal data on this scale has led to the phenomenon of what has been called 'the disappearance of disappearance'- a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions.[72] State authorities have thus access to a wealth of personal data enabling practices such as profiling and data mining. The impact of state intervention on the individual is intensified when one considers the potential of combining personal data from different databases collected for different purposes in order to create a profile of risk or dangerousness. This impact is even more far-reaching when everyday personal data collected under the processes of pre-emptive

68 Ibid, 105–106.

69 Ibid, 141.

70 See (n 68) 8–10.

71 Ibid.

72 KD Haggerty and RV Ericson, 'The Surveillant Assemblage' (2000) 51 British Journal of Sociology 605.

surveillance analysed in this article are combined with personal data resulting from the deepening of surveillance practices by the state including DNA samples and biometrics.[73] In addition to the substantive privacy challenges these developments pose, risk assessment in these terms also challenges the place of the citizen in a democratic society. According to Lyon:

'Data from the body (such as biometrics, DNA) or triggered by the body (…) are sucked into databases to be processed, analysed, concatenated with other data, then spat out again as a 'data double.' The information that proxies for the person is made up of 'personal data' only in the sense that it originated with a person's body and may affect their life chances and choices. The piecemeal data double tends to be trusted more than the person'.[74]

The use of personal data in those terms leads to a process whereby individuals embarking on perfectly legitimate everyday activities are constantly being assessed and viewed as potentially dangerous without having many possibilities of knowing or contesting such assessment. As Solove has noted, predictive determinations about one's future behaviour are much more difficult to contest than investigative determinations about one's past behaviour.[75] Generalised pre-emptive surveillance thus has considerable implications not only for privacy as such but also for the rule of law and citizenship, and for the relationship between the citizen and the state more broadly. The adverse effect of surveillance on the freedom of action of citizens in a democratic society has been noted as early as the 1980s by one of the fathers of privacy law in Europe, Spiros Simitis. Simitis recognised that personal information is increasingly used to enforce standards of behaviour, with information processing developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct.[76] Simitis conceptualised privacy as both a refuge for the individual and a condition for participation,[77] noting that inhibition tends to be the rule once automated processing of personal data becomes a normal tool of both government and private enterprises.[78] The negative impact of surveillance on citizenship and democracy, including fundamental rights such as freedom of expression and association, has also been

73 On the deepening of surveillance in the context of biometrics see Mitsilegas (n 11).

74 Z Bauman and D Lyon, *Liquid Surveillance: A Conversation* (Polity 2013) 8.

75 DJ Solove, 'Data Mining and the Security-Liberty Debate' (2008) 74 University of Chicago Law Review 343, 359.

76 S Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707.

77 Ibid 729ff and 732ff respectively.

78 Ibid 734.

flagged up by scholars and scrutineers on the other side of the Atlantic. Cohen has argued that freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship.[79] According to Cohen, a society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy.[80] The adverse impact of mass surveillance on democracy has been eloquently expressed in the US as 'the chilling effect.' In its Report on the NSA telephone surveillance programme, the US Privacy and Civil Liberties Oversight Board noted that the bulk collection of telephone records by the NSA can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups engaged in sensitive or controversial work have less reason to trust in the confidentiality of their relationships as revealed by their calling patterns.[81]

3 Legal Responses to Pre-emptive Surveillance: From Data Protection to Privacy, from Legislative to Judicial Protection

The various transatlantic agreements analysed above and the data retention Directive attempted to address the privacy challenges posed by the systems of pre-emptive surveillance they established by focusing on data protection as a safeguard on three different levels. Firstly, EU legislative instruments contain a number of specific provisions on the protection of personal data. Secondly, the transatlantic agreements are based on a presumption of adequacy of the US data protection framework, which justifies the transfer of personal data to the US from the EU. Declarations of adequacy have been central to the conclusion of transatlantic PNR and TFTP Agreements.[82] Thirdly, the agreements aim at safeguarding data protection by introducing additional elements of monitoring and review at the implementation stage, with a key example being the EU-US TFTP Agreement which provides for a system of ex ante scrutiny in the EU before data is being transmitted by Europol and an ex post mechanism of scrutiny in the US by an EU representative.[83] The provisions on oversight and review in these agreements can be considered as representative examples of experimentalist governance. As de Goede has noted in relation to the TFTP agreement, the

79 JE Cohen, 'What Privacy is For' (2013) 126 Harvard Law Review 1904.

80 Ibid 1912.

81 Privacy and Civil Liberties Oversight Board (n 68) 13.

82 See Article 19 of the latest EU-US PNR Agreement and Article 8 of the TFTP Agreement.

83 Articles 4 and 12 of the EU-US TFTP Agreement respectively. For further details of the review and adequacy arrangements see Mitsilegas (n 55).

SWIFT affair can be comprehended through the lens of experimentalist governing which draws attention to the processes of 'recursive definition of means and ends' through which participants learn 'what problem they are solving, and what solution they are seeking, through the very process of problem solving'.[84]

However, these three levels of data protection safeguards have not proven to provide an effective protection of privacy and their potential to address the challenges posed by generalised pre-emptive surveillance on the affected individuals remain questionable. As mentioned earlier in the article, the data protection provisions included in the various instruments are limited and subject to national discretion of EU Member States or a number of caveats regarding US law. The presumption of adequacy of the US data protection system is highly questionable, especially in the light of the recent Snowden revelations and the current debate on privacy taking place in the US. Recent implementation reports on the functioning of the transatlantic agreements on PNR and TFTP have demonstrated that the various monitoring and review mechanisms established therein have not resulted in an effective data protection control or in a meaningful scrutiny or limitation of generalised surveillance as set out in the agreements.[85] None of these three levels of data protection safeguards questions the very essence and principle of the mass collection of everyday personal data from the private sector. Data protection standards in the articulation of EU law act largely in the aftermath of the collection of such data and are set out to place limits on the subsequent transfer or processing of such data. However, even at that level, the protection offered by the legislative instruments remains limited.

The limits of the EU instruments analysed in this article can be explained within the broader framework of the limits of data protection law when viewed independently from a more general framework of the protection of privacy. The use of data protection as a regulatory tool for surveillance offers a number of distinct advantages: data protection rules follow and regulate in detail instances of data collection, processing and exchange; data protection rules have established and developed key substantive legal principles addressing challenges posed in particular by the extension of access and use of personal data such as the principle of purpose limitation; data protection also focuses on issues of procedural justice by establishing rules on remedies for the data

84 M de Goede, 'The SWIFT Affair and the Global Politics of European Security' (2012) 50 Journal of Common Market Studies 214, 222, referring to Sabel and Zeitlin, *Experimentalist Governance in the European Union. Towards a New Architecture* (Oxford University Press 2010) 11.

85 Mitsilegas (n 55).

subject; developments in data protection law have led to proposals for substantive legislative innovations in the field, including recent proposals on the introduction of a 'right to be forgotten';[86] and last but not least, the development of substantive data protection rules has been inextricably linked with a strong institutional framework in the form of expert, dedicated supervisory bodies whose role is both to advise on legislative developments impacting upon data protection and to enforce data protection law. However, there are two main limitations on the effectiveness of data protection alone to address the challenges posed by pre-emptive surveillance. The first limitation stems from the limited capacity of data protection to question the political choice to maximise and generalise the collection and processing of personal data as such. As it has been noted, data protection differs from privacy as it does not aim to create zones of non-interference by the state, but rather operate on a presumption that public authorities *can* process personal data. It follows that 'the sheer wordings of the data protection principles (…) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice', with data protection law creating 'a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal'.[87] The second limitation of data protection in relation to privacy is the specificity of data protection which is in turn linked with the difference in the focus of protection: while data protection is centered on the various categories of personal data, with the specific information collected and processed being the reference point, privacy focuses on the person in terms of identity and the Self, providing thus a more holistic framework for assessing the impact of surveillance on the relationship between the individual and the state. While the specificity in data protection is useful in closely scrutinising various instances of data processing, such specificity may lead to fragmentation and ultimately miss the big picture as far as phenomena of profiling, discrimination and broader human rights implications of surveillance are concerned. The inherent generality in the concept of privacy[88] gives it the potential to be flexible enough and evolve in order to address parallel developments in pre-emptive surveillance.[89]

86 Case C-131/12 *Google Spain SL, Google Inc* (ECJ GC 13 May 2014).

87 P de Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 77–78.

88 DJ Solove, *Understanding Privacy* (Harvard University Press 2008) 46.

89 Mitsilegas (n 6).

Courts in Europe have now increasingly had to deal with pre-emptive surveillance measures embracing both the collection of data by the state and the collection of data by the private sector. In *Marper*[90] the European Court of Human Rights examined the compatibility with the ECHR of the systemic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued in the UK. The Court found that such blanket and indiscriminate retention of data is disproportionate and thus non-compliant with Article 8 of the Convention. The ruling is important in rejecting the *retention* of DNA data per se: according to the Court, the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[91] It is also important in highlighting the broader impact of retention on the affected individuals and in particular the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons.[92] As Vedaschi and Lubello detail in their contribution to this Special Issue, a number of constitutional courts in Europe have declared the unconstitutionality of domestic data retention legislation implementing the EU data retention Directive.[93] A common thread which can be discerned in the reasoning of constitutional courts is the emphasis on the adverse impact of breaches of privacy on the relationship between the individual and the state more broadly. By focusing on the individual and adopting a holistic approach to protection, the judiciary has begun to develop privacy into a meaningful constitutional safeguard against pre-emptive surveillance.

Following up to these potent rulings from national constitutional courts in Europe, a decisive move towards using privacy to limit pre-emptive surveillance has come from the EU Court of Justice (ECJ). In its landmark ruling in the case of *Digital Rights Ireland*,[94] the Court of Justice annulled the data retention Directive on the grounds that the EU legislature had exceeded the limits

90 *S. And Marper v. The UK* [2008] Application nos. 30562/04 and 30566/04.

91 Ibid para 121.

92 Ibid para 122.

93 See A Vedaschi and V Lubello, 'Data Retention and its Implications for the Fundamental Right to Privacy' in this Special Issue and F Fabbrini, 'Human Rights in the Digital Age, The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the US' (2015) 28(1) Harvard Human Rights Journal (forthcoming).

94 Case C-293/12 *Digital Rights Ireland* (ECJ 8 April 2014).

imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

The implications of the ruling of the Court of Justice in *Digital Rights Ireland* for the reconfiguration of the relationship between pre-emptive surveillance and privacy cannot be underestimated. Although the Court did accept that the interference of the Directive with the rights involved was legitimate, it clearly found the system of mass, blanket surveillance set out by the Directive disproportionate and in breach of the rights to private life and data protection as enshrined in the Charter. The Court's findings on the creation by the Directive of a system of generalised and unlimited surveillance based on the blanket retention of telecommunications data of everybody are particularly instructive in this context, and have been echoed on the other side of the Atlantic by the Privacy and Civil Liberties Oversight Board findings on the US NSA programme.[95] It is highly likely that similar questions will continue to reach the Court in the context of EU measures on pre-emptive surveillance. The Court's findings in *Digital Rights Ireland* made the Court decide to annul the Directive retroactively without granting an interim period of validity pending the adoption of a new EU instrument. The Court's ruling has significant implications not only in questioning the constitutionality of data retention frameworks, but also in questioning the compatibility with the Charter of the surveillance systems established and legitimised by the transatlantic PNR and TFTP agreements as well as the proposals for internal EU PNR and TFTP instruments. The Court's findings with regard to the establishment of a system of generalised and unlimited surveillance with very weak provisions with regard to access and length of retention of data are also applicable in the context of the PNR and TFTP legislation. Transfer of personal data to the US under the respective agreements would not be compatible with the Charter following *Digital Rights Ireland* in view of the very weak data protection and privacy safeguards provided by the Agreements and by US law and the system of massive, generalised surveillance consisting of the bulk transfer of everyday personal data to US authorities that the agreements entail. Following the revelations about the NSA, which have caused a strong political backlash in Europe and questions about the viability of transatlantic counter-terrorism cooperation more broadly,[96] there are efforts in the US to address privacy concerns at least as

95 Privacy and Civil Liberties Oversight Board (n 68) 57–58.

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

regards telephone data.[97] The EU and the US are in the process of negotiating an EU-US agreement on privacy.[98] The European Commission views this agreement as providing a general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism placing this within the broader framework of establishing mutual trust.[99] At the global level, the UN General Assembly has called for further work to be done on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data including on mass scale.[100] Transatlantic and global standards on privacy are welcome to the extent that they will underpin systems of pre-emptive surveillance.[101] Their development, however, should come hand in hand with revisiting the principle and content of mass surveillance systems operating globally today, including systems of surveillance of passenger, financial and telecommunications data as outlined in this article.

4 Conclusion

The post/9/11 legal landscape has witnessed a fundamental reconfiguration of the relationship between the individual and the state in the US, the EU and globally. The emphasis of governments on generalised pre-emptive surveillance has been key to this reconfiguration. Masses of personal data emanating from everyday private activities have been transferred by bulk from the private sector to state agencies, in particular in the US. Data has been collected and transferred without any specific link with the commission or suspicion of commission of a criminal offence. Pre-emptive surveillance is also based on maximum access to such data by a variety of state authorities and lengthy retention periods by state agencies. This US-led model of pre-emptive surveillance – often operating in secret- has caused controversy and concern in Europe with EU institutions being faced with calls to respond on the one hand to US security

97 C Savage, 'House Votes To Curb NSA Scrutiny of American's Communications' *New York Times* (New York, 20 June 2014).

98 For details see Mitsilegas (n 55).

99 Commission, 'Rebuilding Trust in EU-US Data Flows' (Communication) COM (2013) 846 final.

100 United Nations General Assembly Res 68/167 (13 December 2013) UN Doc A/RES/68/167.

101 See further the contribution of K Lachmayer, 'Rethinking Privacy Across Borders: Developing Transnational Rights on Data Privacy' in this Special Issue.

demands while upholding on the other hand fundamental rights as enshrined by European constitutional law. The EU legislator has attempted to reconcile these aims by the adoption of a number of transatlantic co-operation agreements on pre-emptive surveillance, aiming to ensure counter-terrorism cooperation within a framework of EU-inspired data protection. At the same time, US models of pre-emptive surveillance based on private data have been copied by EU institutions either in the form of legislative proposals or in the form of legislation as such. In developing these standards the EU legislators have backed these with a series of provisions on data protection and its enforcement. While constituting a starting point, these provisions have not proven to be sufficient to address the considerable challenge pre-emptive surveillance has posed on privacy and the relationship between the individual and the state more broadly. There is a need for a more holistic approach addressing the impact of pre-emptive surveillance on the individual as a whole, both in terms of privacy and in terms of citizenship. A broader conception of privacy can address this challenge, and such conception has been put forward in Europe not by the legislator, but by the judiciary. A number of national constitutional courts, the European Court of Human Rights and the Court of Justice have all placed limits upon generalised pre-emptive surveillance, recognising – in particular in the case of national constitutional courts- the potential 'chilling effect' that generalised surveillance may have on the individual and on society as a whole. This potential for a 'chilling effect' has also been acknowledged by the US Privacy and Civil Liberties Oversight Board in its response to the NSA telephone surveillance scandal. Courts' intervention and political pressure has led so far to the annulment of key EU law on pre-emptive surveillance (the Data Retention Directive) and to efforts to limit US law on pre-emptive surveillance. Transatlantic and global standards on privacy are also being talked about or developed. These efforts signify the return of privacy with a vengeance and a turnaround in the reconfiguration of the relationship between the individual and the state. However, efforts to legislate privacy should not come at the expense of, but should rather be accompanied with, an urgent re-examination of the necessity and legality of existing programmes of pre-emptive surveillance at both sides of the Atlantic. PNR, TFTP and national data retention schemes as they currently stand do not seem to be compliant with the fundamental rights benchmark set out by the Court of Justice in *Digital Rights Ireland*. To achieve full compliance with this benchmark, the review of current and draft EU legislation on pre-emptive surveillance is now a matter of urgency.