European Union Regulation of Transatlantic Data Transfers and Online Surveillance

Maria Tzanou*
Lecturer in Law, Keele University, UK

KEYWORDS: US mass surveillance, Snowden revelations, privacy, Safe Harbour, Articles 7, 8 and 47 Charter of Fundamental Rights of the European Union, Privacy Shield, *Schrems v Data Protection Commissioner*.

1. INTRODUCTION

In April 2014, the Court of Justice (CJEU) ruled in *Digital Rights Ireland*[1] that the mass metadata retention surveillance established in the EU by the Data Retention Directive[2] interfered disproportionately with the fundamental rights to privacy and data protection enshrined in Articles 7 and 8 of the European Union Charter of Fundamental Rights (EUCFR). The judgment was hailed as a victory of fundamental rights over surveillance in Europe.[3] In October 2015, a further major jurisprudential development occurred in the EU: following the Snowden revelations that the United States has been operating a secret mass electronic surveillance programme that grants it access to Internet data, such as email, chat, videos, photos, and file transfers held by leading Internet companies, including Facebook, Google, Microsoft, Yahoo, Skype, Apple and Youtube, the CJEU in its judgment in *Schrems*[4] invalidated the Commission's decision finding that the US ensured an adequate level of protection for the transfer of personal data under the Safe Harbour privacy principles. It did so on the basis that the US authorities were able to access the personal data transferred from EU Member States and process them beyond what was strictly necessary and proportionate to the protection of national security.

The CJEU's decision in *Schrems* is undoubtedly a significant judgment that marks another victory of fundamental rights, this time against international surveillance. *Schrems* raises a number of important legal questions, but the present article will focus on three aspects of the ruling that concern fundamental rights. Firstly, it will assess the admissibility issue concerning standing rights in secret surveillance cases in order to demonstrate the extensive scope of EU data privacy law. Secondly, it will discuss the implications of the judgment for transborder data flows and their regulation in the light of fundamental rights. Thirdly, it will focus on the challenges that the US secret mass electronic surveillance poses for fundamental rights. All of these three aspects of the *Schrems* judgment demonstrate the broad reach of EU fundamental rights law, and especially the right to privacy, which has been

* E-mail: m.tzanou@keele.ac.uk.
[1] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland ltd and Seitlinger and others* [2014] ECR I-238.
[2] 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, O.J. 2006, L 105/54.
[3] See Ojanen, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance' (2014) 10 (3) *European Constitutional Law Review* 528.
[4] Case C-362/13 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, unreported.

brought into prominence by the CJEU's recent judgments in *Digital Rights Ireland*, *Google Spain*[5] and *Schrems*.

However, two main lines of criticism will be advanced. The first concerns the fundamental rights analysis of the Court. Despite the obvious victory of fundamental rights over surveillance, the CJEU missed in *Schrems* the opportunity to discuss some crucial elements of the US online surveillance programme that further challenge EU fundamental rights. Moreover, the Court refrained from engaging with the inherent problem of today's electronic surveillance programmes in general, viz the systematic government access to private-sector data. This raises the so-called 'function-creep problem' which goes to the heart of the right to data protection, a fundamental right recognized in the EU legal order in Article 8 EUCFR alongside the right to privacy.[6] Finally, the regrettable lack of depth of the CJEU's analysis of the essence of fundamental rights will also be considered. The second line of criticism is broader and concerns the future developments for transatlantic data transfers and the safeguarding of EU citizens' fundamental rights from US online surveillance after the *Schrems* judgment.

2. LEGAL AND FACTUAL BACKGROUND

Transatlantic trade is of critical importance for the economies of both the EU and the US. A crucial aspect of this relation, which makes possible the realization of transatlantic commercial transactions, is the transatlantic flow of personal data.[7] Under the EU data protection legal framework, personal data can cross the EU's external borders only if an 'adequate' level of protection is ensured in the country of destination.[8] The EU regulation of transborder data flows has been broadly based on a centralized model according to which the EU institutions – and, in particular, the Commission - decide whether a third country ensures adequate protection. In terms of the criteria used to assess the adequacy of protection, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the 'Data Protection Directive') stipulates that all the circumstances surrounding a data transfer and more particularly the nature of the data, the purpose of the proposed processing operation and the rules of law in force in the third country in question should be taken into consideration.[9] According to the Working Document adopted by the Article 29 Working Party on the protection of individuals with regard to the

[5] Case C-131/12 *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, 13 May 2014, unreported. See McGoldrick, 'Developments in the Right to be Forgotten' (2013) 13 *Human Rights Law Review* 761 and Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 *Human Rights Law Review* 761.

[6] See Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 *International Data Privacy Law* 88.

[7] See Tourkochoriti, 'The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance' (2014) 36 (2) *University of Pennsylvania Journal of International Law* 459.

[8] Article 25 (1) Directive 95/46/EC [1995] OJ L 281/31.

[9] Article 25 (2) Directive 95/46/EC.

processing of personal data, an adequacy analysis essentially focuses on two basic elements: the content of the rules applicable and the means for ensuring their effective application. [10]

The Commission has recognized a number of countries or jurisdictions as providing adequate protection.[11] However, there has been no general adequacy finding for the US, given that it lacks comprehensive data protection legislation.[12] In order to allow for international trade, transatlantic data flows between the EU and the US were made possible through the Safe Harbour scheme.[13] Safe Harbour was based on a system of voluntary self-certification and self-assessment of US-based companies that they abide with certain data protection principles, the 'Safe Harbour principles,' combined with some intervention by the public authorities. In particular, under the scheme, US companies were required to register their self-compliance with the Safe Harbour principles with the US Department of Commerce, while the US Federal Trading Commission (FTC) was responsible for enforcing the agreement. On the basis of this, the Commission issued Decision 2000/520/EC (hereafter 'the Safe Harbour Decision') recognizing the adequacy of protection provided by the Safe Harbour principles.[14] The Safe Harbour decision served as the legal basis for transfers of personal data from the EU to US – based companies which have adhered to the Safe Harbour privacy principles. Safe Harbour proved to be an important tool of transatlantic commercial relations, with over 3200 companies signing up to the scheme. However, the Snowden revelations in 2013 that the US' National Security Agency (NSA) has been operating a secret mass electronic surveillance programme, PRISM, that grants it access to Internet data held by leading Internet companies[15] raised serious concerns about the systematic access of US law enforcement authorities to data held by these companies and transferred to the US under the Safe Harbour scheme. [16]

The *Schrems* case arose from the proceedings between Mr Maximillian Schrems, an Austrian national residing in Austria, and the Irish Data Protection Commissioner ('the Commissioner'). Mr Schrems, who had been a subscriber to the social network Facebook since 2008, lodged a complaint with the Commissioner in June 2013, by which he asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the US. Mr Schrems's complaint was based on the fact that any person

[10] 'Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive', 24 July 1998, 5.

[11] Switzerland, Canada, Andorra, Argentina, Guernsey, Isle of Man, Faroe Islands, Israel, Jersey, New Zealand and Uruguay.

[12] See Papakonstantinou and de Hert, 'The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic' (2009) 46 *Common Market Law Review* 885, 892; Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 (2) *International Data Privacy Law* 68, 70.

[13] See http://web.archive.org/web/20150910175747/http://export.gov/safeharbor/eu/eg_main_018493.asp. ? Its harbor or harbourXXXX

[14] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

[15] See Glenn Greenwald and Ewen MacAskill 'NSA Prism program taps in to user data of Apple, Google and others', *Guardian,* 7 June 2013; Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *Washington Post,* 7 June 2013.

[16] See Communication from the Commission to the European Parliament and the Council, 'Rebuilding Trust in EU-US Data Flows', 27.11.2013 COM(2013) 846 final.

residing in the EU who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is itself established in the US. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. located in the US, where it undergoes processing. In his complaint Mr Schrems referred to the revelations made by Edward Snowden concerning the activities of the US intelligence services, and in particular the PRISM programme, under which the NSA obtained access to mass data stored on servers in the United States owned or controlled by a range of companies active in the internet and technology field, such as Facebook USA. In this regard, he contended that the law and practice in force in the US did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. The Commissioner rejected Mr Schrems' complaint as 'frivolous or vexatious' on the basis that it was unsustainable in law. Mr Schrems brought an action before the Irish High Court challenging the Commissioner's decision. The High Court found that the mass and undifferentiated accessing of personal data was contrary to the principle of proportionality and the fundamental rights to privacy and to inviolability of the dwelling, protected by the Irish Constitution.[17] However, the High Court considered that this case concerned the implementation of EU law and in particular it raised the issue of the legality of the Safe Harbour regime, established by Decision 2000/520 in the light of articles 7 and 8 of the EU EUCFR.[18] In this respect, the High Court decided to stay the proceedings and refer two preliminary questions to the Court asking whether National Data Protection Authorities (NDPAs) were bound by the Commission's Safe Harbour adequacy decision or whether they could conduct their own investigation of the matter in the light of factual developments that arose after the publication of this decision.

3. THE JUDGMENT OF THE COURT

Following the Opinion of Advocate General Bot,[19] the Court discussed two issues. The first concerned the powers of NDPAs to investigate complaints concerning transfers of personal data to a third country where it is alleged that this does not guarantee an adequate level of protection despite a Commission's adequacy finding to the contrary. The second concerned the suspension of data transfers to the US under the Safe Harbour regime in light of Articles 7 and 8 EUCFR on the basis that this did not provide adequate protection.

Insofar as the powers of the NDPAs were concerned, the CJEU held that NDPAs must be able to examine, with complete independence, whether transfers of data to third countries comply with fundamental rights and the requirements of the Data Protection Directive.[20] The Court clarified how NDPAs should proceed in doing so, employing an *a fortiori Foto-Frost*[21] argument that would enable it to have the final saying in a question of

[17] *Schrems*, supra n 4 at para 30.
[18] Ibid. at para 35.
[19] Opinion of Advocate General Bot delivered on 23 September 2015 in Case C-362/13 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, unreported.
[20] Ibid. at para 57.
[21] Case 314/419, *Foto-Frost v Hauptzollamt Lübeck-Ost*, [1985] ECR 4199.

validity. According to this, following *Foto-Frost*, national courts are entitled to consider the validity of an EU act, but they do not have the power to declare such an act invalid themselves; *a fortiori*, NDPAs can examine complaints on the compatibility of a Commission's adequacy decision with fundamental rights, but they are not entitled to declare that decision invalid themselves.[22] The CJEU distinguished two potential outcomes when NDPAs are asked to examine a complaint lodged by an individual regarding the transfer of his data to third countries: if the NDPA comes to the conclusion that it is unfounded and therefore rejects it, the individual can challenge this decision before the national courts –as Mr Schrems did- and the latter must stay the proceedings and make a reference to the Court for a preliminary ruling on validity.[23] If the NDPA considers, however, that the individual's claim is well-founded, it must engage in legal proceedings before the national courts in order for them to make a reference for a preliminary ruling on the validity of the measure.[24]

On the basis of this pronouncement and in order to give the referring national court a full answer, the CJEU decided to examine the validity of the Commission's adequacy decision 2000/520.[25] Having explained that adequacy requires essentially a level of protection of personal data in third countries equivalent to the one guaranteed within the EU,[26] the CJEU went on to discuss Articles 1 and 3 of Decision 2000/520. It observed that the derogation to the Safe Harbour principles on the basis of 'national security, public interest, or law enforcement requirements' constituted an interference with the fundamental right to privacy of the persons whose personal data is transferred from the EU to the US.[27] The US legislation was 'not limited to what is strictly necessary' since it authorised, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the EU to the US without any any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use.[28] In particular, the Court found that legislation permitting generalised access to the content of electronic communications compromises the essence of the fundamental right to privacy established in Article 7 EUCFR,[29] and legislation not providing for legal remedies to individuals to access and obtain rectification or erasure of their data affects the essence of the fundamental right to effective judicial protection enshrined in Article 47 EUCFR.[30] The Court also held that Article 3 of Decision 2000/520 was problematic because it denied the NDPAs the powers granted by Article 28 of the Data Protection Directive to investigate complaints brought forward by individuals.[31] Since the invalidity of Articles 1 and 3 of Decision 2000/520 affected the validity of the decision in its

[22] *Schrems*, supra n 4 at para 62.
[23] Ibid. at para 64.
[24] Ibid. at para 65.
[25] Ibid. at para 67.
[26] Ibid. at para 73.
[27] Ibid. at paras 86-7.
[28] Ibid. at para 93.
[29] Ibid. at para 94.
[30] Ibid. at para 95.
[31] Ibid. at para 102.

entirety,[32] the Court annulled the Commission's adequacy decision regarding data transfers to the US under the Safe Harbour scheme.

4. ANALYSIS

A. Victim Status in Secret Surveillance: No 'Frivolous or Vexatious' Privacy Claims Under EU law

It is significant that there are no standing requirements for the admissibility of secret surveillance claims under EU law. Unlike the Data Protection Commissioner, who considered that there was no evidence that Mr Schrem's personal data held by Facebook had actually been accessed by the NSA and, therefore, rejected his complaint as 'frivolous or vexatious', neither the AG nor the Court raised any issue of victim status for the admissibility of complaints about secret surveillance. This is in accordance to long established CJEU case-law, pursuant to which data protection law applies irrespective of whether an individual has suffered actual damage or harm.[33]

This approach should be distinguished from the one adopted by the European Court of Human Rights (ECtHR) regarding admissibility of complaints in secret surveillance cases. The Court has repeatedly held that the Convention does not provide for an *actio popularis* and the ECtHR does not normally review the law and practice *in abstracto*.[34] Therefore, in order to be able to lodge an application an individual was required to show that he was 'directly affected' by the measure complained of.[35] The ECtHR recognized, however, that this might prove problematic in cases of secret surveillance. In *Klass v. Germany* the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him.[36] The Court explained the reasons for its approach as follows: where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, this means necessarily that the surveillance remains unchallengeable because the persons concerned are unaware of the violation.[37] According to the ECtHR, such surveillance measures could reduce Article 8 ECHR to a nullity and, therefore the Court stated that an applicant is entitled to '(claim) to be the victim of a violation of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance.'[38] Following *Klass*, however, the ECtHR followed in its case law two different approaches to victim status in secret surveillance cases. In some cases, the

[32] Ibid. at para 105.
[33] *Schrems*, supra n 4 at para 87: 'To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered *any adverse consequences* on account of that interference.' See also *Digital Rights Ireland*, supra n 1 at para 33 and Joined Cases C 465/00, C 138/01 and C 139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989 at para 75.
[34] See *N.C. v Italy* ECHR Reports 2002‑X at para 56; and *Centre for Legal Resources on behalf of Valentin Câmpeanu v Romania* ECHR Reports 2014 at para 101.
[35] Ibid.
[36] *Klass and Others v Germany*, 6 September 1978, Series A No. 28 at para 34.
[37] Ibid.
[38] Ibid. at para 38.

applicant was required to show a 'reasonable likelihood' that the security services had intercepted information concerning his private life.[39] In other cases, the Court reiterated its pronouncement in *Klass* and agreed to hear cases where a mere existence of secret surveillance laws entailed 'a threat of surveillance for all those to whom the legislation might be applied'.[40]

It should be noted that the ECtHR sought to clarify its case law in *Kennedy*[41] and further explained it and consolidated in its recent judgment in *Zakharov*.[42] According to the ECtHR secret surveillance cases will be reviewed under two conditions: first, legislation can be challenged when the applicant is considered to be 'potentially at risk' of being subjected to such measures; secondly, the Court will consider the availability of remedies at the national level and adjust the degree of scrutiny depending on the effectiveness of such remedies.[43] Where the domestic system does not afford an effective remedy to the person who suspects that he was subjected to secret surveillance, 'the menace of surveillance' can constitute an interference with Article 8 ECHR. In such instances, the ECtHR opined that there is a greater need for scrutiny by the Court and, thus, an exception to the rule, which denies individuals the right to challenge a law in *abstracto*, is justified.

Finally, it is worth mentioning that a strict standing condition for challenging surveillance measures targeting non-US nationals exists in the US since the US Supreme Court has held in *Clapper v Amnesty International*[44] that neither individuals nor organizations have standing to bring a lawsuit under Section 702 of the Foreign Intelligence Surveillance (FISA) Amendments Act (FAA) because they cannot know whether they have been subject to surveillance or not.

B. Transnational Data Transfers and 'Adequacy' of Protection: Extraterritorial Application of EU Fundamental Rights?

Global trade has brought with it an 'information explosion', where personal data is considered 'crucial raw materials of the global economy'[45]. As a result, cross-border data flows have grown massively in volume and complexity.[46] There are a number of risks associated with transborder data transfers,[47] which have prompted governments around the world to regulate them in order to protect the fundamental rights to data protection and privacy of individuals and to ensure their own 'informational sovereignty'.[48] Among the systems adopted worldwide to regulate transborder data flows, the EU's adequacy requirement under the Data Protection Directive – that will be retained and further

[39] *Esbester v the United Kingdom*, Application No. 18601/91, Commission decision of 2 April 1993.
[40] *Malone v the United Kingdom*, 2 August 1984, Series A No. 82 at para 64; and *Weber and Saravia v Germany*, Application No. 54934/00, ECHR Reports 2006-XI at para 78.
[41] *Kennedy v the United Kingdom*, Application No. 26839/05, 18 May 2010.
[42] *Zakharov v Russia*, Application No. 47143/06, 4 December 2015.
[43] Ibid.
[44] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).
[45] Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press 2013) at 1.
[46] Schwartz, 'Managing Global Data Privacy: Cross- Border Information Flows in a Networked Environment' (2009), < http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf> [last accessed 4 April 2016] at 4.
[47] Kuner, supra n 45 at 103-6.
[48] Ibid. at 28.

strengthened in the General Data Protection Regulation[49] - has been characterized as 'gunboat diplomacy'[50] that has prompted many countries to change their data protection rules – or indeed introduce new ones- in order to be able to receive data transfers from the EU.[51] Although it has been argued that the Safe Harbour scheme has levelled up US privacy protection standards,[52] the voluntary system of US companies' self-certification has revealed low levels of compliance with the basic data protection principles of the scheme[53] and several weaknesses in transparency and enforcement.[54]

The Court took the opportunity in *Schrems* to clarify the adequacy criterion. While noting that there was no definition provided in law of the concept of an adequate level of protection,[55] the CJEU observed that adequacy does not require a level of protection 'identical to that guaranteed in the EU legal order', but nevertheless protection of fundamental rights and freedoms that is 'essentially equivalent' to the one of the EU.[56] This requires an assessment of the content of the applicable domestic and international law rules in the third country as well as the practice designed to ensure compliance with those rules. The 'essentially equivalent' criterion shows that the Court is trying to bring external legal systems as close as possible to the EU's internal data protection legal framework[57] in order to ensure that domestic data protection rules are not circumvented by transfers of personal data from the EU to third countries.[58]

This means that the CJEU is taking a stricter approach to international data transfers than the one adopted 13 years earlier in *Lindqvist*.[59] In that case, which concerned a Swedish woman who set up an Internet page and loaded there personal data concerning her colleagues, the Court stated that even if such data is accessible to persons in third countries, one cannot presume that transfers of data to third countries under EU law were intended to cover situations such as where an individual loads data on an Internet page.[60] This pragmatic approach adopted by the Court seemed to be based on a consideration of the potential consequences of a contrary decision, which could 'effectively make the entire Internet subject to EU data protection law'.[61] Such an approach appears to be significantly restricted in recent

---

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 4.5.2016, L119/1.
[50] Papakonstantinou and de Hert, supra n 12 at 901.
[51] See Birnhack, 'The EU data protection directive: an engine of a global regime' (2008) 24 *Computer Law & Security Report* 508.
[52] Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' (2000) 25 *Yale Journal of International Law* 1 at 22.
[53] See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final.
[54] Ibid at 13.
[55] *Schrems*, supra n 4 at para 70.
[56] Ibid. at para 73.
[57] Peers, 'The party's over: EU data protection law after the Schrems Safe Harbour judgment', posted on 7 October 2015, available at: < http://eulawanalysis.blogspot.co.uk/2015/10/the-partys-over-eu-data-protection-law.html> [last accessed 4 April 2016].
[58] *Schrems*, supra n 4 at para 73.
[59] Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] I-12971.
[60] Ibid. at para 68.
[61] Kuner, supra n 45 at 12.

case law and replaced by a more privacy-proactive approach that brings the Internet under EU data protection law. This line of jurisprudence started in *Google Spain*[62] where the Court held that, in certain circumstances, Internet search engines are required under EU law to delist links concerning individuals from their results. Admittedly the data protection issues raised in *Schrems* are significantly different from the ones that arose in *Lindqvist*, but faced with mass surveillance the Court seems to be moving towards a more stringent approach, in accordance with its role as the constitutional court preserving the rule of law in the EU legal order.

There is a second element that differentiates *Schrems* from *Lindqvist*. Since the latter was decided, data protection has been recognized as a fundamental right in the EUCFR alongside the right to privacy. This necessarily means that transborder data flows should be regarded now as part of the EU institutions' fundamental rights protective duty.[63] In this respect, the Court stated that individuals cannot be deprived of their fundamental rights by the transfer of their data to third countries.[64] A valid argument can be made, therefore, in favour of the extraterritorial application of EU data protection standards.[65] The judgment of the Court in *Schrems* confirms this. The Court adopted a broader application of its fundamental rights law to cover data processing in the US. However, it did so in a cautious way: it dealt with the problems of the Commission's adequacy decision, rather than directly challenging the US legislation. This approach is reminiscent of the one followed in its seminal *Kadi*[66] decision: there as well the Court did not review directly the UNSC resolutions, but the EU measures implementing these.[67]

The new powers of NDPAs to investigate complaints of individuals regarding the adequacy of data protection provided in third countries, as confirmed in *Schrems,* can be seen as an additional safeguard concerning the application of these fundamental rights outside the EU's territory. Until now, only the Commission was responsible for making an assessment of adequacy; after *Schrems* NDPAs are also granted the important role of investigating individuals' complaints alleging a third country's non-compliance with EU fundamental rights, despite a Commission's adequacy decision on the matter. This means that NDPAs, alongside their current powers to oversee the application of data protection laws in the territories of their respective Member States, also have the power to review the extraterritorial application of the fundamental rights to privacy and data protection when personal data is transferred from their home country to a third country. The final decision, however, on whether a third country does not ensure adequate protection is left to the CJEU as NDPAs do not have the power to invalidate a Commission's adequacy decision, but merely to investigate complaints and -if they consider them well-founded- initiate proceedings before national courts, which must then make a preliminary reference to the

[62] *Google Spain*, supra n 5 at para 97.
[63] See Kuner, supra n 45 at 129-133.
[64] *Schrems*, supra n 4 at para 58.
[65] Taylor, 'The EU's human right obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 (4) *International Data Privacy Law* 246.
[66] C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi, Al Barakaat International Foundation v Council of the European Union*, [2008] ECR I-6351.
[67] See Scheinin, 'Is the ECJ ruling in Kadi Incompatible with International Law?' (2008) 28 *Yearbook of European Law* 637.

CJEU. The European Court, thus, retained for itself the role of the ultimate adjudicator of the adequacy of the protection of fundamental rights outside the EU.

C. US Mass Online Surveillance and Fundamental Rights

The Court also considered issues relating to mass surveillance in its landmark decision in *Digital Rights Ireland*. There the CJEU annulled the Data Retention Directive on the basis that it affected in a generalized and comprehensive manner all persons using electronic communications services in the EU.[68] While the Court's judgment in *Digital Rights Ireland* demonstrated that domestic measures of mass surveillance interfered disproportionately with fundamental rights, in *Schrems* the CJEU sent the message that mass surveillance of European citizens would not be tolerated outside the borders of the EU either. The Court's judgment is not surprising. Indeed, since the Court annulled the Data Retention Directive, which required the collection of telecommunications' metadata by service providers in order to be made available to law enforcement authorities for the purposes of fighting 'serious crime', it seemed that the US secret mass electronic surveillance would be most unlikely to survive scrutiny under EU law. In particular, the CJEU reiterated in *Schrems* that legislation authorizing on a generalised basis storage of all the personal data of all the persons whose data has been transferred from the European Union to the US without any differentiation being made in the light of the objective pursued was not limited to what is strictly necessary.

The CJEU fundamental rights' analysis in *Schrems* is different, however, from the one in *Digital Rights Ireland.* In the latter case, the Court concluded that, while the Data Retention Directive did not affect the essence of Articles 7 and 8 EUCFR, it had exceeded the limits imposed by the principle of proportionality in the light of Articles 7, 8 and 52 (1) EUCFR.[69] In *Schrems* the Court did not engage in any further analysis with regard to the principle of proportionality because it found that the essence of both the fundamental rights to privacy and to effective judicial protection under Article 47 EUCFR had been affected. There are two major reasons justifying why the US mass online surveillance programmes, such as PRISM, violate EU fundamental rights.[70] The first concerned the broad scope of PRISM, which grants access on a generalized basis not only to communications' metadata – as was the case with the Data Retention Directive - but to the actual content of electronic communications. This was deemed by the Court to breach the essence of the right to privacy. The second, a systemic one, has to do with the fact that the US legislation does not provide EU citizens with sufficient guarantees and effective legal remedies to exercise their data access, rectification and erasure rights. On the one hand, the remedies available under the Safe Harbour scheme -the private dispute resolution mechanisms and the procedures before the FTC - did not cover complaints on fundamental rights questions as they were limited to unfair or deceptive acts and practices in commerce and could not deal with the US'

[68] *Digital Rights Ireland* supra n 1 at para 58.
[69] Ibid.
[70] It should be mentioned here that the CJEU, constrained by the limits of the preliminary reference procedure, did not engage in fact-finding, but endorsed the Commission's and the AG's findings regarding the US secret surveillance measures and the lack of remedies and safeguards.

authorities access to the data held by the companies.[71] On the other hand, the US privacy regime is not as protective as the EU one and there are serious limitations regarding the rights of EU citizens to challenge surveillance measures in the US. The Fourth Amendment, which constitutes the US constitutional prohibition of unreasonable search and seizure is substantially limited by the 'reasonable expectations' doctrine and it is doubtful whether it applies to non-US persons.[72] Regarding protection from intelligence surveillance, the Foreign Intelligence Surveillance Court (the 'FISC'), which exercises supervisory jurisdiction under section 702 of the FISA does not offer remedies to EU citizens whose personal data is transferred to the US, because this applies only to US citizens and foreign citizens legally resident on a permanent basis in the United States.[73] Furthermore, the proceedings before the FISC are secret and *ex parte*.[74] This lack of legal remedies was considered by the Court to violate the essence of the fundamental right to effective judicial protection guaranteed by Article 47 EUCFR.

However, there are two further problems with US mass surveillance that the CJEU did not discuss. First, there is a total lack of transparency regarding PRISM, which operates as a secret programme at least in practice, if not in law. Starting with the legal basis of PRISM, this seems to be found in Section 702 of the FISA Amendments Act ('FAA') which allows US intelligence surveillance to seek access to information, including the content of internet communications, by targeting a non-United States person who is 'reasonably believed to be located outside the United States'. In accordance with this, the Attorney General and the Director of National Intelligence may authorize surveillance upon the issuance of an order from the FISC without showing a probable cause or any other standard to believe that the individuals are properly targeted; what is required is merely that 'a significant purpose of the acquisition is to obtain foreign intelligence information'.[75] In practice, the operation of the programme was obscured and only brought to light and made known in the EU because of the Snowden revelations. It is regrettable, therefore, that the CJEU did not even mention in *Schrems* the requirement of 'provided for by law' under Article 52 (1) EUCFR and the 'in accordance with the law' condition under Article 8 (2) ECHR on the basis of Article 52 (3) EUCFR. The ECtHR has repeatedly held in this respect that the law must be accessible to the person concerned and foreseeable as to its effects in order to satisfy this requirement.[76] While the ECtHR has accepted that 'foreseeability' in the context of secret surveillance cannot be the same as in other fields, the risks of arbitrariness of the powers vested in the executive are higher, therefore surveillance rules must be clear and detailed and citizens must be given adequate indication as to the circumstances in which

[71] *Schrems*, supra n 4 at para 89.
[72] Note by Bowden, Directorate General for Internal Policies, European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, 'The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights' (2013) at 20.
[73] Tourkochoriti supra n 7 at 487.
[74] Ibid.
[75] See Privacy and Civil Liberties Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act' ('PCLOB Report'), 2 July 2014) available at: < https://www.pclob.gov/library/702-Report.pdf> , [last accessed 4 April 2016].
[76] See among others *Rotaru v Romania*, Application No. 28341/95 ECHR Reports 2000‑V at para 52; and *S. and Marper v the United Kingdom*, Application Nos. 30562/04 and 30566/04, ECHR Reports 2008 at para 95.

public authorities can resort to such measures.[77] It seems debatable that these requirements were met under the US secret online surveillance measures, given that EU citizens became aware of them only after the Snowden revelations in the media.

There is also another problematic aspect of PRISM that the CJEU did not mention: the fact that this is inherently discriminatory on grounds of nationality. As the report presented before the European Parliament noted:

> According to the leaked 'targeting procedures' (dated 2009) of FAA known Americans [are eliminated] from being inadvertently targeted by section 702. Analysts may only proceed to access 'content data' under the 702 power if there is more than a 50% likelihood the target is not American and located outside the US, because the Fourth Amendment was held not to apply…This shows that the 'probable cause' requirement for evidence of a 50% likelihood of criminality was converted into a *50% probability of nationality*.[78]

In addition to the Court's omissions of some problematic aspects of the US surveillance programme, also notable is the absence of the fundamental right to data protection enshrined in Article 8 EUCFR from the Court's analysis of the fundamental rights with which mass electronic surveillance interferes. In particular, the CJEU referred only twice to the fundamental right to data protection in its judgment: in paragraph 72, where the Court pointed out that the adequacy requirement under Article 25 (6) of the Data Protection Directive 'implements the express obligation laid down in Article 8 (1) of the Charter to protect personal data', and in paragraph 92, where the Court repeated its pronouncement in *Digital Rights Ireland* that the protection of the fundamental right to privacy at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary. It is surprising, however, that unlike *Digital Rights Ireland*, the substantive fundamental rights' analysis of the Court in *Schrems* took place only on the basis of Articles 7 and 47 EUCFR, without any further mention of the right to data protection. It is submitted that the absence of the fundamental right to data protection from the Court's analysis is regrettable because mass electronic surveillance, based on the systematic government access to private-sector data may lead to the 'function creep' problem: data can be accessed by different bodies and further processed in order to pursue different objectives from the ones for which the data was initially collected, just because it is readily available and the relevant technology exists.[79] 'Function creep' goes against the heart of a central data protection principle, the purpose limitation principle. 'Purpose specification and limitation', which requires that personal data must be collected for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with the initial purposes,[80] embodies the values of transparency, foreseeability in data processing and

[77] See *Rotaru* supra n 69 at para 55; *Malone* supra n 37 at para 67; *Leander v Sweden*, 26 March 1987, Series A No. 116 at para 51; and *Zakharov* supra n 39 at para 229.
[78] Note by Bowden supra n 72 at 23-4. Emphasis added.
[79] Tzanou, 'The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection' (2010) 4 *Vienna Journal on International Constitutional Law* 407.
[80] Article 6 (1) (b) Directive 95/46/EC; and, Article 5 (b) Council of Europe Convention for the Protection of

accountability of data controllers in order to mitigate the inherent power asymmetries in data protection law between data subjects and data controllers and is, thus, another expression of the right to informational self-determination.[81] The systematic government access to private-sector data[82] in order to fight terrorism challenges the very essence of the purpose limitation principle. The personal data that EU citizens transferred to companies such as Facebook in order to be able to use their respective services are accessed by the US authorities in a way incompatible with the grounds on which the data was originally collected for: completely unrelated commercial purposes.[83] By not including the right to data protection in its analysis, the Court missed an opportunity to clarify whether the purpose limitation principle is 'dead' in the Internet era of mass electronic surveillance.

Finally, while it is understandable that the CJEU did not assess in detail the proportionality of US mass surveillance measures because it considered the interference to be so serious as to affect the essence of the fundamental rights to privacy and effective judicial review, the lack of depth of its analysis of the essence of fundamental rights is particularly disturbing. The Court has often held that restrictions to fundamental rights are justified when they do not impair '*the very substance* of the rights guaranteed.'[84] Nevertheless, it has been ambiguous on whether the essence of fundamental rights under Article 51 (2) EUCFR refers to the common and universal essence of a fundamental right or whether it can have a different meaning in each particular case.[85] The judgments in *Digital Rights Ireland* and *Schrems* did not shed light on this question. The line drawn between public authorities accessing the content of communications or not, which seemed to be determinant of the Court's assessment of whether the essence of the fundamental right to privacy was infringed, presents only a superficial analysis of what constitutes the essence of the fundamental right to privacy. Given that the CJEU, unlike the ECtHR, is not a specialized human rights court, it is very regrettable that it did not engage in a more thorough discussion of the essence of fundamental rights drawing inspiration from a comparative perspective[86] and from national and supranational Courts that have assessed the issue,[87] such as the ECtHR[88] and the German Constitutional Court.

Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108; adopted 28 Jan. 1981.

[81] Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 *Law and Philosophy* 559 at 576; and, Tzanou supra n 6 at 91.

[82] See Cate, Dempsey and Rubinstein, 'Systematic government access to private-sector data' (2012) 2 (4) *International Data Privacy Law* 195.

[83] See Communication from the Commission supra n 16 at 4.

[84] This pronouncement is often used with regard to the right to property. See Case 44/79 *Hauer* [1979] ECR 3727 at para 23; and Joined Cases C‑402/05 P and C‑415/05 P *Kadi* supra n 66 at para 355. Emphasis added.

[85] See Dirk Ehlers et al (eds.), *European Fundamental Rights and Freedoms* (De Gruyter 2007) at 393.

[86] See Bernhard Shima, 'EU Fundamental Rights and Member State Action After Lisbon: Putting the ECJ's Case Law in its Context' (2015) 38 (4) *Fordham International Law Journal*, 1095 at 1111.

[87] See Besselink, 'General Report. The Protection of Fundamental Rights Post-Lisbon: The Interaction Between the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and National Constitutions' (XXV FIDE Congress, Tallinn, 30 May–2 June 2012) at 47.

[88] The ECtHR case law on the right to privacy should have been taken into account all the more because the EU is legally obliged to accede to the ECHR and, pursuant to Article 52 (3) EUCFR, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the Convention and the Explanations relating to the Charter confirm that

D. What Now For Transatlantic Data Flows and Protection of EU Citizens' Fundamental Rights from US Surveillance?

The annulment of the Commission's Safe Harbour adequacy decision has important practical consequences, on the one hand, for commercial data transfers to the US and the everyday operations of Internet giants, and, on the other hand, for the access of law enforcement authorities to commercial data in order to fight terrorism. There are, therefore, two pertinent questions that need to be answered after the Court's judgment in *Schrems*. What happens to transatlantic data transfers now? And, under which conditions can the US authorities (still) access EU citizens' data held by private companies in a manner that means that they do not violate fundamental EU rights? The two questions seem inextricably linked to each other given that the CJEU invalidated the Safe Harbour scheme on the ground that US mass electronic surveillance did not respect the essence of EU fundamental rights. Yet, there might be good reasons to deal with these two issues separately.

Insofar as transatlantic data flows are concerned, the first obvious ramification of the invalidation of the Commission's adequacy decision is that Safe Harbour cannot serve anymore as a legal basis for data transfers to the US.[89] A number of possible short and longer-term solutions are available at different levels: individual-initiated, private-sector initiated, technological solutions and legislative solutions.[90] Article 26 (1) of the Data Protection Directive provides that data can be transferred to third countries even when those do not ensure an adequate level of protection, a) on the basis of the consent of the data subject; or b) when the transfer is necessary for the performance of a contract between the data subject and the controller. Individuals based in the EU could use this provision in order to continue to use the services of US-based Internet companies, such as Facebook or Google. A second set of solutions could be private-sector initiated: US undertakings collecting and processing data of EU citizens could store this data solely in Europe in order to prevent them from being accessed by US authorities. It should be recalled that this solution was adopted by SWIFT in the wake of the revelations that the US had established a secret Terrorist Financing Tracking Programme (TFTP), under which the US Department of Treasury in collaboration with the Central Intelligence Agency (CIA) collected and analysed for counter-terrorism purposes huge amounts of data from SWIFT's database. [91] Another possibility for companies comes under Article 26 (2) of the Data Protection Directive. According to this, Member States may authorize a transfer to a third country that does not ensure an adequate level of protection, 'where the controller adduces adequate safeguards' under either the so-called 'standard contractual clauses' approved by the Commission or the 'ad hoc' clauses drafted by the undertakings and approved by the relevant DPA.[92] Finally, it should be noted that

---

'Article 7 corresponds to Article 8 ECHR'. Explanations relating to the Charter of Fundamental Rights, OJ [2007] C 303/17.

[89] See Article 29 WP Statement, 16 October 2015.

[90] See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM(2015) 566 final, 6.11.2015.

[91] See Press Release, SWIFT Board approves messaging re-architecture, http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_board_approves_messaging_re_architecture/index.page.

[92] Kuner supra n 45 at 43.

technological solutions, such as the encryption of personal data originating from the EU do not seem to offer effective protection from US surveillance.

The most comprehensive solution seems to be the adoption of a new Commission adequacy decision which will provide the legal basis for data transfers to the US on the basis of a new privacy transfer scheme that will replace Safe Harbour. Adequacy can be asserted only if the new data transfer regime complies with the requirements that the Court set out in *Schrems*: no access of the US authorities to the content of the data, sufficient safeguards and effective judicial mechanisms for the data subjects, and no circumscription of the NDPAs powers.[93] On 2 February 2016, the Commission announced that a political agreement was reached on a new framework for transatlantic data flows, the EU-US Privacy Shield, which will replace the annulled Safe Harbour system.[94] On 29 February 2016, the Commission published a draft Privacy Shield adequacy decision,[95] followed by seven Annexes that include the US government's written commitments on the enforcement of the arrangement.[96] Similar to its predecessor, Privacy Shield is based on a system of self-certification by which US organisations commit to a set of privacy principles. However, unlike Safe Harbour, the draft Privacy Shield decision includes a section on the 'access and use of personal data transferred under the EU-US Privacy Shield by US public authorities'.[97] In this, the Commission concludes that 'there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the EU to the US to what is strictly necessary to achieve the legitimate objective.'[98] This conclusion is based on the assurances provided by the Office of the Director of National Intelligence (ODNI) (Annex VI), the US Department of Justice (Annex VII) and the US Secretary of State (Annex III), which describe the current limitations, oversight and opportunities for judicial redress under the US surveillance programmes. In particular, the Commission employed four main arguments arising from these letters to reach its adequacy conclusion. Firstly, US surveillance prioritizes targeted collection of personal data, while bulk collection is limited to exceptional situations where targeted collection is not possible for technical or operational reasons (this captures the

[93] See Article 29 WP Statement on the consequences of the Schrems judgment, 3 February 2016; Article 29 WP Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP237, 13 April 2016.

[94] See http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en

[95] See http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

[96] The Annexes include the following: Annex I, a letter from the International Trade Administration of the Department of Commerce, which administers the programme, describing the commitments that it has made to ensure that the Privacy Shield operates effectively; Annex II, the EU-US Privacy Shield Framework Principles; Annex III, a letter from the US Department of State and accompanying memorandum describing the State Department's commitment to establish a Privacy Shield Ombudsperson for submission of inquiries regarding the US' intelligence practices; Annex IV, a letter from the FTC describing its enforcement of the Privacy Shield; Annex V, a letter from the Department of Transportation describing its enforcement of the Privacy Shield; Annex VI, a letter prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to US national security authorities; and, Annex VII, a letter prepared by the US Department of Justice regarding safeguards and limitations on US Government access for law enforcement and public interest purposes.

[97] Draft Privacy Shield adequacy decision supra n 95 at Section 3.

[98] Ibid at para 75.

essence of the principles of necessity and proportionality, according to the Commission).[99] Secondly, US intelligence activities are subject to 'extensive oversight from within the executive branch'[100] and, to some extent, from courts such as the FISC.[101] Thirdly, three main avenues of redress are available under US law to EU data subjects depending on the complaint they want to raise: interference under FISA; unlawful, intentional access to personal data by government officials; and access to information under Freedom of Information Act (FOIA).[102] Fourthly, a new mechanism will be created under the Privacy Shield, namely the Privacy Shield Ombudsperson who will be a Senior Coordinator (at the level of Under-Secretary) in the State Department in order to guarantee that individual complaints are investigated and individuals receive independent confirmation that US laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied.[103]

Despite the plethora of privacy-friendly words ('Privacy Shield', 'robust obligations', 'clear limitations and safeguards'), one cannot be very optimistic that the new regime will fully comply with the Court's judgment. A first problematic aspect with the US assurances is that they describe the US surveillance legal framework and the relevant safeguards that already exist. The Commission observes in its draft decision that this legal framework has been 'significantly strengthened' since the 2013 Snowden revelations. This assumption is based on two legal developments: the issuance of Presidential Policy Directive 28 (PPD-28) which set out a number of principles on the collection and use of 'signal intelligence' data;[104] and the passing of the USA Freedom Act which imposed some limits on the mass collection of US persons' telecommunications metadata by US intelligence authorities.[105] Given that one can legitimately assume that the Court was aware of these developments when laying down its judgment in *Schrems* in October 2015,[106] it seems that, with the exception of the Ombudsperson, Privacy Shield does not change much in US surveillance law. In fact, the Commission has entirely based its draft adequacy analysis on a mere detailed description of this law without any further commitment that this will improve in any way in order to comply with EU fundamental rights as interpreted by the CJEU.

While the assurance that US surveillance is mainly targeted and does not take place in bulk is certainly important, there is no reference to the fact that US authorities access the content of the personal data that was deemed to violate the essence of the right to privacy in *Schrems*. Furthermore, PPD-28 allows for the bulk collection of signals intelligence data when deemed necessary 'in order to identify new or emerging threats.'[107] This information can then be used for six purposes, including counter-terrorism and other forms of serious (transnational) crimes.[108] In this respect, the 29WP observed that this purpose limitation

[99] Ibid at para 63.
[100] Ibid at para 77.
[101] Ibid at para 89.
[102] Ibid at para 95.
[103] Ibid at para 100.
[104] Presidential Policy Directive/ PPD-28 Signals Intelligence Activities, 17 January 2014.
[105] H.R. 2048, Pub. L. 114-23, 2 June 2015.
[106] It should be noted that the CJEU did not make any reference to these legal developments in *Schrems*.
[107] Draft Privacy Shield adequacy decision supra n 95 at para 59.
[108] Ibid at para 61.

appears too wide to be considered as 'targeted.'[109] Moreover, even if the US authorities engage only in targeted surveillance, the CJEU has held in *Digital Rights Ireland* that the mere retention of private-sector data for the purpose of making it available to national authorities affects Articles 7 and 8 EUCFR[110] and might have a chilling effect on the use by subscribers of platforms of communication, such as Facebook and, consequently, on their exercise of freedom of expression guaranteed by Article 11 EUCFR.[111] When faced with surveillance, individuals cannot know when they are targeted; nevertheless, the possibility of being the object of surveillance has an effect on the way they behave.[112] Insofar as Article 47 EUCFR and the right to effective judicial protection is concerned, the Commission itself notes in its draft adequacy decision that the avenues of redress provided to EU citizens do not cover all the legal bases that US intelligence authorities may use and the individuals opportunities to challenge FISA are very limited due to the strict standing requirements.[113] The recently adopted Judicial Redress Act[114] that aims to provide equal treatment of EU citizens with US citizens with regard to judicial redress avenues does not sufficiently address these concerns as it does not apply to national security and is fraught with exceptions.[115]

The creation of the Ombudsperson with the important function of ensuring individual redress and independent oversight should be welcomed as the main addition of the draft Privacy Shield. Individuals will be able to access the Privacy Shield Ombudsperson without having to demonstrate that their personal data has in fact been accessed by the US intelligence activities, and the Ombudsperson, who will be carrying out his functions independently from Instructions by the US Intelligence Community, will be able to rely on the US oversight and review mechanisms. However, there are several limitations to the function of the Privacy Shield Ombudsperson. First, the procedure for accessing the Ombudsperson is not as straightforward as lodging a complaint before NDPAs. Individuals have to submit their requests initially to the Member States' bodies competent for the oversight of national security services and, eventually, a centralized EU individual complaint handling body that will channel them to the Privacy Shield Ombudsperson if they are deemed 'complete'.[116] In terms of the outcome of the Ombudsperson's investigation, the Ombudsperson will provide a response to the submitting EU individual complaint handling body –who will then communicate with the individual- confirming (i) that the complaint has been properly investigated, and (ii) that the US law has been complied with, or, in the event of non-compliance, such non-compliance has been remedied.[117] However, the Ombudsperson

---

[109] Article 29 WP Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13 April 2016 at 38.
[110] *Digital Rights Ireland* supra n 1 at para 29.
[111] Ibid. at para 28. See also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx at para 11 [last accessed 4 April 2016].
[112] Birnstil et al, 'Privacy-preserving surveillance: an interdisciplinary approach' (2015) 5 (4) *International Data Privacy Law* 298.
[113] Draft Privacy Shield adequacy decision supra n 95 at para 99.
[114] H.R. 1428 Judicial Redress Act of 2015, 24 February 2016.
[115] Article 29 WP Opinion on the EU – U.S. Privacy Shield supra n 110 at 43.
[116] Ibid at para 102.
[117] Annex III at p. 4.

will neither confirm nor deny whether the individual has been the target of surveillance nor will the Ombudsperson confirm the specific remedy that was applied.[118] Finally, Annex III stipulates that commitments in the Ombudsperson's Memorandum will not apply to general claims that the EU-US Privacy Shield is inconsistent with EU data protection requirements.[119] In the light of the above, the Privacy Shield Ombudsperson does not seem to provide the redress guarantees of an independent supervisory authority[120] such as the NDPAs.

Draft Privacy Shield is problematic for another reason as well: it puts together the regulative framework for commercial transactions with the regulation for law enforcement access to private sector data. These are, however, different issues and they should be dealt with separately. It is important to encourage and facilitate transborder trade, thus flexible mechanisms allowing for undertakings self-compliance with data protection principles should continue to apply. But, the challenges of online surveillance on fundamental rights are too serious to be regularized[121] and covered by the same regime and some 'assurances' that essentially describe the current US law. The adoption of a transatlantic privacy and data protection framework that also ensures the transparency and accountability of transnational counter-terrorism operations could be a possible solution to this problem. Regrettably, the current Agreement negotiated between the EU and the US on the protection of personal data when transferred and processed for law enforcement purposes (the 'Umbrella' Agreement)[122] does not apply to intelligence agencies operations and raises serious concerns as to its compatibility with EU fundamental rights.[123] Thus, the best option for the moment would be the accession of the US to the Council of Europe Convention 108[124] and its Additional Protocol.[125] These contain a comprehensive framework of data protection safeguards and some enforcement mechanisms and are open to accession by non-Member States.[126]

5. CONCLUDING REMARKS

[118] Ibid.
[119] Ibid.
[120] Regarding the concerns raised about the independence of the Ombudsperson see Article 29 WP Opinion on the EU – U.S. Privacy Shield supra n 110 at 49-50; EDPS Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016 at 8.
[121] As the EDPS observes: 'whereas the 2000 Safe Harbour Decision formally treated access for national security as an exception, the attention devoted in the Privacy Shield draft decision to access, filtering and analysis by law enforcement and intelligence of personal data transferred for commercial purposes indicates that the exception may have become the rule.' Ibid. at 2.
[122] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf [last accessed 14 June 2016]. The Umbrella Agreement was initialled on 8 September 2015 and following the enactment of the Judicial Redress Act the Commission put forward on 29 April 2016 a proposal for a Council decision on its signing. The Agreement must also obtain the consent of the European Parliament.
[123] See EDPS, Opinion 1/2016, Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, 12 February 2016.
[124] Council of Europe Convention 108 supra n 80.
[125] Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8.XI.2001.
[126] Greenleaf supra n 12 at 82.

The *Schrems* judgment undoubtedly features as a constitutional decision marking the judicial protection of fundamental rights in the area of counter-terrorism. It marks a significant vindication of the right to privacy vis-à-vis modern electronic surveillance techniques and sends out a strong message that the mere availability of personal data held by private-sector companies does not justify access to them by public authorities even for the purpose of achieving important objectives such as fighting terrorism. This is a point that strongly defies the different letters of assurances received by the Commission from the US in the aftermath of the *Schrems* judgment, according to which, US authorities target only certain individuals. The mere fact that the data of potentially all EU citizens held by US Internet companies can be accessed by law enforcement and intelligence authorities is enough to trigger the application of the fundamental right to privacy and create a chilling effect on individuals' freedom of expression.

The CJEU's judgment can also been read as championing once again privacy activism following the Court's line of reasoning in its decisions in *Digital Rights Ireland* and *Google Spain*. The broad reach and interpretation of EU data protection law is evidenced, first, by the fact that, according to long established case-law there are no standing requirements for challenging secret surveillance in the EU legal order or in general alleging interference with the right to privacy. Furthermore, the strengthening of the interpretation of the 'adequacy' criterion for transborder data transfers in *Schrems* opens up the path to the application of EU privacy rights to third countries and even to the virtual borderless space of the Internet. Nevertheless, as discussed, the Court's fundamental rights' analysis has significant gaps and omissions.

Finally, it is worth pondering upon the legislative developments triggered in the aftermath of the *Schrems* judgment. The currently negotiated Privacy Shield that will replace the invalidated Safe Harbour system fails to address the CJEU's fundamental rights concerns in many respects: its fundamental rights safeguards are seriously limited and it conflates the regime for transatlantic data transfers with the need for regulation of counter-terrorism operations. Its only novelty, the creation of an Ombudsperson does not guarantee full redress for individuals. Thus, the Court may have stricken in *Schrems* another blow against online electronic surveillance in the name of fundamental rights, but the reality seems to be that little will change on the other side of the Atlantic. Should the Commission nevertheless decide to proceed with the current draft, the Court might be called in the future to examine the validity of Privacy Shield in the light of EU fundamental rights in a *Schrems* 2 case.

AKNOWLEDGEMENTS

I would like to thank the organizers of the 'Accountability for Transnational Counter-terrorism Operations' conference held at King's College London on 10-11 March 2016 and its participants for their comments on a previous version of this paper. I am also very grateful to Professor Dominic McGoldrick and David Harris for their valuable feedback. The usual disclaimers apply.