scripted

Volume 12, Issue 2, December 2015

WHEN THE SAFE HARBOUR IS NOT SAFE: WHAT NEXT FOR THE EU (CASE C-362/14, SCHREMS)

Jiahong Chen[*]

DOI: 10.2966/scrip.120215.167

[*] PhD Candidate, School of Law, University of Edinburgh. The author is funded by China Scholarship Council-University of Edinburgh Joint Scholarship programme.

1. Facts

Directive 95/46/EC (referred to as the Data Protection Directive)[1] imposes restrictions on transfers of personal data to a third country (i.e. non-EU/EEA country), which are allowed only if that country has ensured an "adequate" level of protection. However, Article 25(6) of the Directive provides that the Commission may, through a consultation procedure, find that a third country has met that requirement so that in principle restrictions are lifted. Pursuant to this provision, the Commission adopted Decision 2000/520[2], finding that transfers of personal data from the EU to the US compliant with the "Safe Harbor" Scheme are considered to have provided adequate safeguards. The scheme was introduced by the US Department of Commerce, containing a set of Safe Harbor Privacy Principles as well as an FAQ section, both annexed to the Commission Decision.

Maximillian Schrems (widely known as Max Schrems) is an Austrian national and has been a user of Facebook since 2008. Facebook users residing in the EU are required to conclude a contract with Facebook Ireland, a subsidiary of the US-based Facebook Inc., whereby their data are transferred to the US. After the 2013 Snowden revelations of mass surveillance by the US NSA and other intelligence services, Mr Schrems lodged a complaint with the Irish Data Protection Commissioner, requesting the latter to prohibit Facebook from transferring his personal data to the US. The Commissioner rejected Mr Schrems's complaint on the ground, *inter alia*, that the adequacy of the level of protection afforded by the US is a matter determined by Decision 2000/520. The case was then brought before the High Court of Ireland[3], which referred it to the Court of Justice of the EU (CJEU) for a preliminary ruling.[4]

2. Judgment

2.1 The separation of powers between the Commission and National Data Protection Authorities regarding the adequacy finding

The CJEU was asked to clarify, where a complaint against the adequacy of data protection provided by a third country has been made to a national data protection authority (DPA), whether the latter shall be absolutely bound by the adequacy Decision 2000/520 that the Commission makes pursuant to Article 25(6) of Directive

---

[1] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (accessed 30 Nov 2015) (hereinafter Data Protection Directive).

[2] *Commission Decision 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*, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000D0520 (accessed 1 Nov 2015).

[3] *Schrems v Data Protection Commissioner* [2014] IEHC 310.

[4] *Maximillian Schrems v Data Protection Commissioner*, Case C‑362/14 [2015] ECLI:EU:C:2015:650 (hereinafter *Schrems*).

95/46, or, alternatively, if the DPA has independent power to carry out an investigation.

The CJEU began its reasoning by reiterating each Member State's responsibility, under primary treaties (Article 8(3) of the Charter of Fundamental Rights (CFR) [5] and Article 16(2) of the Treaty on the Functioning of the European Union (TFEU)[6]) and secondary legislation (Article 28(1) of the Data Protection Directive), to set up a national supervisory authority to independently oversee the enforcement of data protection law within its territory.[7] The Court explained the purpose of Article 28(3), to provide DPAs with a number of powers and thus guarantee their effective operation, through the power to investigate, to effectively intervene and to engage in legal proceedings.[8] The transfer of personal data from a Member State to a third country constitutes "processing of personal data"[9] and is therefore subject to the oversight of the DPA in that State, as well as other safeguards laid down by the Directive.[10]

To that end, either the Commission or a Member State may determine whether a particular third country has ensured an adequate level of data protection to data subjects.[11] However, when the Commission decides that the third country in question *has* ensured an adequate level of protection, pursuant to Article 25(2) of the Data Protection Directive, Member States must "take the measures necessary to comply with the Commission's decision". In order to maintain the certainty and uniformity of EU law, the power to invalidate such a decision is exclusively reserved to the CJEU.[12] However, as the Court reasoned, it does not follow that an adequacy decision of the Commission would by any means preclude a data subject's right to lodge a complaint or a DPA's competence to hear that complaint.[13] Such preclusion would run counter to the objective of Article 28 in the effective operation of independent supervisory authorities.[14] The Court added that because a DPA, cannot on its own, declare a Commission's decision invalid, does not mean their investigation is meaningless; regardless of the investigation's outcome, the dispute is subject to judicial review: to be brought before the Court, either by the DPA (if it decides in favour of the data subject) or by the data subject (if it does the opposite).[15]

---

[5] *Charter of Fundamental Rights of the European Union*, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P (accessed 1 Nov 2015).

[6] *Consolidated Version of the Treaty on the Functioning of the European Union*, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E/TXT (accessed 1 Nov 2015). Article 16(2) (ex Article 286 TEC) reads "… [c]ompliance with these rules shall be subject to the control of independent authorities."

[7] *Schrems*, para 40.

[8] *Schrems*, para 43.

[9] *Schrems*, para 45.

[10] *Schrems*, paras 47-49.

[11] *Schrems*, para 50.

[12] *Schrems,* paras 61-62.

[13] *Schrems*, para 53.

[14] *Schrems*, paras 56-57.

[15] *Schrems*, paras 64-65.

Based on this reasoning, the CJEU concluded that the adequacy decision of the Commission did not prevent the DPA from examining the data subject's complaint against the actual level of protection provided by the law and practices in force in the third country.

2.2 The validity of Decision 2000/520

Despite the fact that the Irish High Court did not explicitly question the validity of Decision 2000/520, the CJEU found it relevant to consider this in its decision. The Court did not directly examine the specifics of the Decision but rather, tried to establish a standard of "adequate level of protection" as the first step. It is noted that there is no straightforward definition of such a standard contained in the Directive,[16] but it is clear from the wording of Article 25(6) that personal data should remain under a high level of protection even if they are transferred to a third country. Such a standard does not have to be identical to that provided by EU law, but "essentially equivalent" to it (paras. 71-73). That means, according to the Court, when the Commission is deciding on the adequacy of protection in a third country, its discretion should be limited (para. 78). The Decision is subject to stricter scrutiny, taking into account the content of the national law and international commitment of the country concerned, the availability of review at regular intervals, and the new circumstances after the adoption of the Decision (paras. 75-77).

With these criteria in place, the CJEU examined the content of Decision 2000/520 starting from Article 1. The Court quotes a number of stipulations of the Decision and its Annexes so as to make clear the actual effects and implications thereof. First, the Safe Harbor Scheme takes a self-certification approach, which, while not necessarily contrary to the "domestic law or international commitment" requirement set out by the Directive, must be founded on effective enforcement mechanisms.[17] However, since the Safe Harbor Principles apply only to organisations joining the scheme and are not binding on US public authorities, this could not satisfy the Directive's conditions.[18] Second, the Annexed Principles and FAQs drafted by the US have embodied derogation clauses when it comes to national security, public interest and law enforcement, as well as rules of conflicts that demand the participating organisations to comply with US law,[19] giving the latter, in effect, a superior status to EU law. Third, the Decision makes no reference to any rules restricting US powers or any remedies for data subjects to challenge US actions.[20] The Court then compares EU legislation and case law – which regards mass untargeted surveillance as a violation of fundamental human rights – with the level of protection guaranteed by the Decision, concluding that it has not fulfilled the "essentially equivalent" standard.[21]

In the last part of its judgment, the Court analyses Article 3 of Decision 2000/520, which concerns the conditions under which national DPAs may suspend transfers of

---

[16] *Schrems*, para 70.

[17] *Schrems*, para 81.

[18] *Schrems*, para 82.

[19] *Schrems*, paras 84-86.

[20] *Schrems*, paras 88-89.

[21] *Schrems*, paras 91-98.

personal data. Under Article 3, a DPA may suspend transfers if an organisation is found violating the Safe Harbor Principles by a US government body or an independent recourse mechanism, or if the DPA, subject to certain substantive and procedural restraints, has established a substantial likelihood of violation. According to the Court, while this provision makes it clear that it is without prejudice to the DPAs' powers, Article 3 does deny DPAs the possibility of taking direct actions to ensure compliance with the Directive.[22] To this extent, the Court rules that Article 3 of the Decision exceeds the Commission's statutory power and is therefore invalid.[23]

Since Articles 1 and 3 are inseparable parts of Decision 2000/520, the Decision is invalid in its entirety.[24]

3. Comment

Schrems is hailed as a landmark ruling in the field of EU data protection law.[25] The significance of the judgment lies in that the CJEU has dealt with the rather complicated relationships between the Commission and national DPAs with regard to the power to determine whether a third country has guaranteed adequate level of data protection. In doing so, the CJEU has struck down Decision 2000/520 concerning the Safe Harbor Agreement, though this was not part of the initial questions formulated by the referring court. The whistle-blower Edward Snowden's revelations of the US surveillance programme "PRISM" in 2013 caused worldwide concerns over governmental access to personal data. The *Schrems* decision was thus decided at a time when public criticisms remain intense and steps taken by the US remain unsatisfactory. It is also a timely judgment given that the EU data protection overhaul is underway and moving closer to its completion, on which the judgment could shed further light. It is clear that the CJEU maintains its consistent position, from *Digital Rights Ireland*[26] to *Google Spain*[27], in upholding a high level of personal data protection. As will be shown below, however, along with the profound implications to which the judgment gives rise, it also leaves certain significant uncertainties unsolved.

3.1 Regulatory model and the one-stop-shop approach

Throughout the *Schrems* judgment, the CJEU repeatedly highlights the importance of preserving the independence of DPAs, a principle enshrined in multiple European Community instruments and reflective of the objectives of data protection laws.

---

[22] *Schrems*, paras 101-103.

[23] *Schrems*, para 104.

[24] *Schrems*, paras 105-106.

[25] Article 29 Data Protection Working Party, "Statement of the Article 29 Working Party" (2015) available at europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (accessed 1 Nov 2015).

[26] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, Joined Cases C-293/12 and C-594/12, [2014] OJ C 175/07.

[27] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case-131/12, [2014] OJ C 212/04.

However, when the adequacy of data protection afforded by a third country is questioned, the role of DPAs become extremely complex. This is due to the potentially conflicting roles that the Commission and DPAs might play in determining the adequacy status of a third country. As explained above, both the Commission and DPAs may make their own decisions under Article 25 of the Data Protection Directive. However, the Commission's finding appears to have greater weight (not just in that it has EU-wide effect), given that Article 25(6) requires "Member States shall take measures necessary to comply with the Commission's decision". Under this two-tier design, national DPAs are obliged to obey the Commission's findings as organs of the Member States, until it is no longer valid.[28] As a result, there is tension between Member States' obligations and DPAs' independence.

Such a tension is aggravated by the different nature of the interests they represent. As the executive body of the EU, the Commission is bound to represent the interests of the EU in a more general way, whereas the DPAs are designed to protect individuals with regard to the processing of personal data[29]. To the extent that the Commission and DPAs have different functions, the CJEU has persuasively interpreted the provisions of the Directive in holding that while the DPAs are legally bound by the Commission's decisions (pursuant to Article 25(6)), they can challenge decisions in legal proceedings or through the exercise of their functions, where appropriate.

The strengthened roles of DPAs could secure greater data protection to individuals, but their elevated role could be incompatible with the more centralised approach proposed in the current legal reform. Apart from retaining the Commission's power in making an adequacy decision, the proposed General Data Protection Regulation, which is to replace the Data Protection Directive, is to introduce what is called the "one-stop-shop" mechanism to further harmonise the application of data protection laws. Under the latest Council draft of the Regulation[30], the DPA of the Member State in which the data controller (or processor) has its main establishment, shall act as the lead authority (Article 51(1)). The lead DPA shall cooperate with DPAs of other concerned Member States and provide mutual assistance (Articles 54a(1) and (1a)). However, if these DPAs fail to reach a consensus on the outcome of a case, the matter shall be submitted to a European Data Protection Board (Article 54a(3)). The Board is composed of the European Data Protection Supervisor and one representative of the DPA from each Member State (Article 64) and its decision would be binding on national DPAs (Article 58a(1)).

In this light, *Schrems* is important to the shaping of the one-stop-shop mechanism. It is arguable that the one-stop-shop approach taken in the draft Regulation could compromise the independence of national DPAs, depending on how the binding force of the European Data Protection Board's decision is understood. Given that the CJEU has ruled Decision 2000/520 as invalid, not just based on the Data Protection Directive but also on the basis of the TFEU, in the worst-case scenario, the one-stop-

---

[28] *Schrems*, paras 51-53.

[29] Data Protection Directive, Recital 62.

[30] Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Preparation of a general approach" available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (accessed 30 Nov 2015).

shop mechanism might also be declared invalid for violating 16(2) TFEU, a primary source from which the independence of DPAs derives. This would place the mechanism under grave uncertainty as the draft Regulation does not make clear whether a Board decision would prevent a DPA from carrying out further investigation on the same subject-matter or bringing a legal challenge. If so, that might be contrary to *Schrems*; if not, what is the point of the one-stop-shop?

3.2 Conditions of suspension and the role of DPAs

One of the grounds on which the CJEU invalidated Decision 2000/520 is that Article 3 imposes unreasonable restrictions on DPAs' powers to suspend the transfers when substantial risks are identified. While it is true that the substantive and procedural thresholds laid down by Article 3 are quite high, it nevertheless provides national DPAs a clear legal basis on which they can take measures to stop data transfers when Safe Harbor Principles are being violated. By contrast, the Data Protection *per se* does not include any provision which unambiguously confers such a power to DPAs, but instead requires Member States to comply with Commission decisions on adequacy. In this light, it is proposed that Article 3 of Decision 2000/520 should be viewed as a clause that empowers – not limits – DPAs.

As the CJEU reasoned, Article 3 explicitly provides that it is without prejudice to DPAs' powers, but the Court maintains that it excludes the possibility for DPAs to take actions. Unfortunately, the Court did not specify under what circumstances their powers could be undermined. In fact, it would be more logically consistent to treat Article 3 as a supplementary provision to the Directive rather than a restrictive one. If the Directive implies such powers, the DPAs are not affected; if not, the DPAs gain such powers from the Decision instead. Either way, the DPAs have sufficient ground to suspend non-compliant transfers.

Another pragmatic reason why the Court should not rule Article 3 invalid is that the ruling might affect the legitimacy of personal data transfers to third countries other than the US. The US is not the only country with existing arrangements for personal data transfers from the EU. The Commission made a series of decisions that recognise a further eleven non-EU/EEA jurisdictions as providing adequate levels of data protection.[31] Each of these adequacy decisions contains a provision almost identical to Article 3 of Decision 2000/520, the nullification of which might in turn threaten the validity of these remaining eleven decisions. It is praiseworthy that the CJEU reiterated the importance of DPAs' independence, but given that the functioning of Article 3 depends entirely on the validity of Article 1, there is no need to examine the former when the latter has been ruled invalid. To eliminate the uncertainties resulting from *Schrems*, the Commission must carry out a comprehensive sweep of these decisions and, where necessary, make appropriate amendments.

---

[31] These jurisdictions are Switzerland (Decision 2000/518), Canada (Decision 2002/2), Argentina (Decision 2003/490), Guernsey (Decision 2003/821), the Isle of Man (Decision 2004/411), Jersey (Decision 2008/393), the Faeroe Islands (Decision 2010/146), Andorra (Decision 2010/625), the State of Israel (Decision 2011/61), the Eastern Republic of Uruguay (Decision 2012/484) and New Zealand (Decision 2013/65). See: "Commission decisions on the adequacy of the protection of personal data in third countries" (2015) available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed 30 Nov 2015).

3.3 The fate of alternative legal bases for EU-US data transfers

While Decision 2000/520 can no longer serve as a valid justification for US-based companies to receive personal data, it is far from true that such data transfers will come to a halt. The Data Protection Directive provides alternative mechanisms by which personal data can be transferred to a third country. Under Article 26(2), for instance, if two data controllers (one being outwith the EU) conclude a contract using Commission-approved model clauses[32], this contract will be regarded as offering sufficient safeguards and thus transfers of personal data to the third country controller will be still allowed. Similar exemptions include, *inter alia*, obtaining informed consent from data subjects (Article 26(1)(a)) and adopting binding corporate rules (BCRs)[33].

However, the availability of these options does not render the *Schrems* judgment pointless. These alternative arrangements would subject data exporters and importers to stricter rules and tougher scrutiny. Also, the legitimacy of these alternatives has become more vulnerable to challenges after *Schrems*. For instance, German DPAs have suspended approvals of BCRs and disputed the validity of model clause-based transfers.[34] National DPAs may prohibit or suspend data flows to a third country if the governing law of the data importer sets out derogations from data protection law that "go beyond the restrictions necessary in a democratic society".[35] The question is: if the CJEU finds that a third country (in this case, the US) fails to provide sufficient data protection, does this finding necessarily lead to the conclusion that data flows to the third country in question based on model contractual clauses should be stopped immediately as some DPAs have suggested?[36] Unlike the case of an adequacy decision where restrictions on data transfers to a third country are generally removed,

---

[32] For Controller-to-controller clauses: Decision 2001/497 (2001) available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001D0497&from=en (as amended by Decision 2004/915 (2004) available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004D0915&from=EN) (accessed 30 Nov 2015). For Controller-to-processor clauses: Decision 2010/87 (repealing Decision 2002/16) (2010) available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=EN (accessed 30 Nov 2015).

[33] Article 29 Data Protection Working Party, "Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (2003) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (accessed 1 Nov 2015); Article 29 Data Protection Working Party, "Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities" (2012) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc (accessed 1 Nov 2015); Article 29 Data Protection Working Party, "Explanatory Document on the Processor Binding Corporate Rules" (2015) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf (accessed 1 Nov 2015).

[34] C Ritzer et al, "German Data Protection Authorities Suspend BCR approvals, question Model Clause transfers" (2015) available at www.dataprotectionreport.com/2015/10/german-data-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers (accessed 28 Oct 2015).

[35] Decision 2001/497, Article 4 (see note 35 above); Decision 2010/87, Article 4 (see note 35 above).

[36] "Model clauses no substitute for 'safe harbour' data transfers to the US, says German watchdog" (2015) available at www.out-law.com/en/articles/2015/october/model-clauses-no-substitute-for-safe-harbour-data-transfers-to-the-us-says-german-watchdog (accessed 28 Oct 2015).

model clause-based transfers are subject to national DPAs' approval. Therefore, it is arguable that in the course of assessing the law of a third country, the threshold in the latter case (model clauses) should not be as high as the former (adequacy decision). In other words, the fact that a third country cannot guarantee adequate data protection does not necessarily mean that contractual safeguards in that country are all ineffective. Having said that, the judgment in *Schrems* still constitutes a compelling ground if a DPA considers suspending data transfers to the US.

Even if US companies decided to ask their users for consent, it would not offer much reassurance to data controllers. National DPAs have already indicated different attitudes towards the implications of *Schrems* for consent to operate as a valid justification for third country data transfers. While a UK regulator claimed that "transfers can always be made on the basis of an individual's consent",[37] German DPAs would argue for further limitations over consent by data subjects.[38] Inconsistent interpretations of data protection laws among Member States will not only create difficulties for data controllers in compliance with the law, but also cause *de facto* unequal protection standards within the EU. If the long-expected General Data Protection Regulation is to mitigate these uncertainties and divergences, an effective harmonisation approach is required. However, effective harmonisation requires reverting back to discussions on maintaining a balance between a centralised decision-making process and the dependent role of DPAs, which could be an intractable problem. On this view, *Schrems* does not signal the end of the dispute, but rather the beginning.

[37] D Smith, "The US Safe Harbor – breached but perhaps not destroyed!" (2015) available at https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed (accessed 1 Nov 2015).

[38] Ritzer et al, see note 34 above.