Institutionalizing personal data protection in times of institutional distrust: the Schrems Case

Loïc Azoulai, Marijn van der Sluis

Common Market Law Review **53**: 1343–1372, 2016.

CASE LAW

A. Court of Justice

Institutionalizing personal data protection in times of global institutional distrust: *Schrems*

Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, joined by *Digital Rights Ireland,* judgment of the Court of Justice (Grand Chamber) of 6 October 2015, EU:C:2015:650

1. Introduction

The case discussed here is the result of the actions of two individuals, Edward Snowden and Maximilian Schrems. In 2013, Snowden exposed several programs, run by United States (US) intelligence agencies, capable of collecting, storing, and analysing personal data of both US citizens and others on an unprecedented scale. These revelations severely shook the trust of European citizens in the online activities of governments. The outrage did not immediately lead to legal action from the EU, but the Commission did initiate a review of Safe Harbour, the Commission decision under which personal data can be transferred from the EU to the US.[1] Using the information released by Snowden, Mr Schrems, an Austrian, lodged a complaint with the Irish Data Protection Commissioner about the transfers of his personal data by Facebook Ireland ltd to the US under the Safe Harbour decision, Commission Decision 2000/520. The Commissioner felt bound to the Commission's assessment in the Safe Harbour decision on the adequacy of personal data protection in the US and rejected the complaint. The Irish High Court, to which Mr Schrems appealed, was less sure. Although it held that the Commissioner acted in accordance with the letter of Directive 95/46 on data protection and Decision 2000/520, it was highly critical of "the mass and undifferentiated accessing by State authorities of personal data" which was deemed to be contrary to the

1. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. 2000, L 215/7.

fundamental values protected by the Irish Constitution.[2] Therefore it doubted whether the current implementation of Safe Harbour can withstand scrutiny under EU law, having regard to Article 7 and Article 8 of the EU Charter of Fundamental Rights, and referred the case to the ECJ.

The fact that it was the actions of two individuals that led ultimately to the Court striking down Safe Harbour is by no means a mere curiosity of this case; it illustrates the inability or unwillingness of the institutions and public bodies to take forceful action to protect the right to personal data protection when data is transferred to third countries. At the same time, it reflects well on the EU legal system that individuals were in fact able to set in motion such a chain of events.

This judgment is about finding the appropriate institutional and legal design for protecting individuals confronted with international transfers of their personal data. The Court seems highly concerned that free online activities of European individuals are turned into forms of institutional domination. In line with the referring court, which sees in the US activities "the gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker",[3] it intends to ensure that the high level of protection guaranteed to individuals within the EU "continues where personal data is transferred to a third country".[4] The challenge confronting the Court, therefore, was twofold. It was, firstly, to find appropriate forms of institutional protection, in the circumstances that the credibility of the Commission was contested. It was, secondly, for the EU to remain a constructive player in the international arena where there are legal and political incentives to balance the requirement of individual protection with other competing interests such as free trade and international security.

2. Background

The two provisions of Directive 95/46 most relevant to this case are Articles 25 and 28. Article 25 determines the conditions under which personal data may be transferred to third countries. Article 28 regulates the tasks and responsibilities of the independent national supervisory authorities that monitor the application of the Directive in their respective Member States. The

2. Directive 95/46/EC of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31.

3. High Court of Ireland, *Maximillian Schrems* v. *Data Protection Commissioner*, judgment of 18 June 2014, [2014] IEHC 310, para 53.

4. Judgment, para 72.

Directive should of course be seen in the light of Articles 7 and 8 of the Charter.

Article 25(1) lays down the core principle: Member States may only allow the transfer of personal data to third countries if that third country ensures an adequate level of protection.[5] Notably absent from paragraph 1 is an indication of who can make a binding negative or positive assessment about the level of protection in a third country. Article 25(3) requires that Member States and the Commission inform each other where they consider that a third country does not ensure an adequate level of protection. When the Commission is of that opinion, Member States should prevent personal data transfers to that country (Art. 25(4)). At the appropriate time, the Commission should enter into negotiations with the third country (Art. 25(5)). Article 25(6) describes the opposite situation, namely when the Commission finds that a third country ensures an adequate level of protection, by reason of its domestic law or international commitments. Member States should comply with that finding.

Personal data transfers may take place to third countries that do not offer an adequate level of protection on the basis of a number of exceptions found in Article 26 of the Directive; one such exception is the unambiguous consent of the data subject. More importantly, international data transfers may take place on the basis of Model Contract Clauses (Art. 26(4)) or Binding Corporate Rules (Art. 26(2)). Model Contract Clauses, as approved by the Commission, can be used by organizations to adduce adequate safeguards for the right to privacy for transfers of data to another organization in a third country. Binding Corporate Rules can be adopted by an organization wanting to send personal data to a third country but within the organization itself. These rules must be approved by a national supervisory authority.

On 26 July 2000, the Commission adopted Decision 2000/520 establishing that the US ensures adequate personal data protection for organizations that subscribe to the Safe Harbour Principles. The adequacy decision of the Commission therefore does not establish that the US *as such* ensures an adequate level of personal data protection, but it is limited to organizations and private actors that have agreed to conform to the Safe Harbour Principles. These Principles were adopted by the US Department of Commerce and are included in Decision 2000/520. The Safe Harbour Principles follow the

5. The rules on transferring personal data to third countries should be viewed in conjunction with the rules on applicable law as contained in Art. 4 of the Directive. See further Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013), p. 128. See also Colonna, "Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?", 4 *International Data Privacy Law* (2014), at 203–221. Arts. 4 and 28 of the Directive were the subject of another case before the Court just before *Schrems:* Case C-230/14, *Weltimmo* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639.

substantive requirements of data protection as laid down in the Directive to some extent, for example concerning notification and consent, access to data by the data subject, data integrity, and data security. The Principles are expanded upon in the *Frequently Asked Questions* (FAQ's), developed by the Department of Commerce and also attached to Decision 2000/520 as annex.

The Safe Harbour Principles are based on voluntary participation. An organization participates if it has "publicly disclosed its commitment to comply with the Principles",[6] and has self-certified "its adherence to the Principles implemented in accordance with the FAQs".[7] Enforcement is organized at two levels. Firstly, organizations may join a self-regulatory privacy program that follows the Principles or they may develop their own privacy policies that adhere to the Principles.[8] Secondly, the US Federal Trade Commission (FTC) can, in accordance with its mandate of preventing unfair and deceptive acts and practices affecting commerce, investigate compliance with the Principles and, if necessary, issue fines: "the FTC takes the position that misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice".[9] In other words, whilst subscribing to the Safe Harbour Principles is voluntary, adherence to them once an organization has done so, is not.

The fact that the Safe Harbour Principles are based on a declaration by an organization in order to become effective and are not based on US law (except indirectly, for enforcement) raises the question about their effectiveness in case of counteracting legal obligations. This question is unambiguously answered in the Principles: "Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization".[10] Also a letter from the Department of Commerce concerning explicit authorizations states that: "we owe deference to the legislative prerogatives of our elected lawmakers".[11] It is therefore clear that organizations complying with legal obligations arising from US law thereby do not violate the Safe Harbour Principles, and that the US has moreover no duty to refrain from creating legal obligations that contradict these Principles.

6. Art. 1(2)(a) of Commission Decision 2000/520/EC, O.J. 2000, L 215/7.
7. Ibid., Art. 1(3).
8. Ibid., Annex I.
9. Ibid., Annex III.
10. Ibid., Annex I.
11. Ibid., Annex IV.

The number of organizations participating in Safe Harbour has steadily grown over the years, from 401 in 2003 to several thousand in 2015.[12] The actual implementation of the Safe Harbour Principles has not been an unqualified success. In a 2004 review of Safe Harbour, the Commission noted that: "a relevant number of the reviewed US organizations seem to have difficulties in correctly translating the Safe Harbour principles into their data processing policies".[13] Violations of data protection rights by the US Government were hardly an issue at the time, with one study in 2004 concluding that "[t]he controversial provisions of the USA PATRIOT Act are essentially irrelevant for SH [Safe Harbour] data flows", even though the study took note of the "broad powers" of intelligence agencies to get secret court orders for the production of business records.[14]

Those broad powers and the secrecy with which they were employed were then at the heart of the Snowden revelations, starting in June 2013. The first of many publications concerned a court order to telecom provider Verizon for "all call detail records or 'telephony metadata' created by Verizon for communications between the United States and abroad" or "wholly within the United States, including local telephone calls".[15] Further publications revealed the existence of the PRISM-program, under which several internet companies (including Facebook) provided US intelligence agencies direct access to personal data. The publications also disclosed the participation of the British intelligence agency GCHQ in some of these activities.

The Commission then sent two communications to the European Parliament and Council in November 2013. One of them was a review of Safe Harbour, the other was on "Rebuilding Trust in EU-US Data Flows".[16] The Commission found that "[l]arge-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans" and that Safe Harbour acts as a "conduit" for data transfers to companies required

12. Dhont, Asinari and Poullet, "Safe harbour implementation study" (2004), available at <ec.europa.eu/justice/data-protection/document/studies/files/safe-harbour-2004_en.pdf> (all websites last accessed 14 July 2016), 26.

13. Commission Staff Working Document of 20 Oct. 2004 on the implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC(2004)1323, at 7.

14. Dhont, Asinari and Poullet, op. cit. *supra* note 12, at 104.

15. Foreign Intelligence Surveillance Court, court order of April 2013, in Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian*, 6 June 2013, available at <www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

16. Commission Communication of 27 Nov. 2013 on rebuilding trust in EU-US data flows, COM(2013)846 final. Commission Communication of 27 Nov. 2013 on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU, COM(2013)847 final.

to give access to personal data to US intelligence agencies.[17] The conclusion was that "[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US".[18] Instead, the Commission wanted to strengthen Safe Harbour through re-negotiations with the US.

Mr Schrems had already lodged several complaints with the Irish Data Protection Commissioner (DPC) about the privacy policies of Facebook when the Snowden publications appeared. Schrems then asked the DPC to conduct further investigations, to ensure that Safe Harbour was interpreted in line with the Directive and fundamental rights, and, despite the odd nature of this latter question, to "review" the validity of Decision 2000/520.[19]

The office of the DPC is established under national legislation implementing Article 28 of Directive 95/46. An important element of the EU data protection regime is the use of independent national supervisory authorities. Their position was entrenched by the Charter, as independent supervision was introduced as an element of the right to personal data protection in Article 8(3).[20] The competences of the national supervisory authorities are outlined in Article 28(3) of the Directive and include: investigate powers, effective powers of intervention, and the power to engage in legal proceedings. National supervisory authorities moreover shall hear claims by individuals regarding their right to personal data protection (Art. 28(4)).

The DPC decided not to make use of its powers in response to the complaints by Schrems. Section 11 of the Irish Data Protection Act of 1988 prescribes that if a "Community finding" has been made concerning the adequacy of the level of protection in a third country, that finding is binding insofar as it concerns the implementation of the Act. Hence, the complaint was found to be "frivolous or vexatious" in the sense that it was unsustainable in law.[21]

Schrems appealed to the High Court. In its decision, the High Court first examined Irish law: "If this matter were entirely governed by Irish law, then, measured by these constitutional standards, a significant issue would arise as

17. Commission Communication of 27 Nov. 2013 on rebuilding trust in EU-US data flows, COM(2013)846 final, at 6.

18. Ibid., at 7.

19. It should be clear that a DPC does not have the ability to review a Commission decision. An overview of the complaints can be found at <europe-v-facebook.org>.

20. Charter of Fundamental Rights of the European Union, O.J. 2000, C 364/01 and O.J. 2010, C 83/389.

21. High Court of Ireland, *Maximillian Schrems* v. *Data Protection Commissioner,* cited *supra* note 3.

to whether the United States 'ensures an adequate level of protection …' [and] this would indeed have been a matter which the Commissioner would have been obliged further to investigate".[22] Nevertheless, it acknowledged, "that the matter is only partially governed by Irish law". Under EU law, the High Court held, the safeguards of data protection are even more explicit than under Irish law, citing Articles 7 and 8 of the Charter, as well as the recent decision in *Digital Rights Ireland*.[23] The High Court thus decided to refer the following questions to the ECJ: "Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520) having regard to Article 7 and Article 8 of [the Charter], the provisions of Article 25(6) of [the Directive] notwithstanding? Or, alternatively, may the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

3. The Opinion of Advocate General Bot

Although the Court and Advocate General Bot disagreed on a few points, they argued mostly along the same lines. Both favoured a strong role for national data protection authorities, allow for only a narrow margin of discretion in assessing adequacy, and held that "adequate" in the Directive must be interpreted as "essentially equivalent to EU standards". Most importantly, after answering the question referred, both the Advocate General and the Court assessed the validity of Decision 2000/520 and both came to a negative conclusion. Moreover, the Court referred several times directly to the Opinion of Advocate General Bot.

The first move by the Advocate General was to broaden the question. Whereas the High Court asked whether the Commissioner is "absolutely bound" by an adequacy decision of the Commission, the Advocate General saw an opportunity to clarify the tasks of both the national supervisory authorities and the Commission when faced with shortcomings in the

22. Ibid., para 56.

23. Ibid., paras. 61–62; Joined Cases C-293 & 594/12, *Digital Rights Ireland*, EU:C:2014:238.

application of Decision 2000/520.[24] The Advocate General saw two distinct parts in the obligation of the national supervisory authorities.[25] The first is to investigate and the second is to suspend data transfers, if necessary.

The authority and obligation for a national supervisory authority to investigate the adequacy of third countries with respect to the level of personal data protection is to be found in Article 28. A Commission adequacy decision based on Article 25 cannot limit the authority of a national supervisory authority to conduct an investigation. There is no indication of a hierarchical relationship between Articles 28 and 25. Moreover, there is a right to an independent authority for data protection, as enshrined in Article 8(3) of the Charter, also covering transfers of personal data to third countries; excluding transfers of data from the investigative competences of the national supervisory authorities would unduly limit that right.

If a national supervisory authority finds that a third country does not ensure an adequate level of protection, "it has the power to suspend the transfer of data in question, irrespective of the general assessment made by the Commission in its decision".[26] To be sure, adequacy decisions are binding on the Member States as is the case for all EU decisions according to Article 288 TEU. However, it follows from the scheme of Article 25, and from Article 25(3) in particular, that "the finding that a third country does or does not ensure an adequate level of protection may be made either by the Member States or by the Commission".[27] There is no exclusive power conferred on the Commission in that regard.

The Advocate General repeatedly emphasized that the Directive must be interpreted so as to achieve a high level of personal data protection. Placing personal data transfers in that context, the Advocate General saw a parallel with the Court's reasoning in *N.S.*.[28] In that decision the Court held that, concerning the transfer of asylum seekers to the Member State primarily responsible, "it must be assumed that the treatment of asylum seekers in all Member States complies with the requirements [of fundamental rights]".[29] However, this assumption is not unassailable. When a Member State cannot be unaware of systemic deficiencies in the human rights record of the other Member States that amount to "substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment",[30] it may not transfer the asylum seeker to that Member

24. Opinion of A.G. Bot in Case C-362/14, *Schrems*, EU:C:2015:627, para 5.
25. Ibid., para 51.
26. Ibid., para 81.
27. Ibid., para 86.
28. Ibid., paras. 100–105; Joined Cases C-411 & 493/10, *N.S. and Others*, EU:C:2011:865.
29. Joined Cases C-411 & 493/10, *N.S. and Others*, para 80.
30. Ibid., para 94.

State. Accordingly, the Advocate General saw an adequacy decision by the Commission as a rebuttable presumption.[31] In case of systemic deficiencies in personal data protection in a third country, a Member State must intervene to safeguard fundamental rights. Decision 2000/520 already contains a safety valve in Article 3(1)(b), but the conditions imposed therein strictly circumscribe the powers of the national supervisory authorities and thus cannot be interpreted as preventing the supervisory authorities from exercising their competences as found in Article 28(3) of the Directive.[32]

The Advocate General then embarked on an assessment of the validity of Decision 2000/520. He noted that although the validity was not directly questioned before the High Court, it should nonetheless be examined, as it is clear that it is at the heart of the case.[33] However two procedural aspects must be clarified. Firstly, the examination must necessarily be limited, as not all aspects of the Safe Harbour scheme have been discussed in the present proceedings. Secondly, the Advocate General argued that although generally the legality of a measure must be assessed in light of the facts when the measure was adopted, that approach cannot be applied to adequacy decisions, as they concern the ongoing obligation to protect fundamental rights.[34]

Given the importance of the phrase "an adequate level of protection", especially for future cases, it is surprising that the Advocate General spent little time on its meaning. Of primary importance for the Advocate General was that the interpretation must take account of the role of personal data protection with regard to the fundamental right to privacy.[35] According to the Advocate General, the objective of Article 25 is thus "to ensure the continuity of the protection afforded by that directive where personal data is transferred to a third country".[36] Therefore, "an adequate level of protection" must mean here "essentially equivalent to that afforded by the Directive".[37]

The Advocate General began the assessment of Decision 2000/520 with two findings of fact, as made by the High Court and supported by the Commission itself. First, US intelligence agencies are capable of accessing personal data transferred to the US and, second, EU citizens have no effective

31. Opinion, para 104.
32. Ibid., para 114.
33. This argument is not entirely convincing. When Digital Rights Ireland requested to join the proceedings as an *amicus curiae*, it also urged that questions on the validity of the Directive and Safe Harbour decisions be added to the reference for a preliminary ruling. Justice Hogan refused on the ground that "the addition of these questions would radically change the nature of the proceedings". See High Court of Ireland, *Maximilian Schrems* v. *Data Protection Commissioner*, judgment of 16 July 2014, [2014] IEHC 351, para 38.
34. Opinion, paras. 131–138.
35. Ibid., para 140.
36. Ibid., para 139.
37. Ibid., para 141.

right to be heard on this matter.[38] This demonstrates that the Decision does not contain sufficient guarantees.[39] It follows that the fundamental rights protected by Articles 7, 8 and 47 of the Charter are interfered with.[40]

The Advocate General first considered that the derogations found in the Safe Harbour Principles are formulated too broadly and therefore cannot be held to pursue an objective of general interest, except for the derogation regarding national security.[41] The proportionality test with regard to this objective starts by repeating the finding in *Digital Rights Ireland* that the review of discretion in case of a serious interference with the right to personal data protection must be strict.[42] The Advocate General then found it extremely doubtful that the interferences respect the essence of Articles 7 and 8 of the Charter,[43] and concluded that the "mass, indiscriminate surveillance" by US intelligence services is "inherently disproportionate".[44] Regarding effective oversight by an independent authority, the Advocate General observed that the jurisdiction of the FTC is limited to commercial activities and that moreover no supervisory authority is authorized to monitor possible breaches by US intelligence agencies.[45] For a multitude of reasons, the Advocate General therefore advised the Court to declare the Safe Harbour decision invalid.

4. Judgment of the Court

The first notable point of the Court's judgment came before any question of law was discussed: in the overview of the "legal context" the Court included lengthy references to the 2013 Communications from the Commission to the European Parliament and Council that outline the failures of Safe Harbour and the Commission strategy in remedying those failures. This foreshadows the conclusions of the judgment.

Just like the Advocate General, the Court did not limit its answer to whether national supervisory authorities are absolutely bound by a Commission decision. Instead, it expounded the responsibilities of those authorities when they receive a complaint from an individual concerning the adequacy of the level of personal data protection offered by a third country.

38. Ibid., para 154.
39. Ibid., para 159.
40. Ibid., para 174.
41. Ibid., paras. 181–184.
42. Ibid., paras. 189–190.
43. Ibid., para 177.
44. Ibid., para 200.
45. Ibid., paras. 204–207.

Most importantly, the Court stated that it is the task of national supervisory authorities to examine with all due diligence claims from individuals regarding the processing of their data in a third country that is the subject of a Commission adequacy decision.[46] The Court reached this conclusion after it emphasized the primary importance of independent oversight for the protection of the right to personal data. On earlier occasions, the Court mentioned, it was explained that the independence of these national supervisory authorities serves the effectiveness and reliability of the monitoring of data protection rules.

The Court also observed that neither Article 28(3) of the Directive, nor Article 8(3) of the Charter exclude international data transfers from their scope of action.[47] Although the national supervisory authorities only supervise the application of the provisions of the Directive on their national territory, the transfer of data itself can be considered to be a form of processing occurring on a Member State's territory and therefore falls under the preview of the national supervisory authorities.[48]

More specifically relating to the relationship between Articles 28 and 25, the Court clarified its statement in *Lindqvist* that Article 25 is part of a "special regime".[49] The Court specified that Article 25 is complementary to the general rules on personal data protection. The implication is that it is not a special regime in relation to Article 28. It is therefore on the basis of Article 28 of the Directive and Article 8 of the Charter that national supervisory authorities must examine claims from individuals regarding international data transfers to countries subject to an adequacy decision.[50] Another interpretation would contradict the right, as guaranteed by Article 8(1) and (3) of the Charter, "to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights".[51] Moreover, Article 25 itself assigns the responsibility to certify the adequacy of the level of protection in third countries both to the Member State and the Commission.

The duty for national supervisory authorities to examine claims from individuals does not translate into a power to repudiate Commission adequacy decisions. Here, the Court trod the well-beaten paths of EU law. In order to guarantee legal certainty and the uniform application of EU law, national courts and national supervisory authorities may not invalidate EU acts. Instead, if a national supervisory authority is of the opinion that the claim of an individual is well founded, it must present that opinion before a national court,

46. Judgment, paras. 47 and 63.
47. Ibid., para 54.
48. Ibid., paras. 44–45.
49. Case C-101/01, *Lindqvist*, EU:C:2003:596, para 63.
50. Judgment, para 47.
51. Ibid., para 58.

as Article 28(3) of the Directive specifically provides that national supervisory authorities must be able to engage in legal proceedings. A national court must, if it shares the doubts of the national supervisory authority on the protection of fundamental rights, then refer the matter to the ECJ for a preliminary ruling.[52] If a national supervisory authority holds that a claim is unfounded, the claimant may seek judicial redress before a national court, which may then refer the matter to the ECJ.[53]

Following the reasoning of the Advocate General, the Court also assessed the validity of Decision 2000/520, likewise taking into account facts that arose after its adoption.[54] The Court also took "an adequate level of protection" to mean "essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in light of the Charter",[55] later rephrased as "essentially equivalent to that guaranteed in the EU legal order".[56] Otherwise, the high level of protection offered by the Directive and the Charter could easily be circumvented. The Court added to this that the discretion of the Commission is reduced here because of the important role of data protection for the respect to private life and the large amounts of personal data concerned. Judicial review of the requirements of Article 25 should be strict.[57]

The Court repeatedly emphasized that the adequacy assessment by the Commission must be based on the domestic laws and international commitments of the third country involved, as prescribed by Article 25(6).[58] It is therefore not surprising that the Court concluded that Decision 2000/520 does not contain sufficient observations or conclusions on how the domestic laws and international commitments of the US help secure an adequate level of protection.[59] More specifically, the broadly formulated derogations found in the Decision allow for interference with the fundamental rights of those whose data is transferred to the US, but no finding is made in the Decision with regard to any rules adopted in the US to limit those interferences.[60] Regarding the system of self-certification under Safe Harbour the Court found that it "is not in itself contrary" to Article 25 of the Directive.[61] However, such a system relies on effective mechanisms of detection and supervision.

52. Ibid., para 65.
53. Ibid., para 64.
54. Ibid., paras. 67 and 77.
55. Ibid., para 73.
56. Ibid., para 96.
57. Ibid., para 78.
58. Ibid., paras. 69, 71, 73, 75 and 81.
59. Ibid., paras. 83, 96 and 97.
60. Ibid., paras. 87–88.
61. Ibid., para 81.

Following the Advocate General, the Court highlighted two aspects of the Commission's findings from 2013: first, that US authorities were able to access transferred personal data and process it beyond what was strictly necessary and proportionate and, second, that data subjects had no means of administrative or judicial redress in order to gain access to personal data.[62] Concerning the first point, the Court reiterated its findings from *Digital Rights Ireland*. In the EU, the Court stated, interferences with Articles 7 and 8 of the Charter require precise rules and minimum safeguards, so that individuals have sufficient guarantees against the risk of abuse of their data. In particular, legislation allowing generalized access to the *content* of electronic communication strikes at the essence of Article 7 of the Charter.[63] On the second point, the Court found that the lack of legislation providing for legal remedies for individuals to access their personal data, or to obtain rectification or erasure of personal data violates the essence of Article 47 of the Charter.

The Court concluded with a review of Article 3 of Decision 2000/520. It read this provision as going beyond the implementing powers of the Commission, because it limits the powers of the national supervisory authorities as found in Article 28 of the Directive.[64] In combination with the problems affecting Article 1 of the Decision, the Court declared the Decision to be invalid in its entirety.

5. Comments

The configuration of the *Schrems* case is unique. In cases such as *Huber, Schecke* or *Digital Rights*, the Court was confronted with disputes between individuals and public authorities and these were resolved through enhanced judicial control over public authorities.[65] Cases such as *Promusicae* or *Google Spain* involved disputes between individuals and private corporations, and these were resolved through balancing between conflicting rights and enhanced responsibility of the private data controller.[66] All of these cases were framed as issues of individual protection in a digital world dominated by public or private corporate players. In *Schrems*, the complaint lodged before the Irish Commissioner concerned the behaviour of Facebook and the

62. Ibid., para 90.
63. Ibid., para 94.
64. Ibid., para 102.
65. Case C-524/06, *Heinz Huber* v. *Bundesrepublik Deutschland*, EU:C:2008:724; Joined Cases C-92 & 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, EU:C:2010:662; Joined Cases C-293 & 594/12, *Digital Rights Ireland*.
66. Case C-275/06, *Promusicae*, EU:C:2008:54; Case C-131/12, *Google Spain* v. *AEPD and Costeja Gonzalez*, EU:C:2014:317.

surveillance activities that were engaged by the US public authorities. However, as framed by the High Court and then the ECJ, the dispute is about the adequacy decision of the Commission concerning the transfer of data from the Union to the United States and the institutional implications for the office of the national supervisory authority. The case thus places the individual in opposition to the public authorities *and* private corporations.

There are two main aspects in this case. Firstly, what is at stake is institutional competition within the European Union where the two players – the Commission and the national supervisory authorities – in the field are both independent institutions responsible for the protection of European individuals and their privacy. There were two possible options: one was to subordinate the national player to the supranational one, so as to ensure consistency and uniformity in supervision of international data transfers from Europe; the other option was to disconnect one from the other, so as to expand the venues through which scrutiny of international data transfers may be obtained. The latter was the option chosen by the Court. In contrast with a traditional bias towards centralization, this judgment gives rise to an institutional configuration empowering national supervisory authorities. It reflects a form of institutional trust shifting (5.1 below). Secondly, the case is about the position of the EU as a big player in the field of protection of personal data in a global context. Again there were two possible options: one was to accommodate the EU system of protection to the conflicting interests pursued by trade partners such as the US; the other was to accord precedence to the higher level of data protection enshrined in EU law. The Court opted for the latter. After the *Kadi* judgment, *Schrems* sounds like a further declaration of independence of protective Europe, this time in the digital field (5.2). These two choices are then seen in the light of related developments on data protection (5.3).

5.1. *A shift in institutional trust*

Of the institutional actors involved in this clash between counter-majoritarian institutions, the Commission is the apparent loser. The role of national supervisory authorities is strengthened although in a rather ambiguous way. For them, the judgment will mean a considerable addition to their workload. Two other independent institutions take on greater responsibility for the supervision of international data transfers: the national courts and the ECJ.

The most important innovation of the judgment is the explicit role awarded to national supervisory authorities in examining whether a Commission adequacy decision conforms with the Directive. Previously, national supervisory authorities were only indirectly involved in such adequacy

decisions, viz. through their so-called Article 29 Working Group, composed of representatives of all the national supervisory authorities, of the European Data Protection Authority and of the Commission. The Working Group submits an opinion to the Commission on the level of protection in third countries (Art. 30 Directive). This expansion of the role of national supervisory authorities is mainly the result of the Court's interpretation of Article 8(3) of the Charter as given shape in the Directive by Article 28.[67] The fact that Article 28 is construed as a provision directly implementing a requirement of the Charter, whereas Article 25 does not, appears to be the main motivation behind the Court's reasoning on the relation between these Articles. As a result, the Court relies on Article 28 so as to empower national supervisory authorities in the realm covered by Article 25, i.e. transfers of data to third countries. In line with its own case law, the Court favours a view of data protection authorities as fundamental rights supervisors over their role as economic regulators concerned only with the well-functioning of the market.[68]

On the one hand, the Court remains true to the spirit of the Directive. The EU legislature clearly opted for a decentralized model of governance by vesting data protection authorities at the national level.[69] On the other hand, however, it departs from the spirit of the classic EU decentralization model that sets strict supranational limits to national authorities' operation with the aim of ensuring the effectiveness of EU policy objectives and enhancing consistency across Member States. Competition policy is a case in point.[70] Article 16 of Regulation 1/2003 provides that when national actors rule on agreements which are already the subject of a Commission decision, they cannot take decisions running counter to the decision adopted by the Commission.[71] True, this is in the framework of an exclusive competence conferred on the Union and it concerns a specific decision on a given

67. In para 58, the Court makes the curious step of interpreting Art. 8(3) of the Charter as meaning that an individual has the right to lodge a complaint with a *national* supervisory authority. This would imply that the current form of monitoring of the right to personal data protection being mainly in the hands of the national supervisory authorities may not be changed for a completely centralized form of supervision.

68. Szydło, "Principles underlying independence of national data protection authorities: *Commission* v. *Austria*", 50 CML Rev. (2013), at 1816.

69. For the broader effects of decentralization for privacy protection, see Petkova, "The safeguards of privacy federalism", 20 *Lewis & Clark Law Review* (forthcoming 2016), 593–643.

70. Wilks, "Agency escape: Decentralization or dominance of the European Commission in the modernization of competition policy?", 18 *Governance* (2005), 431–452, at 431.

71. Monti, "Legislative and executive competences in competition law" in Azoulai (Ed.), *The Question of Competence in the European Union* (OUP, 2014), p. 117. This may be different in the context of leniency programmes where more leeway is granted to national authorities, see Case C-428/14, *DHL* v. *AGCM*, EU:C:2016:27.

agreement. Data protection is a field of shared competence and the Commission decision covers a broad set of practices in a foreign territory. Yet, in other areas where independent national authorities are set up to ensure the establishment of the internal market in field of electronic communications, the creation of a level playing field is ensured through a supervising power granted to the Commission.[72] Moreover, this judgment stands in sharp contrast with the development of new arrangements in the fields of economic governance and financial regulation. In these fields, a move towards more centralized intervention enhancing the powers of the Commission and EU authorities is taking place.[73]

What is striking in this case is not that that the Court considers that the activities of data protection authorities are entirely concerned with the requirement of protection of fundamental rights, but the fact that their independence is directed against any supranational influence or guidance. The notion of independence of national supervisory authorities has not been uncontroversial, with the Commission challenging the implementation of Article 28(1) of Directive 95/46 in several Member States.[74] The Commission, followed by the ECJ, defended a broad understanding of the notion of "complete independence" which not only requires a strict separation from private market parties but also prohibits any direct or indirect influence from the government and other public authorities. In *Commission* v. *Germany*, the Court observed that the purpose of the independence was "to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim".[75] In *Schrems*, this extends to independence from EU institutions and in particular the one presented as the most trustable one for national authorities and the most protective one for individuals, the European Commission.

It may be that the model that comes closest to the one designed by the Court in this case is that of national courts vested with an EU mandate. Just as national courts may be empowered on the basis of Article 47 of the Charter, national supervisory authorities are directly vested through Article 8(3) of the

72. See e.g. Art. 7 of Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), O.J. 2002, L 108/33.

73. Chiti, "In the aftermath of the crisis: The EU administrative system between impediments and momentum", *EUI Department of Law Working Paper No. 2015/13* (2015).

74. Case C-518/07, *Commission* v. *Germany,* EU:C:2010:125; Case C-614/10, *Commission* v. *Austria*, EU:C:2012:631; Case C-288/12, *Commission* v. *Hungary*, EU:C:2014:237.

75. Case C-518/07, *Commission* v. *Germany*, para 25.

Charter construed as a power-conferring norm.[76] This connection between institutional power, complete independence and protection of individuals with regard to the processing of personal data stems from the Court's own case law. However, this way of matching the objective of protection of individuals with a specific institutional arrangement has a twofold negative consequence. First, it obscures the fact that the supervisory authorities are not just concerned with the protection of data subjects; rather, presumably, their task is to "ensure a fair balance between, on the one hand, observance of the fundamental rights to private life and, on the other hand, the interests requiring free movement of personal data".[77] Second and conversely, the Commission is presented as the holder of these interests requiring free movement of personal data not particularly bothered by the protection of fundamental rights.

The Court's apparent distrust towards the Commission is not without merit. The negotiations on Safe Harbour were conducted as trade negotiations.[78] Moreover, two years after the start of the re-negotiations of Safe Harbour the Commission had not (yet) secured the necessary guarantees for an adequate level of personal data protection. The assessment from 2013 that although the current safeguards of the Safe Harbour decision were inadequate, withdrawing the decision would adversely affect business interests clearly showed the lopsided priorities of the Commission. In this instance, the Commission is regarded by the Court as a political body and not as technical body responsible for the oversight of Union law. Had the Court trusted the Commission in sticking to its traditional role as a guardian of the rule of law, the Court might have invalidated its adequacy decision whilst keeping the national authorities fully subordinate to the Commission. Instead, it decided to rely on supervisory authorities as trustees in the field of data protection. This trust appears mainly to derive from a theoretical analysis of the position of these national supervisory authorities (independence combined with significant powers), rather than from any empirical observations of their actual capacities.

Note, however, that the Court applies its reasoning only insofar as it concerns the right to lodge a complaint with a national supervisory authority (Art. 28(4)), the subsequent duty to examine that claim with all due diligence

76. On the connection between the requirement of effective judicial protection and the empowerment of national courts, see Case C-432/05, *Unibet*, EU:C:2007:163; Joined Cases C-317-320/08, *Alassini and Others*, EU:C:2010:146; Case C-93/12, *ET Agrokonsulting-04-Velko Stoyanov,* EU:C:2013:432.

77. Case C-518/07, *Commission* v. *German*, para 24; Case C-288/12, *Commission* v. *Hungary*, para 51; judgment, para 42.

78. Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishing, 2005), Ch. 4: "Keeping privacy advocates out of the loop: Negotiating the Safe Harbor Agreement".

and the competence to engage in legal proceeding (Art. 28(3)). Yet, Article 28(3) also expressly awards the national supervisory authorities "effective powers of intervention" including "imposing a temporary or definitive ban on processing". This is where the Advocate General and the Court diverge. The Advocate General recognizes a power of the national authorities to suspend data transfers on their own. The Court is more prudent. Supervisory authorities should not be prevented "from *examining* the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country". Here, the Court obviously allows a restriction on the powers of the national supervisory authorities on the basis of an adequacy decision. It is clear that if one does consider that Articles 25 and 28 regulate more or less the same subject matter, and thus that a Commission adequacy decision is binding on all Member State organs, a compromise has to be constructed. The compromise consists in keeping Article 28(4) applicable (the fair processing of claims), whilst disregarding a part of Article 28(3) (the powers of intervention). It ensures that national supervisory authorities are involved in the process, yet maintains that any serious issue with a Commission decision may effectively be solved at the EU level through a request for a preliminary reference.

This also leads to the main critique on the solution proposed by the Advocate General. Granting all the 28 national supervisory authorities the ability to effectively review personal data protection laws and practices in third countries does not lead to a proper European solution and would thus create a fragmentation in the level of protection. Also, it must be doubted whether the analogous application of the exception found in *N.S.* is appropriate here. The exception to the general application of EU law becomes relevant where EU law has already failed to accomplish an appropriate standard of protection. In *Schrems*, the question whether an appropriate level of protection is guaranteed was still open, or in any case not settled at EU level. Lastly, it must be noted that the differences are rather small between the requirements for the application of the exception found in *N.S.* and the requirements for the application of the exception as found in Article 3(1)(b) of Decision 2000/520, raising the question why it was necessary to create another exception.

That the Court focuses on the right to lodge a complaint and the power to engage in legal proceedings, whilst setting aside the power to intervene, raises questions concerning the overall position of these authorities. The Court mentions several times that the supervisory authority must examine a complaint concerning data transfers to a third country that allegedly does not ensure an adequate level of protection, as based on Article 28(4) of the

Directive. To this is added that the claim must be examined with all due diligence.[79] In this part of the argument, the Court does not mention the broad investigative powers found in Article 28(3) of the Directive. This interpretation seems to conflict with the assessment of validity of Article 3 of Decision 2000/520. The Court states that Article 3, which outlines the exceptional circumstances under which a national supervisory authority may suspend data flows to an organization participating in Safe Harbour, must be understood as unduly restricting the powers of the national supervisory authorities. Article 3 of Decision 2000/520 thus awards the supervisory authorities with a power (no matter how limited), that the Court itself has denied to these authorities in the previous part of the judgment. It is then difficult to see how this provision limits the powers of the national supervisory authorities as described in the Directive. It is true that Article 3(1) of Decision 2000/520 was meant as the only action to be undertaken by national supervisory authorities, and that the Court has greatly expanded the scope of action of these authorities. By striking down Article 3, the Court thus appears to want to reinforce its message on the role of those authorities, rather than limit the discretion of the Commission to include narrowly tailored exceptions in an adequacy decision.

That the Court does not mention the investigative powers of the supervisory authorities raises the second question, namely that of the relation of these authorities with the judiciary. The institutional framework created by the Court awards a strong role to national courts. Even though the emphasis of the judgment is on the tasks of national supervisory authorities, the role of the national courts is in a way even more important, as a positive opinion of a supervisory authority on the transfer of data as supported by a Commission adequacy decision can be challenged before the national courts. National courts and the preliminary reference procedure become the primary route to challenge the legality of a Union legal measure. What is not obvious from the Court's interpretation concerns a case where the national authority considers that the individual claim is well founded. According to Article 28(3) of the Directive, national data protection authorities are the primary institutions that engage with possible infringements of data protection rules. However, as noted by both the High Court and the Advocate General, Schrems's complaints in this case did not really concern the behaviour of Facebook, but the adequacy decision of the Commission. An organization transferring personal data to a third country is thus an unlikely opponent for a national

79. The requirement to examine the claim with all due diligence is reminiscent of the regime concerning the position of complaints in EU State aid law, where a compromise is to be found between the wide margin of discretion accorded the Commission and the protection of the complainants.

supervisory authority. In that case, what legal question or what conflict should be brought before the national court? If a national supervisory authority finds fault with an adequacy decision, against whom should it then initiate legal proceedings? When the Court leaves open the question what exactly the legal conflict before the national courts will be in case a supervisory authority wants to challenge an adequacy decision, this also opens up the possibility that individuals might circumvent the national supervisory authorities and appeal directly to a national court, challenging the behaviour of an organization as a proxy.

That the ECJ is the final arbiter on the validity of adequacy decisions should not come as a surprise. What matters is the procedure by which the case arrives at the Court. What is surprising in that regard is that the national supervisory authorities and the national court can bring a case to the ECJ without first coordinating with the Commission. This is problematic for three reasons. Firstly, it ignores without good reason Article 25(3) of the Directive, laying down a requirement of mutual information for the Commission and Member States about third countries' level of protection of personal data. Secondly, it deprives the Commission of an opportunity to use the internal pressure for a higher level of protection for a strengthened external negotiating position *vis-à-vis* third countries. Juxtaposing the somewhat more business-friendly Commission with presumably more fundamental rights oriented national supervisory authorities at the EU level can enhance the credibility of the Commission when it comes to convincing third countries about the value attached in Europe to personal data protection. Article 25(5) of the Directive also hints at such a strategic interaction.[80] Finally, it offers a picture of a fragmented institutional landscape, setting apart the trustable and non-trustable institutions. Instead, what are most needed are clear criteria to apprehend transfers of data applicable to all institutions acting in the field.

5.2. *A declaration of independence of digital Europe*

In 1996, John Perry Barlow famously published the *Declaration of the Independence of Cyberspace*.[81] The point of it was to release the global digital

80. The A.G. found that "the purpose of the negotiations entered into with a third country [under Art. 25(5) of the Directive] is to remedy the absence of an adequate level of protection found in accordance with the procedure laid down in Art. 31(2) of that directive". By viewing the purpose of Art. 25(5) of the Directive in such black-and-white terms, the A.G. also misses an opportunity to consider the strategic opportunities for international negotiations; see Opinion, paras. 232–234.

81. Barlow, "A declaration of the independence of cyberspace", 8 Feb. 1996, available at: <www.eff.org/cyberspace-independence>.

community from any public regulation or intrusion.[82] It soon became clear that this declaration underestimated the phenomena of digital commodification and institutional domination. *Schrems* may be seen as a response to the risk that free online activities are turned into operations of mass third State surveillance of European citizens. This is reflected in the assessment of the validity of Decision 2000/520.

The Court had to reflect on the meaning of the notion "an adequate level of protection". This notion is at the heart of Article 25, but not described in more detail. Article 25(2) describes how to measure adequacy, but does not provide any clues as to the standard against which to measure. Citing fears of circumvention, the ECJ found that "adequate" must mean a level of protection essentially equivalent to that guaranteed by Directive 95/46 (as seen in the light of the Charter). EU citizens are thus offered a consistent area of data protection both within and outside the Union.[83]

The requirement of essentially equivalent protection is not unknown in Europe. It comes very close to the *Solange* approach adopted by the German *Bundesverfassungsgericht* in its ruling of 29 May 1974 when it had to consider the level of protection of fundamental rights available at the Community level. A level of protection identical to that guaranteed in the German constitutional order is not required, but Germany is allowed to be a member of the Community "as long as" the European Economic Community provides for an "essentially comparable" standard of protection.[84] It was also the approach suggested by Advocate General Maduro in his Opinion in *Kadi*.[85] However, there are two ways of implementing a *Solange* approach: either by requiring the conflicting system to make improvements to align with its own standards of protection, leaving it a probationary time period, or by requiring immediate adherence to standards equivalent to those guaranteed at home.[86] In this case, the Court decided to make the transfer of personal data to the US dependent on strict and immediate adherence to EU standards. This is also shown by its decision not to mitigate the temporal effects of its annulment judgment.

82. Lindahl, "We and cyberlaw: The spatial unity of constitutional orders", 20 *Indiana Journal of Global Legal Studies* (2013), 697–730, at 703–708.

83. For the construction of this area within the EU, see Case C-524/06, *Huber*.

84. Mayer, "The force awakens: The *Schrems* case from a German perspective", 16 Oct. 2015, available at <verfassungsblog.de/the-force-awakens-the-schrems-case-from-a-germ an-perspective-2/>.

85. Opinion of A.G. Poiares Maduro in Joined Cases C-402 & 415/05 P, *Kadi and Al Barakaat,* EU:C:2008:11.

86. On the first option, see Kuner, "The sinking of the Safe Harbor", 8 Oct. 2015, available at <verfassungsblog.de/the-sinking-of-the-safe-harbor-2>.

This part of the judgment raises three issues. First of all, it may be questioned whether it is appropriate to use the level of protection offered by the Directive as a point of comparison, considering the restrictions on the scope of application of the Directive. Article 3(2) of the Directive provides that "this Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law". The Directive sets no standards of protection concerning these processing operations. By extension, the level of protection as offered by that Directive cannot provide a yardstick when it concerns the processing in third countries for the purposes of public security, defence, criminal justice and law enforcement area.[87] This was clearly pointed out by the Court in the *PNR* case concerning the validity of the Commission Decision 2004/535/EC 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.[88] Since it concerned public security and the activities of a third State in areas of criminal law, the adoption of the Commission decision was considered to be *ultra vires*.

In fact, the Court implicitly assumes that the processing of personal data taking place in the context of the relationship between Schrems and Facebook Ireland was commercial in nature, disconnecting it from the broader context in which the data are made accessible to US national security agencies. It assumes that the adequacy decision concerns processing of data as referred to in Article 3(1) of the Directive. As a result, the Court never asks whether the measures as adopted in the US would on this side of the Atlantic fall within the scope of the Directive or not. The test of "essentially equivalent" is used in a rather loose manner, as the Court and the Advocate General fail to answer this question: essentially equivalent to what exactly? Perhaps as a way to solve the problem, the Court refers at a certain point to the broader level of protection

87. But see the recently adopted Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J. 2016, L 119/89 and Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, O.J. 2016, L 119/132. See further De Hert, "The new police and criminal justice Data Protection Directive: A first analysis", 7 *New Journal of European Criminal Law* (2016), 7–19.

88. Joined Cases C-317 & 318/04, *Parliament* v. *Council* (*PNR)*, EU:C:2006:346, paras. 54–61.

offered "in the EU legal order". It is true that the EU is becoming more active on (public) security, especially with the adoption of the new Directive 2016/680 on the processing of personal data for criminal justice purposes; yet in this area the division of competences between the EU and Member States remains unsettled.[89] On many topics of counter-terrorism, defence, and security the EU legal order does not offer clear points of comparison. In this case, the Court demands from third countries what it may not be in a position to demand from the Member States.[90] It must be remembered that the Snowden revelations also uncovered involvement of UK intelligence services in mass surveillance. Mass surveillance is not exclusively an American practice.

This leads to the second issue, namely the role played by security in the assessment of the validity of the adequacy decision. As the Court itself observes, the right to personal data protection has to be balanced with the value of free movement of data.[91] However, no mention is made of the balance that must be struck between data protection and security concerns. The mere fact that, in the adequacy decision, "national security, public interest, or law enforcement requirements" have general and absolute primacy over the safe harbour principles means that the decision enables illegitimate interference with the fundamental rights of data subjects. Such an access to content of electronic communications, with no possibility for an individual to pursue legal remedies, compromises the very "essence" of the fundamental rights to respect for private life and to effective judicial protection. As noted by Tracol, "this finding stands in stark contrast to the judgment of the Grand Chamber in the case of *Digital Rights* in which the invalidation of the data retention directive was based on the application of compliance with the principle of proportionality".[92] Reading the Directive in light of the Charter allows the Court to apply the methodology of Article 52 of the Charter referring to the essence of fundamental rights and so to avoid getting into the need of

89. Directive (EU) 2016/680 (*supra* note 87) concerns transfers of personal data for the purpose of "safeguarding against and the prevention of threats to public security" but it excludes from its scope activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of the Common Foreign and Security Policy. It is not clear whether counter-terrorism is to be related to "public security" or "national security".

90. Peltz-Steele, "The pond betwixt: Differences in the US-EU Data Protection/Safe Harbor negotiation", 19 *Journal of Internet Law* (2015), 14–27, at 23. However, see Case C-698/15, *Davis and Others*, pending, on data retention in the UK in light of the decision in Joined Cases C-293 & 594/12, *Digital Rights Ireland*.

91. Judgment, para 42.

92. Tracol, "'Invalidator' strikes back: The harbour has never been safe", 32 *Computer Law & Security Review* (2016), 345–362, at 357.

balancing between privacy and security. Judging the conditions to transfer data to third countries in this light, the Court could state that it did not need "to examine the content of the safe harbour principles".[93]

It also spared the Court from dealing with the issue of how reliable and complete information concerning the third country can be obtained. In this particular case, the Court had a relatively easy task, as it could rely on the Commission reports drawn up in response to the Snowden revelations and the High Court decision, which was also largely based on these publications. But already in this case, the Advocate General's Opinion was criticized by the Americans for allegedly using out-of-date information.[94] The issue of public and reliable information is of course a broader problem in the supervision of government intelligence agencies. In many instances it is only through leaks and whistle-blowers that pertinent information becomes public. But when it concerns third countries, the problems grow exponentially. Without the information provided by Snowden, the Court would have had a much harder task invalidating Safe Harbour. It may be especially challenging for the national supervisory authorities to examine accurately claims about privacy practices in third countries. Again, a mechanism of coordination between the national supervisory authorities and the Commission might have been helpful here in order to employ the more formidable resources of the latter to investigate (and not merely examine) claims concerning the level of protection in a third country.

The last issue is that the Court's approach is primarily concerned with the European aspects of personal data protection, without due regard to international aspects. The Court equates the level of protection offered by the Directive with the rights protected in the Charter. What is missing from this approach is a sense of strategy about the manner in which the Commission can act effectively on the international level. It can be doubted whether, in the absence of internationally workable standards, the individual is indeed better protected and whether in the absence of such standards the legal walls imposed to restrict the flow of personal data are permeable in practice.[95] International cooperation in personal data protection – though difficult – is

93. Judgment, para 98.

94. US Mission to the EU, "Safe Harbor protects privacy and provides trust in data flows that underpin transatlantic trade", statement of 28 Sep. 2015, available at <useu.usmission.gov/st-09282015.html>. See also Swire, "Don't strike down the Safe Harbor based on inaccurate views about US intelligence law", 5 Oct. 2015, available at <iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/>.

95. Kuner, op. cit. *supra* note 5, Chs. 7–8. This should also be seen in the light of an increasing legal and technical difficulty to determine whether data transfers have taken place. See Hon and Millard, "Data export in cloud computing: How can personal data be transferred outside the EEA? The cloud of unknowing: Part 4", Queen Mary School of Law Legal Studies Research Paper No. 85/2011 (London, 2012).

probably the best way to close the gap between fundamental rights protection on paper and in practice. However, it would be unfair to criticize the Court harshly in this instance: sacrificing basic data protection rights by accepting the practices as reported in this case would not only undermine the EU concept of the rule of law, but would also encourage courts in Member States to take the guarantees in their own hands and to question the primacy of EU law over national law.[96] International cooperation should not come at all costs. Maybe subsequent cases will give the ECJ more opportunities to take account of strategic considerations.

5.3. *Looking forward*

5.3.1. *The privacy shield*

The Court invalidated Safe Harbour on 6 October 2015 without limiting in either direction the temporal effects of the judgment, thus requiring an immediate response from the relevant institutions. Within a few days, the Article 29 Working Party declared that before the end of January 2016 an "appropriate solution" should be found, or the national supervisory authorities would start to take enforcement actions.[97] It noted furthermore that data transfers on the basis of Safe Harbour are now unlawful, but Standard Contractual Clauses and Binding Corporate Rules could still be used. In the following months, the Commission negotiated a new agreement with the US. The agreement, called the Privacy Shield, was announced early February 2016, and the Commission's implementing decision was adopted on 12 July 2016.[98]

The comment from the Article 29 Working Party about Standard Contractual Clauses and Binding Corporate Rules raises an important issue, namely about the level of protection offered by these instruments. Even though Article 26 of the Directive offers a derogation from the requirement that a third country offers an adequate level of protection, the question is whether these instruments are effective in protecting the right to personal data protection.[99] It is obvious that personal data transfers on the basis of Article 26

96. Kokott and Sobotta, "The *Kadi* Case: Constitutional core values and international law: Finding the balance?", 23 EJIL (2012), at 1015–1024.

97. Statement of the Article 29 Working Party on the implementation of the judgment of the ECJ of 6 Oct. 2015 in the *Maximilian Schrems* v. *Data Protection Commissioner* case (C-362/14), 16 Oct. 2015.

98. Commission Adequacy Decision of 12 July 2016, C(2016)4176 final, available at <ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>. See also Commission Communication of 27 Feb. 2016, "Transatlantic data flows: Restoring trust through strong safeguards", COM(2016)117 final.

99. Kuner, op. cit. *supra* note 86.

of the Directive must not infringe Articles 7 and 8 of the Charter. As the standard of "essentially equivalent" explicitly aims at preventing circumvention of the high levels of protection offered by the Directive and Charter, the system of derogations under Article 26 becomes problematic.[100]

The Privacy Shield is built on a similar approach of self-certification as Safe Harbour, with the addition of several assurances regarding the activities of US intelligence agencies, as well as some institutional innovations. The latter include the creation of a recourse mechanism of last resort, the Privacy Shield Panel, offering binding arbitration in disputes between individuals and participating organizations, and an Ombudsperson with regard to complaints concerning intelligence agencies.[101]

On mass surveillance, the Decision on the Privacy Shield refers extensively to a Presidential Policy Directive, signed by US President Obama in 2014 (hence prior to the *Schrems* judgment), limiting the use of information collected in bulk to six national security purposes, such as counterterrorism and "detecting and countering certain activities of foreign powers".[102] Lastly, it is interesting to note that the Commission recognizes the power of national supervisory authorities to suspend data transfers if it believes a person's personal data is not afforded an adequate level of protection on the basis of Article 28(3) of the Directive.[103] Somewhat strangely it recognizes this power by direct reference to the *Schrems* decision.[104]

This is not the place to assess in depth if and to what extend the Privacy Shield will resolve the problems identified by the Court in *Schrems*. Suffice it to note that opinions and resolutions by the Article 29 Working Party, the EDPS and the European Parliament have so far been quite critical, especially relating to the provisions on mass surveillance.[105]

100. The matter is already brought before the Irish High Court, with the Irish Data Protection Commission seeking declaratory relief and a referral to the ECJ "to determine the legal status of data transfers under Standard Contractual Clauses"; see Irish Data Protection Commissioner, "Statement by the Office of the Data Protection Commissioner in respect of application for Declaratory Relief in the Irish High Court and Referral to the CJEU", 25 May 2016, available at <www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm>.

101. Commission Adequacy Decision of 12 July 2016, C(2016)4176 final, Recitals 56–57 and 116–122. For the position of the Privacy Shield Ombudsperson, see also Annex III.

102. Ibid., Annex VI, at 4.

103. Ibid., Art. 3.

104. Ibid., Recital 142. More than an interpretation of the *Schrems* decision itself, the Adequacy Decision appears to anticipate the new Regulation, discussed *infra*, in confluence with the *Schrems* decision.

105. Article 29 Working Party, "Opinion 01/2016 on the EU-US Privacy Shield Draft Adequacy Decision", 13 April 2016, WP 238; European Data Protection Supervisor, "Opinion on the EU-US Privacy Shield Draft Adequacy Decision", 30 May 2016, Opinion 4/2016; European Parliament, "Resolution on transatlantic data flows", 26 May 2016, 2016/2727(RSP).

5.3.2. *The General Data Protection Regulation*

In the background to the case, negotiations had been ongoing for a new regulation on data protection, replacing the Directive.[106] Proposed already in 2012, political agreement was reached in December 2015.[107] The General Data Protection Regulation (Regulation 2016/679, GDPR) will apply as from May 2018.[108] Adopted at the same time as the GDPR are a directive on the processing of personal data for criminal justice purposes, including the transfer of data by public authorities to third countries, and a directive on the use of passenger name records (PNR).[109] It falls outside the scope of this case note to discuss the full implications of the new regulation and directives for the transfer of data to third countries, only the main tenets of the new regime for adequacy decisions in the GDPR are discussed.

The legal structure for personal data transfers remains largely intact. Personal data transfers to third countries are allowed if the third country ensures an adequate level of protection (Art. 45 GDPR), if appropriate safeguards (Art. 46 GDPR) are adduced through, for example, Standard Protection Clauses or Binding Corporate Rules (Art. 47) or on the basis of derogations for specific situations (Art. 49 GDPR). The decision on whether a third country (or an international organization, a territory or even specific sectors in a third country)[110] ensures an adequate level of protection is now solely in the hands of the Commission, but the requirements for such decisions are strictly described. Adequacy decisions must take into account "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case law, as well as effective and enforceable data subject rights

106. See De Hert and Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", 28 *Computer Law and Security Review* (2012), at 130–142; Voss, "Looking at European Union data protection reform through a different prism: The proposed EU General Data Protection Regulation two years later," 17 *Journal of Internet Law* (2014), at 11–22.

107. Commission, "Agreement on Commission's EU data protection reform will boost Digital Single Market", 15 Dec. 2015, Press Release IP/15/6321.

108. Regulation 2016/679 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. 2016, L 119/1.

109. Directive (EU) 2016/680 and Directive (EU) 2016/681, cited *supra* note 87.

110. Blume, "EU adequacy decisions: The proposed new possibilities", 5 *International Data Privacy Law* (2015), at 34–39.

and effective administrative and judicial redress for the data subjects whose personal data are being transferred" (Art. 45(2)(a)). Moreover, the existence and functioning of an independent supervisory authority in the third country must be taken into account. The Commission must monitor, on an ongoing basis, developments in third countries and review its adequacy decision at least every four years. The GDPR thus requires a wider-ranging assessment of third countries than the Court demands on the basis of the Directive read in light of the Charter, whilst maintaining "adequate" as the relevant standard.[111]

As for the institutional division of labour, the main question is whether the Court's interpretation of the Directive also applies to the GDPR. The reasoning of the Court seems to suggest so, in particular with regard to the duty of national supervisory authorities to examine individual complaints. Noteworthy in that regard is that although Article 45 GDPR departs from the procedures now found in Article 25 of the Directive, the tasks of the national supervisory authorities remains in essence the same. The Court mainly relied on Article 28 of the Directive, read in light of Article 8 of the Charter for the institutional questions, with Article 25(3) of the Directive being used – maybe in anticipation of the GDPR – only as a secondary argument. That the GDPR elevates the Commission as the principal decision maker on the adequacy of the level of protection of third countries therefore leaves the tasks of the national supervisory authorities untouched.[112]

6. Conclusion

The *Schrems* case comes amidst a rapidly changing legal and societal environment. The new Data Protection Regulation and the Privacy Shield are just two very notable ones from a legal point of view. After the judgment was announced in October 2015, terrorist attacks in Paris and Brussels again threw into doubt the balance being struck in our societies between privacy and security. The Irish High Court observed poignantly in its preliminary reference that Safe Harbour was from a more innocent age of data protection. What may be expected from a Court in such times, or put differently, how should we judge this judgment? Of course, we may expect the Court to enforce the fundamental values that make up our legal order. However, an eagerness to

111. Adequacy decisions adopted by the Commission under the Directive remain in force until amended, replaced or repealed according to Art. 45(9) GDPR.

112. Also see Art. 58(2)(j) GDPR, which gives national supervisory authorities the power "to order the suspension of data flows to a recipient in a third country or to an international organization". It is doubtful whether in the absence of *Schrems*, this would have meant that these authorities could interfere in cases where there is an adequacy decision.

formulate red lines may soon lead to a loss of credibility. Ideally, the Court uses its most powerful weapon of persuasion to give direction.

Invalidating Safe Harbour sends a strong signal towards audiences inside and outside the EU about the importance of data privacy for the EU legal order. In light of the Snowden revelations, the Commission's own assessment and the strong wording of the reference of the Irish High Court, Safe Harbour simply could not stand. However, the act of invalidating Safe Harbour does not by itself improve data privacy in Europe. Protecting the individual online from institutional domination is a complex and long term project. It is unfortunate, then, that the institutional shifts resulting from this decision are neither based on strategic considerations, nor part of a narrative aimed at realigning the priorities of the Commission.

Loïc Azoulai and Marijn van der Sluis*

* Loic Azoulai is Professor at Sciences Po Law School, Paris. Marijn van der Sluis is Ph.D. researcher at European University Institute, Florence, and lecturer at Erasmus University Rotterdam.