A REALITY CHECK OF THE SCHREMS SAGA

CLAES G. GRANMAR*

From an enforcement point of view, the revocation of the European Commission's two adequacy decisions on the federal US system of data protection raises many questions regarding the interrelations between the EU data protection regime and the Union's legal frameworks for data 'transfers'. Whereas data uploaded in the Union was once upon a time wired over the Atlantic to be downloaded in the US and vice versa, data packets are nowadays often exchanged over various radio spectra. As online resources around the world can be used to store data, and the data is made available and retrieved from domains rather than 'exported' and 'imported', the idea that the EU data protection regime would no longer apply when data is 'transferred' from the Union easily leads astray. In fact, the location of data or data processing equipment is irrelevant for the applicability of EU law as its territorial scope is determined by the location of the data subjects or undertakings concerned. Whereas the EU legislation applies with regard to legal entities overseas with affiliated undertakings in the Union, the Union seeks to guarantee the EU data subjects an adequate level of protection also in cases of onward transfers of data to non-affiliated organisations and unwarranted interceptions. Furthermore, the European Commission promotes a level of protection in non-EU Member States that is essentially equivalent to that enjoyed under the EU data protection regime since the authorities and courts may refrain from applying EU law pursuant to private international law. However, the Cases which resulted in the revocation of the two adequacy decisions concerned an Austrian citizen filing complaints against an undertaking established in Ireland and its US parent company. Hence, it must be called into question whether the EU data protection regime should at all have been substituted by the US system irrespective of whether it provided an adequate level of data protection. An argument could be made that the adequacy decisions applied beyond the substantive scope of EU law, but that brings questions to fore about the competence of the Union to adopt such decisions. In addition, the procedural system introduced in the first Case regarding Mr. Schrems is rather problematic as it requires national authorities and courts to assess the validity of adequacy decisions. Besides the distortion of the right for national courts to request preliminary rulings into an obligation to do so, most data subject are reluctant to get involved in disputes about the entire legal regime. In many instances, the data subject may rather rely on her or his procedural rights as a consumer. In this article, a systematic analysis of these aspects of the EU privacy safeguards is provided.

1 INTRODUCTION

In the third preliminary ruling resulting from the efforts of the Austrian citizen Mr. Schrems to uphold European Union ('EU') privacy standards, often incorrectly referred to as '*the Schrems II case*', the European Court of Justice ('ECJ') answered questions regarding the European Commission's standard contractual clauses and the amended adequacy decision

* LL.D. DIHR, Associate Professor, Stockholm university, Faculty of Law.

regarding the United States ('US').[1] Mr. Schrems had begun his campaign against internet giants in the noughties, and following the revelations about US online mass-surveillance programs, there can be no doubt about that his complaints regarding the Facebook group lodged with the Irish Data Protection Authority ('DPA') were primarily intended to prevent security agencies from having unrestricted access to personal data.[2] Indeed, the regulation of data processing (or the lack thereof) has political and geopolitical implications. However, the preliminary rulings regarding Mr. Schrems are properly understood only in the light of the powers conferred upon the Union and the pronounced systematics of EU law. Whereas the ECJ is according to Article 5(2) of the Treaty on European Union ('TEU') required to ensure a teleological construction of EU law, consistency between the Union's actions is stipulated most clearly in Article 7 of the Treaty on the Functioning of the EU ('TFEU').[3] Indeed, *Schrems I and III* are explained by the duty of the ECJ to promote a system-coherent scope of fundamental rights, rather than by any (geo)political choices.[4] In addition to the general framework for data protection, there is specific EU legislation on data processing in the electronic communication services- and law enforcement sectors, as well as with regard to the processing of personal data by EU institutions and customs authorities.[5] By contrast, security policy remains pursuant to primarily Articles 4(2) and 21(2)(a) of the TEU, and Parts 5 and 7 of the TFEU, largely within the competences of each Member State.

Whereas the original adequacy decision on the US ('the Safe Harbour Decision') was annulled in *Schrems I*, the amended decision ('the Privacy Shield Decision') was invalidated in *Schrems III*.[6] It is of course reassuring that the ECJ defends the rights to privacy and data

---

[1] Even though the Judgement of the ECJ in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (*Schrems III)* ECLI:EU:C:2020:559 resulted from the second set of complaints lodged by Mr. Schrems with the Irish Data Protection Commissioner pursuant to the preliminary ruling in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650, also Case C-498/16 *Maximillian Schrems v Facebook Ireland Limited* (*Schrems II*) ECLI:EU:C:2018:37, where the ECJ explained the status of the user of a private Facebook account as 'consumer' is relevant from an enforcement perspective.

[2] See primarily Max Schrems, *Kämpf um deine Daten* (Wien edition a GmbH 2014). See also Joshua P Meltzer, 'After *Schrems II*: The Need for a US-EU Agreement Balancing Privacy and National Security Goals' (2021) 1 Global Privacy Law Review 83.

[3] See also, the principles of conferral and sincere cooperation in Articles 4(1) and (3) of the TEU.

[4] See as to the duty to promote Union values in external relations Articles 3(5) and 21 of the TEU. See as to the correlation between internal and external aspects of the EU data protection regime in Communication from the Commission, 'A comprehensive approach on Personal Data Protection in the European Union' COM (2010) 609 final, 19.

[5] See primarily, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (as amended); Directive (EU) 2016/680 on processing of personal data for the purpose of 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 [2016] OJ L119/89; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39; and Regulation (EU) 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code [2013] OJ L269/1, as amended by Commission Implementing Regulation (EU) 2020/893 [2020] OJ L206/8.

[6] Commission Decision 2000/529/EC On the Safe Harbour Principles [2000] OJ L215/7, and Commission Decision (EU) 2016/1250 On the EU-US Privacy Shield (Privacy Shield Decision) [2016] OJ L207/1. See also Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the

protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU ('the EU Charter'). However, the preliminary rulings bring questions to the fore about the possibilities for data subjects to enforce their rights against data exporting controllers and processors in the Union.[7] First of all, why should adequacy decisions that blur the substantive scope of data protection define the rights of the EU data subjects when EU data protection legislation is applicable?[8] In both *Schrems I and III*, the ECJ recognised that the 'transfer' of data from a Member State to a third country constitutes, in itself, data processing 'carried out in a Member State'.[9] As Mr. Schrems lodged complaints with an Irish DPA regarding data processing by undertakings in the Facebook group established in the Union, he could have relied on Irish law approximated by the Data Protection Directive ('DPD') without a detour over any adequacy decision, and the same applies *mutatis mutandis* to the General Data Protection Regulation ('GDPR').[10] An EU data subject could pursuant to Article 4 of the DPD invoke domestic law even against a controller established in a non-Member State ('third country') with an affiliated EU establishment. According to Article 3 of the GDPR that applies also with regard to overseas processors.[11] Notably, if the scope of data protection *in the Union* depends on assessments of legal frameworks in third countries, the EU data subject would be better off without any adequacy decision.[12]

Secondly, in *Schrems I* the ECJ explained the procedural system that enables the Court to assess the validity of an adequacy decision and, if necessary, revoke it indirectly through a preliminary ruling. Again, it is of course appropriate to have a mechanism for assessment of Commission decisions. However, the obligation for a DPA to assess complaints regarding data processing in the Union in the context of imprecise adequacy decisions and to bring legal actions before national courts, which in turn *shall* request preliminary rulings as soon as they are in doubt about the validity of a decision, can be formally called into question and may be counterproductive in the prolongation. Because the imminent risk that a complaint leads to systematic checks ultimately by the ECJ is likely to chill the willingness of most data subjects to seek legal redress for alleged infringements.[13] Thirdly, why did the Austrian citizen Mr. Schrems lodge complaints with an Irish DPA instead of in the country of his habitual

Council [2010] OJ L39/5, as amended by Commission Implementing Decision 2016/2297 (SCC Decision) [2016] OJ L344/100.

[7] See the definitions of 'controller', 'processor', and 'recipient' in Articles 4(7)(8) and (9) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119/1.

[8] Compare with GDPR (n 7) arts 44-45.

[9] See GDPR (n 7) art 4(2), the definition of processing. Compare with *Schrems I* (n 1) para 45, and *Schrems III* (n 1) para 83.

[10] 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 (DPD) [1995] OJ L281/31 and the GDPR (n 7), repealing the DPD. See also Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Facebook Insights)* ECLI:EU:C:2018:388.

[11] Case C-131/12 *Google Spain SL and Google Inc. v Agencia España Proteccion de datos (AEPD) and Mario Costejo González (Google Spain)* ECLI:EU:C:2014:317.

[12] See GDPR (n 7) art 44 establishing that no provision in Chapter V thereof shall undermine the level of protection guaranteed by the Regulation. See also recitals 101 to 104 in the preamble to the GDPR.

[13] Compare with Commission Communication, 'Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the GDPR' COM (2020) 264 final,. There are several private online 'GDPR enforcement trackers', such as GDPR Enforcement Tracker <www.enforcementtracker.com> (*tracked by CMS*) accessed 4 November 2021.

residence, place of work or place of the alleged infringement?[14] Pursuant to the proper *Schrems II* ruling that was handed down by the ECJ in January 2018, a data subject can also be classified among 'consumers' and, hence, challenge the contractual terms for data processing before authorities and courts in the Member State where he or she is domiciled.[15] In the present article, these three aspects of the *Schrems saga* will be explored.

2 WHY SHOULD ADEQUACY DECISIONS THAT BLUR THE SUBSTANTIVE SCOPE OF DATA PROTECTION DEFINE THE RIGHTS OF THE EU DATA SUBJECTS WHEN EU DATA PROTECTION LEGISLATION IS APPLICABLE?

In *Schrems I*, the Austrian data subject had lodged complaints with the Irish Data Protection Commissioner where he contended that the DPA should prohibit or suspend the transfer of his personal data since the US legal system 'did not ensure adequate protection of the personal data held in its territory against the surveillance activities in which the public authorities were engaged'.[16] However, the Irish Data Protection Commissioner rejected the complaints because he considered trans-Atlantic transfers of personal data categorically cleared by the Safe Harbour Decision.[17] Consequently, Mr. Schrems brought proceedings against the Irish DPA before the Irish Hight Court that in turn referred several questions for a preliminary ruling to the ECJ. In response to those questions the ECJ concluded that the adequacy decision did not fit the bill.[18] As the Court invalidated the Safe Harbour Decision, the Irish High Court remanded the case to the DPA, that found it necessary to examine whether the transfers of personal data could be cleared under the standard data protection clauses which Facebook Ireland Ltd and Facebook Inc had undertaken to comply with.[19] In order to do so, the Irish DPA requested the Austrian data subject to reformulate his complaints. Pursuant to the new complaint and 'in order for the High Court to refer a question on that issue to the [ECJ]', the DPA brought proceedings against Facebook Ireland Inc. and Mr. Schrems.[20]

In the interval between the action brought by the Irish Data Protection Commissioner before the national court of first instance and the time when that court referred its second sets of questions for a preliminary ruling to the ECJ, the new adequacy decision on the US was adopted by the European Commission. Pursuant to the self-certification system

---

[14] In the field of data protection, compare GDPR (n 7) art 77 with the distribution of labour between the DPAs in arts 55 – 60. See also recitals 126-138 in the preamble to the GDPR.
[15] See *Schrems II* (n 1). See as to the general definition of 'consumer' in EU law, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64, art 2(1).
[16] *Schrems I* (n 1) para. 52.
[17] ibid paras 29-30.
[18] ibid paras 67-106.
[19] See SCC Decision (n 6).
[20] *Schrems III* (n 1) para 57. See also European Data Protection Board (EDPB), 'Guidelines 02/2020 on the European Essential Guarantees for surveillance measures adopted by the European Data Protection Board' adopted on 10 November 2020 <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en> accessed 11 December 2021.

established by the Privacy Shield Decision, organisations in the US could commit to a set of privacy principles issued by the US Department of Commerce that the European Commission had considered ensuring an adequate level of data protection. Furthermore, the Commission approved the US legal-administrative system for monitoring of compliance with the principles, and the venues for EU data subjects to enforce their rights. However, in *Schrems III* the ECJ found it opportune to assess the validity of the Privacy Shield Decision. Although normative measures do normally not apply retroactively and a preliminary ruling should clarify the state of the law at the time of the event which is the subject matter of the main proceedings, the ECJ explained that the analysis should 'take into consideration the consequences arising from the subsequent adoption of the Privacy Shield Decision'.[21] Hence, the Court reviewed the decision to clear the US data protection regime instead of explaining the rights for an EU data subject to prevent data processing in terms of 'transfers'. As a result, the Privacy Shield Decision was invalidated by the ECJ.

As explained by the ECJ in *Schrems I*, an adequacy decision *complements* EU legislation where it is contended that the laws and practices in the third country do not ensure an adequate level of protection.[22] It was, therefore, established in Article 2 of the Privacy Shield Decision that the adequacy decision did generally speaking not affect the application of the provisions of the DPD 'that pertain to the processing of personal data within the Member States, in particular Article 4 thereof'.[23] More to the point, the EU-US Privacy Shield Principles should according to recital 15 in the preamble to the adequacy decision apply only in as far as processing by a self-certified organisation did 'not fall within the scope of Union legislation. The Privacy Shield does not affect the application of Union legislation governing the processing of personal data in the Member States'. In that connection, some words should be said about use of the location of data or the location of processing activities as criteria for determining what legal regime shall apply with regard to data 'transfers'.[24]

There are still traces in the EU data protection legislation of a time when data was stored in a dedicated server or terminal device under an Internet Protocol (IP) address and bits and bytes were exchanged by means of physical infrastructure for telecommunication such as copper or fibre optic cables. For instance, Articles 44-45 of the GDPR seems to be centred around the idea that the European Commission must approve that personal data geographically leaves the territory of the Union. It transpires from the *first and third Schrems* cases that this induced the Irish Data Commissioner and subsequently the Irish High Court to consider that an adequacy decision applies as soon as personal data is relocated from machines in the Union to machines in a third country.[25] In fact, even the ECJ alludes to

[21] *Schrems III* (n 1) para 151.
[22] *Schrems I* (n 1) para 46.
[23] In Article 2 of the Privacy Shield Decision (n 6), art 2 makes an exemption for DPD (n 10) art 25(1) that was affected.
[24] Data location requirement is at the outset prohibited in the EU, see Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59. Furthermore, the protection of personal data within the scope of the DPD and GDPR is an exemption from the free movement of data in the Union, see in particular GDPR (n 7) recital 4 in the preamble. However, data location requirements in relation to third countries are not prohibited - see W. Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Edward Elgar Publishing 2017).
[25] *Schrems I* (n 1) para 29.

'transfer' as a decisive factor when determining the applicability of EU legislation.[26] However, in the light of the development of the internet infrastructure that would be absurd.

Since the adoption of the DPD in 1995 the internet architecture and protocols have radically changed. Whereas the Open System Interconnection Model ('OSI') enables machines to 'talk' also via radio protocols such as those used for the fifth-generation cellular network technology ('5G'), several 'logical servers' can run on one physical device by means of virtualisation technology.[27] In many instances, dynamic IP-numbers are assigned to machines as tasks are allocated to them. Conceptual models for reconfiguration of available resources in computer networks, metaphorically known as 'cloud computing' promote system redundancy and efficiency.[28] Hence, data found under an IP address can be in many different places, sometimes simultaneously. An undertaking that has pointed its machines under an IP addresses to the domain name 'facebook' on the Irish top-level domain ('TLD') may rent server space from an undertaking headquartered in Sweden, that may in turn use physical servers located in France for one moment and some logical servers originating in the US, or a satellite orbiting the earth, the next.

Obviously, if data is uploaded from a terminal device in an EU Member State, and downloaded in the US, it is 'transferred' overseas in some sense. However, a more appropriate notion is that the data is *accessed from a name space*. Data 'exporting' undertakings in the EU and data 'importing' organisations in third countries process data under one or more TLDs administrated by national network information centres ('NICs') or may choose to use the regional TLD .eu or a generic TLD such as .edu or .com. Even if personal data is collected under national TLDs in the Union and an undertaking established in a Member State such as Facebook Ireland Ltd allows an organisation established in the US such as Facebook Inc. access to that data, the data exchanges may take many different paths. Whereas it is often difficult if not impossible to tell where the data is processed at a given time, it is easy to establish what legal entity is responsible for data processing within an address space.

In the light of this, the concept of an adequacy decision that does not affect the application of Union legislation governing the 'processing of personal data in the Member States' becomes enigmatic. Perhaps the ECJ was led astray in *Schrems I and III* by public discourse, the questions formulated by the Irish court and interventions of some Member States in the *first Schrems case*. Perhaps the Court deliberately overlooked the need to investigate the applicability of EU data protection legislation with a view to acknowledge a procedural system for evaluation of adequacy decisions. In any event the decisions of the ECJ not to reject the references for preliminary rulings as merely hypothetical in the main proceedings and, hence, unfounded, explains why *Schrems I and III* concerned the validity of

[26] *Schrems III* (n 1) paras 59 and 63. See also EDPB, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR adopted by the EDPB on 18 November 2021' ('the interplay guidelines') <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en> accessed 11 December 2021.

[27] For those who are interested in communication technology an early account on the matter is Debbra Wetteroth, *OSI Reference Model for Telecommunications* (McGraw-Hill Education 2001).

[28] See, eg, Cristopher Millard, *Cloud Computing Law* (2nd edn, OUP 2021); Kevin L Jackson and Scott Goessling, *Architecting Cloud Computing Solutions: Build Cloud Strategies that align* (Packt 2018).

adequacy decisions instead of the right of Mr. Schrems to protect his personal data.[29] Having said that, there are limits to what teleology can do to justify rulings by the ECJ.

There are good reasons why an adequacy decision can merely complement EU data protection legislation. EU data subjects enjoy a fundamental right to data protection that can only be limited or qualified by other private or public interests in accordance with Article 52 of the EU Charter.[30] It would create inconsistencies contrary to Article 7 of the TFEU to substitute the balancing of interests within the scope of applicable EU legislation with the limits and safeguards regarding data processing in a third country even if such a regime provides an adequate level of protection. More to the point, not to recognise applicable EU legislation challenges the rule of law.[31] In order to determine whether a data subject must have resort to a legal-administrative framework for data protection in a third country that the European Commission has approved, it is necessary to investigate the territorial and substantive scope of EU data protection legislation.

3 DATA TRANSFERS AND THE TERRITORIAL SCOPE OF EU DATA PROTECTION LEGISLATION

In addition to the difficulties to locate the place for automated data resolution, 'law' as we know it remains normative only for natural persons and legal persons created by man, such as companies.[32] Since controlling human language and legal sanctions are empty blows against algorithms and self-learning systems classified among artificial intelligence ('AI'), the territorial scope of EU data protection legislation is determined by the place where the legal entities are, as opposed to the location of data or data processing infrastructure.[33] It is true that Article 4(c) of the revoked DPD established that it could be taken into consideration whether equipment was situated on the territory of a Member State when determining the territorial scope of national legal frameworks in the absence of other links to the Union. But due to the development of the internet infrastructure, the criterion tended to make the possibility to invoke EU data protection law more and more arbitrary contrary to the rule of law.[34] Consequently, Article 3(1) of the GDPR establishes that the Regulation applies to the

[29] See the limitations of the ECJ's competences in these regards most clearly established in Case C-244/80 *Pasquale Foglia v Mariella Novello* ECLI:EU:C:1981:302, para 18. See for an overview of the right for national courts to request preliminary rulings in Koen Lenaerts, Ignace Maselis and Kathleen Guthman, *EU Procedural Law* (OUP 2014). Compare with Nils Wahl and Luca Prete, 'The Gatekeepers of Article 267 TFEU: On Jurisdiction and Admissibility of References for Preliminary Rulings' (2018) 55(2) Common Market Law Review 511.

[30] See GDPR (n 7) recital 4 in the preamble.

[31] See as to the objective to ensure consistency as an interpretative method in for instance Case C-673/17 *Planet49 GmbH* ECLI:EU:C:2019:801, para 48. Obviously, the understanding of the rule of law is a sensitive topic in the current state of affairs in the Union, see Case C-791/19 *Commission v Poland (Régime disciplinaire des juges)* ECLI:EU:C:2021:596.

[32] See, eg, Alberto de Franceschi and others (eds), *Digital Revolutions – New Challenges for Law* (C.H. Beck 2019); Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence* (Vintage 2018); and Claes Granmar, 'Artificial Intelligence and Fundamental Rights from a European Perspective' in Claes Granmar and others (eds), *AI & Fundamental Rights* (iinek@law and informatics 2019).

[33] On that note, the EDPB is simply wrong when stating on page 3 in the interplay guidelines (n 26) that 'the overarching legal framework provided within the Union no longer applies' when 'personal data is transferred and made accessible to entities outside the EU territory'.

[34] Indeed, the EDPB recognises the implications of these wordings in its Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) ('the Article 3 guidelines') <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en> accessed 11 December

processing of personal data in the context of the activities of an establishment of the controller of processor in the Union 'regardless of whether the processing takes place in the Union or not'.[35] In addition, EU data protection legislation is triggered when the data subjects are in the Union. There must be a sufficient *link* to the Union for the EU data protection legislation to apply.[36]

Even if the DPD applied when the complaints resulting in the *Schrems III* case were lodged, a final decision had not been adopted by the Irish DPA at the time when the GDPR entered into force. Hence, the ECJ established that the questions referred by the Irish court in that Case should be answered in the light of the provisions of the Regulation rather than those of the Directive.[37] Then again, Article 7 of the TFEU required the Court to as far as possible construe the relevant provisions in the GDPR and DPD in the same way, along the lines of evolutionary consistency. Indeed, the *Schrems III* ruling builds on the construction of the DPD in *Schrems I*.[38] However, in the following only provisions in the GDPR will be referred to for practical reasons.

Given the broad interpretation of the criteria for determining the territorial scope of EU data protection law when the controller has its principal place of business in a third country, it is difficult to imagine a situation where the exchange of data regarding individuals in the Union between EU and US entities in the same group of undertakings escapes the scope of the GDPR.[39] In its seminal *Google Spain* ruling, concerning a search engine provider established in the US that processed data regarding a Spanish citizen, the ECJ explained that it only takes a local sales office in the Member State where the data subject is when the data is processed, to consider the data processed in the context of the activities of an establishment of the controller in the Union.[40] Correspondingly, the ECJ has clarified that the existence of a sales office in a Member State is a sufficient basis for jurisdiction when distributing the labour between DPAs within the Union.[41] In fact, the GDPR can be invoked in a Member State where the controller or processor has a merely *affiliated* undertaking, such as a legal representative, that is involved in the processing activity.[42] Hence, it is difficult not

2021. Hence, it is far from convincing the that the EDPB on page 5 in the interplay guidelines (n 26) refers to the Article 3 guidelines when explaining that EU data legislation does not apply when data is 'transferred' to a third country.

[35] Originally this was not recognised as a basis for application in the DPD, but it is now enshrined in GDPR (n 7) arts 3(2)(a) and (b).

[36] This is a system-coherent approach in accordance with Article 7 of the TFEU. Compare, for instance, with EU competition law that applies when conduct in third countries have effect in the Union: Joined Cases C-89/85, Case C-104/85, Case C-114/85, Case 116/85, Case 117/85 to Case 129/85 *A. Ahlström Osekeyhtiö and Others* ECLI:EU:C:1988:447; and Case C-413/14 P *Intel* ECLI:EU:C:2017:632. See also for an overview, Marise Cremona and Joanne Scott, *EU law beyond EU borders* (OUP 2019).

[37] *Schrems III* (n 1) paras 77-79.

[38] ibid para 71.

[39] Claes Granmar, 'Global applicability of the GDPR in context' (2021) 11(3) International Data Privacy Law 225.

[40] *Google Spain* (n 11). It must be said that a discussion on GDPR (n 7) art 3(1) in the light of the *Google Spain* ruling and related rulings is conspicuously absent in the interplay guidelines (n 26). Indeed, the reasoning of the EDPB and the explanations provided in the interplay guidelines are irreconcilable with the case law on GDPR (n 7) art 3(1) and with its own Article 3 guidelines (n 34).

[41] See for instance *Facebook Insights* (n 10).

[42] See GDPR (n 7) recitals 37 and 48 in the preamble. See also, in particular, Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* ECLI:EU:C:2015:639.

to arrive at the conclusion that EU data protection law applied to the transfer of personal data from Facebook Ireland Ltd to Facebook Inc. in *Schrems I and III*.

As undertakings in third countries may monitor or target data subjects in the Union or have affiliated EU establishments, it is easily believed that EU law reaches around the world without discernment. A common misconception is that the GDPR has vaguely defined 'extraterritorial' applicability. From a distance the EU institutions seem to throw their weight around for obscure political reasons and the discourse has sometimes been fraught with overtones about 'digital colonialism'. Evidently, the construction of the criteria in Article 3 of the GDPR contributes to significant overlaps between EU law and the jurisdiction of norm giving powers in third countries. However, overlapping jurisdictions is a smaller problem than it may seem in a first glance. In view of the duty of the EU institutions to afford everyone in the Union access to justice pursuant to Article 47 of the EU Charter it is, indeed, preferable to lawless domains in cyberspace.[43] Furthermore, it is far from sure that EU law can be invoked against overseas legal entities within its territorial scope, since there are *procedural aspects* of the enforcement of legal rights.

Whereas the GDPR establishes a system for enforcement of fundamental rights in the Union, the EU legislator has no authority to decide how justice should be administered in a third country. If an EU data subject of some reason would consider it necessary to take legal actions overseas, the enforcement of EU law usually depends on rules pertaining to private international law. In that connection, the fundamental rights of data subjects in the Union can be promoted by adequacy decisions.[44] Pursuant to the Privacy Shield Decision, an EU data subject could bring a complaint to a certified organisation in the US that processed her or his data, to an independent dispute resolution body designated by such an organisation, or to the US Federal Trade Commission ('FTC').[45] In addition, a Federal US Ombudsperson was introduced to oversee compliance with the US legal framework regarding data processing for national security and law enforcement purposes.[46] A data subject could also seek redress by lodging a complaint with the competent DPA in an EU Member State when the data was accessed in a third country in the context of an employment relationship, or when the US organisation had voluntarily committed to the DPAs investigatory powers.[47] Then again, in *Schrems I and III* the EU data subject had lodged complaints with an Irish DPA against a

[43] In practice, knowledge thresholds and economic constraints may be hurdles to overcome for the enforcement of rights. See, eg, Lawrence Lessig, *Code: And other Laws of Cyberspace, version 2.0* (Basic Books 2006). Compare with, eg, Dan Jerker B Svantesson, 'Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effects on U.S. Businesses' (2014) 50(1) Stanford Journal of International Law 53; and Christopher Kuner, 'Extraterritoriality and regulation of international data transfer in EU data protection law' (2015) 5(4) International Data Privacy Law 235.

[44] See also GDPR (n 7) art 50 entitling the European Commission to develop 'international cooperation mechanisms' to facilitate effective enforcement. See also a more philosophical account on the impact of EU data protection law on the conceptualisation of privacy worldwide – Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 New York University Law Review 771, 773. See also Maria Helen Murphy, 'Assessing the implications of the *Schrems II* for EU-US data flows' (2021) 4 International and Comparative Law Quarterly 1.

[45] Privacy Shield Decision (n 6) recitals 41 and 45 in the preamble.

[46] ibid recital 65 in the preamble.

[47] ibid (n 6) recital 48 in the preamble.

business group with establishments in the Union, which suggests that compliance with EU legislation that specified his fundamental rights was required without reservations.[48]

4 DATA TRANSFERS AND THE SUBSTANTIVE SCOPE OF EU DATA PROTECTION LEGISLATION

Although the Privacy Shield was invoked within the territorial scope of EU data protection legislation, *Schrems III* arguably concerned data processing beyond the *substantive scope* of EU law. Indeed, the main purpose of the Privacy Shield Decision was to control access and use of personal data by US authorities 'for national security, law enforcement and other public interest purposes'.[49] It was really a 'shield' against onward transferring of personal data from the self-certified undertaking in the US, and unwarranted interception of data from the internet by US authorities. Consequently, the applicability of the Privacy Shield went beyond the substantive scope of the EU legislation. Because, as mentioned in the introduction to this piece, the EU Member States have retained the powers to shape national security policies, and virtually no competences have been conferred upon the EU institutions to regulate the processing of personal data for security policy purposes. Having said that, pre-arranged exchanges of personal data between private parties and national security services are according to the ECJ captured by the general EU data protection regime.[50] By contrast, exchanges between national security services, or interception of data from exchanges between private parties without their consent or awareness escapes the scope of EU law. Arguably, the reason why the DPA and High Court investigated the validity of the Privacy Shield in the *Schrems cases* was the risk of arbitrary processing by US authorities for security purposes. If so, the specific legislation adopted by the Union regarding data protection would have been inapplicable.

It is questionable whether the European Commission's mandate to evaluate and negotiate data protection standards in third countries can at all go beyond the Union's substantive right to regulate. True, the EU institutions have a duty towards the Member States in accordance primarily with Articles 3(5) and 21 of the TFEU, to uphold and promote the values and interests of the Union in its relations with the wider world, and 'to contribute to the protection of its citizens'. And the Member States benefit greatly from the negotiating position of the European Commission when it comes to protection of their citizens against mass surveillance by foreign powers. But, as long as no competences have been conferred upon the Union by the Member States, the only basis for the validity of the Union measure is the silence of the 'Masters of the Treaties'.[51] Having said that, it could be argued that an adequacy decision merely confirms that the limits and safeguards for data processing in the third country are appropriate in some general sense. Even if the European Commission has

[48] Even if not taking secondary EU legislation into account, Article 8 of the EU Charter would probably have horizontal direct effect - compare with Case C-414/16 *Vera Egenberger v EvangelischesWerk für Diakonie und Entwicklung e.V*. ECLI:EU:C:2018:257.

[49] Privacy Shield Decision (n 6) recital 65.

[50] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (Privacy International)* ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others (La Quadrature du Net)* ECLI:EU:C:2020:791.

[51] See as to the possibility for Member States to bring direct revocation proceedings in Article 263 of the TFEU.

no competence to enter into agreements in the field of security policy, it is entitled to confirm that the protection of data in the third country is adequate. Furthermore, it may be difficult to distinguish between data processing for national security purposes and for purposes that come within the competences conferred upon the EU institutions. At some level all bulk data can be considered valuable information for intelligence services. An adequacy decision clarifies the limits and safeguards for data processing in general without specifying the national security requirements that apply to for instance one individual in a photograph that do not apply to other persons in the same photograph. By contrast, national security measures are casuistic and rather override adequacy decisions than limit the competences of the European Commission to approve third country systems. Nonetheless, it is a systematic anomaly that the Safe Harbour and Privy Shield addressed *primarily* US legal-administrative frameworks regarding access to data for security purposes.

It follows from the principle of conferral that the Member States should retain a right to decide what kind of information third country security services should access about the EU data subjects. On that note, it should be mentioned that all the EU Member States are parties to the European Convention on Human Rights ('ECHR') that applies to data processing for any purpose.[52] More to the point, the right to privacy enshrined in Article 8 of the ECHR and the right to a fair trial in Article 6 thereof apply also to data processing for national security purposes. Consequently, also the basis for an assessment of the validity of an adequacy decision adopted by the European Commission with regard to overseas processing for national security purposes, is the construction of those provision by the European Court on Human Rights ('ECtHR').[53] Since the ECtHR and the ECJ seek to ensure a coherent development of fundamental rights in Europe, virtually the same standards for data protection apply under both regimes.[54]

In *Schrems I and III*, the ECJ seemed prepared to accept the competence of the European Commission to adopt adequacy decisions covering data processing in the field of US security policy. Indeed, the substantive scope of the adequacy decision induced the ECJ to conclude in *Schrems I*, that EU data protection law applies 'by its very nature, to any processing of personal data'.[55] That is of course far from convincing since there are as mentioned statutory limitations with regard to the spatial as well as substantive applicability of the general and specific EU data protection legislation. However, the absence of analysis of the scope of EU legislation in the preliminary rulings may be explained, albeit not justified, by an objective that is lurching behind the scenes. By clarifying that an adequacy decision must ensure the EU data subjects a level of protection that is 'essentially equivalent' to that enjoyed under the EU data protection regime, the Court put a pressure on providers of digital

[52] European Convention on Human Rights (ECHR), signed in Rome on 4 November 1950.
[53] See most recently judgement by the ECtHR *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR, 25 May 2021); see also *Big Brother Watch and Others v The United Kingdom* Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).
[54] See Article 53 of the EU Charter and, for instance. Case C-84/95 *Bosphorus* ECLI:EU:C:1996:312. See however, *Opinion* 2/94 *Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms* ECLI:EU:C:1996:140 and *Opinion* 2/13 *On the draft agreement providing for the accession of the European Union to the Convention for the Protection of Human Rights and Fundamental Freedoms* ECLI:EU:C:2014:2454. See as to data processing *Planet49 GmbH* (n 31) para 70.
[55] *Schrems I* (n 1) para 57.

services which have signed up for adequacy principles to improve their encryption and increase the costs for those who want to steal personal data ('data protection by design').[56]

When it comes to systematic and large-scale interception of data by state actors or private firms, only the resources required to tap bits and bytes from the online exchanges, or from the real world by means of terminal devices equipped with cameras, microphones, or sensors, protects the user's integrity. With power comes responsibility and the allocation of costs to build systems that protect personal data should be placed primarily on tech giants that spend most of their resources on the development of internet architecture such as Alphabet Inc. (that owns Google Inc.) and Meta Inc. (that operates 'Facebook'). For the time being it is a mystery how undertakings that 'export' or 'import' data from the Union could in response to an individual claim erase data regarding a specific data subject for instance in a photograph, without also erasing personal data regarding other data subjects in the photograph. Anyhow, the EU Charter requires that EU data subjects have legal remedies to erase the personal data from the internet without regard to the level of technological development.

If accepting that the adequacy decisions on the US did not escape the competences conferred upon the Union, we are back to where we started as to the interrelation with EU data protection legislation. Because, if the transfer of personal data from Facebook Ireland Ltd to Facebook Inc. constituted data processing within the territorial and substantive scope of EU data protection legislation, it would have been an error in law not to recognise the fundamental rights of Mr. Schrems. From what we know, Mr. Schrems addressed his complaints to the Irish company and even if the US Organisation was also targeted there was no need resorting to the US system for data protection.

5 DOES THE RULE OF LAW REQUIRE A DPA TO ASSESS THE VALIDITY OF AN ADEQUACY DECISION WHEN A LEGAL ENTITY IN A THIRD COUNTRY ACCESSES DATA FROM AN ESTABLISHMENT IN THE EU?

In *Schrems I*, several Member States intervened and raised concerns regarding the principle of primacy. They wondered whether a DPA could examine the limits and safeguards for data processing in a third country which have already been categorically approved by the European Commission.[57] Notably, the legal basis for Union measures in the field of data protection is mixed and whereas the EU institutions and the Member States have shared powers to regulate the internal market, the Union has exclusive competences to shape a common commercial policy ('CCP').[58] Most likely, an adequacy decision should be classified

[56] See Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15, and Commission Communication, 'A European Strategy for Data' COM(2020) 66 final.

[57] *Schrems I* (n 1) paras 37-44. See also declaration 17 to the EU Treaties concerning primacy [2008] OJ C115/344.

[58] Article 16 of the TFEU which is referred to as a main legal basis only concerns data processing by the Union and its Member States as opposed to data processing by private parties. See further as to the required consistency in Ramses A Wessel and Joris Larik, 'The EU as a Global Actor' in Ramses A Wessel and Joris Larik (eds), *EU External Relations Law* (2nd edn, Hart Publishing 2020).

among the Union's external actions. If accepting that the Safe Harbour formed part of the CCP, there were good reasons for asking about the right for a national authority to substitute a Commission decision with its own assessment. As mentioned, the ECJ instead took the opportunity to shape a system for checking the validity of adequacy decisions and explained that the *effet utile* of EU law could set aside its primacy.

With a view to promote the overriding objective of the Union to protect personal data, the ECJ established in the *Schrems I* case that there is nothing that prevents a national authority such as a DPA from overseeing transfers of personal data within the framework of an adequacy decision.[59] Conversely, a DPA must be able to examine a processing activity with 'complete independence' and it is incumbent upon the national authority to examine a claim with 'all due diligence'.[60] According to the Court, it would be 'contrary to the system' set up by EU law for a decision to have the effect of hindering a DPA from examining 'a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision'.[61] In order to safeguard fundamental rights and freedoms, those authorities possess

> investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definite ban on processing of data, and the power to engage in legal proceedings.[62]

Ultimately, it followed from a Union concept of 'the rule of law' that a decision must not prevent a DPA

> from examining the claim of a data subject 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 when that person contends that the law and practices in force in the third country [sic!] do not ensure an adequate level of protection.[63]

Indisputably, a data subject must 'have access to judicial remedies enabling him to challenge [a decision] adversely affecting him before national courts' pursuant to Article 47 of the EU Charter.[64] However, Article 47 of the Charter does not necessarily require that every data subject should be entitled to challenge the validity of an adequacy decision adopted by the European Commission. Nonetheless, the ECJ recognised a duty for DPAs to bring proceeding that enable national courts to refer questions for preliminary rulings regarding the validity of adequacy decisions. Furthermore, the right of a national court to request a preliminary ruling pursuant to Article 267 of the TFEU, was translated into an obligation to refer questions to the ECJ on the validity of an adequacy decision if the concerns that have

[59] *Schrems I* (n 1) paras 54-55.
[60] ibid paras 57 and 63.
[61] ibid para 56.
[62] ibid para 43.
[63] ibid para 66.
[64] ibid para 64.

been raised are considered well founded.[65] In the preamble to the Privacy Shield that was annulled in the *Schrems III* case, the European Commission recognised the explanation of the ECJ in the *Schrems I* ruling regarding the assessment of adequacy decisions. According to recital 144, there was an obligation to provide the DPA with legal remedies in national law to put well founded complaints as to the compliance of an adequacy decision with the fundamental rights to privacy and data protection, before a court 'which in case of doubts must stay proceedings and make a reference for a preliminary ruling to the Court of Justice'.

Whereas the Privacy Shield was annulled in substance, the route outlined in *Schrems I* by the ECJ to an indirect revocation procedure under Article 267 of the TFEU, is considered good law.[66] On the surface, this construction of EU legislation and Commission decisions may seem agreeable. It is after all virtually impossible for an individual or a group of people to challenge the legality of a legislative or regulatory act adopted by the EU institutions under Article 263 of the TFEU.[67] However, the *first and third Schrems* rulings become less convincing on closer inspection. Because, when it comes to data processing by controllers or processors in the Union the GDPR still applies by default, and the validity of an adequacy decision has no bearing on the case. In fact, to condition the right for natural persons in the Union to protect personal data on whether the data has been or will be transferred to one country, or another, would be contrary to the rule of law.

In addition to the problem with foreseeability, which is an essential aspect of the rule of law, there is an imminent risk that an individual complaint gives rise to comprehensive checks of legal regimes. Evidently, Mr. Schrems invoked his *individual rights* by filing complaints with the Irish DPA regarding the Facebook group, as opposed to challenging the adequacy decision on the US in the abstract. True, the legal actions brought by the Irish DPA in the *Schrems I* case was in line with his aspirations.[68] But, for most EU data subjects the change in gear from an individual complaint to assessment of whether a decision on adequacy is valid in general is a far from tempting prospect. Already the risk of having the decision in a case significantly delayed due to unnecessary systematic checks of adequacy decisions speaks against the rights to access justice and to a fair trial.[69] It may very well be a contributing factor to the low number of complaints lodged so far with DPAs.[70]

In fact, the procedural system that emerges from the *first and third Schrems* cases seems to be designed for activists and not for data subjects seeking to stop the processing of their personal data. True, the ECJ has clarified that national authorities and courts shall assess an adequacy decision only insofar as the case involves 'well founded complaints' regarding the decision's validity. And there is much leeway for the national authorities and courts to

---

[65] *Schrems I* (n 1) para 64.

[66] Compare with *Schrems III* (n 1) para 73, where the ECJ maintains that it 'solely for the national court' to determine the need for a preliminary ruling and the relevance of the referred questions although it 'must' stay the proceedings and refer questions about the validity of an adequacy decision if it is considered well founded.

[67] See Case C-25/62 *Plaumann* ECLI:EU:C: 1963:17 and Case C-583/11 P *Inuit Tapiriit Kanatami and Others* ECLI:EU:C:2013:625.

[68] An alternative route would be a Citizenship initiative regarding data transfers, see Article 11(4) of the TEU, Article 24(1) of the TFEU, Regulation (EU) 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative [2011] OJ L65/1, and Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative [2019] OJ L130/55.

[69] We are still waiting for the decisions by the Irish DPA on the claims actually lodged by Mr. Schrems.

[70] See supra n 13.

determine the matter. But the fact that the ECJ considered the concerns with the two adequacy decisions on the US well founded in the *Schrems* cases suggests that the threshold for such an assessment is low. As mentioned in footnote 12, Article 44 of the GDPR establishes that no measure regarding data transfers shall undermine the level of protection guaranteed by the Regulation. Hence, the appraisal of trans-Atlantic 'transfers' of bulk data should in the *Schrems* cases have been based on the EU data protection regime and not on merely an 'essentially equivalent level of protection'. At the end of the day, the risk of farfetched assessments of the validity of adequacy decisions sits uncomfortably with the fundamental right to data protection pursuant to Article 7 and 8 of the EU Charter and the right for the data subject to have her or his individual case tried in accordance with Article 47 of the Charter. In view of this, it is difficult to reconcile the procedural system outlined by the ECJ in the f*irst and third Schrems* cases with 'the rule of law' as normally understood in the Member States.

6 WHY SHOULD AN EU DATA SUBJECT WHO IS DOMICILED IN ONE MEMBER STATE LODGE COMPLAINTS ABOUT DATA PROCESSING WITH NATIONAL AUTHORITIES IN ANOTHER MEMBER STATE?

According to Article 77 of the GDPR, every individual classified among EU data subjects

> shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.[71]

Furthermore, each DPA 'should be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'.[72] By contrast, if the subject matter of the processing activity relates to 'a group of undertakings' with establishments in more than one Member State, or affects data subjects in more than one of those States, the DPA of the main establishment of that group of undertakings as defined in Article 4(16a-b) of the GDPR shall be competent to act as the *lead supervisory authority*.[73] A lead supervisory authority may choose to handle a case itself and ultimately decide it, albeit in cooperation with the other DPAs concerned and after taking due account of their views.[74] Since the main establishment of the European Facebook group is located in

[71] See GDPR (n 7) art 4(1) on the definition of EU data subject.
[72] See GDPR (n 7) art 52(2).
[73] See ibid recital 36 in the preamble, and Article 29 Data Protection Working Part, 'Guidelines for identifying a controller or processor's lead supervisory authority' (G29 Guidelines) adopted on 13 December 2006 WP244, 16/EN <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf> accessed 5 November 2021. See further Luca Tosoni, 'Article 4(16). Main Establishment' in Cristopher Kuner and others (eds), *The EU Data Protection Regulation (GDPR): A Commentary* (OUP 2020).
[74] GDPR (n 7) arts 56 and 60.

Ireland, the Irish DPA was the lead supervisory authority in the *Schrems* cases.[75] Perhaps Facebook Inc. also recognised the authority of the Irish DPA, but as mentioned, the adequacy decisions on the US were in any event inapplicable since the approximated Irish legislation applied.[76]

According to Article 78(1) of the GDPR, each natural or legal person in the Union shall without prejudice to any other applicable administrative or non-judicial remedy, 'have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them'.[77] Pursuant to Article 78(3) of the GDPR, proceedings against a supervisory authority 'shall be brought before the courts of the Member State where the supervisory authority is established'. Consequently, in *Schrems I* the Austrian data subject brought an action before the Irish High Court challenging the decision by the Irish lead supervisory authority to reject his complaints.[78] Also, the DPA that is competent to handle a case may bring proceedings against legal entities involved in the processing activity to assess the validity of an adequacy decision.[79] In *Schrems III*, it was as mentioned the Irish DPA that considered itself compelled to bring actions before the Irish High Court.[80]

Since only national administrative courts can normally review decisions taken by national authorities, it is uncontroversial that the jurisdiction of the national DPAs and the national courts coincide. Nonetheless, a data subject using online social network services is at the same time a 'consumer'.[81] Each user must enter into an agreement with the service provider and accept the policy of the undertaking, albeit in many instances merely in the form of a 'click and wrap' approval. Hence, some words should be said about the right to an effective remedy and to a fair trial pursuant to Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters ('the amended Brussels I Regulation').[82] It establishes specific rules on *locus standi* for individuals in cases regarding consumer contracts.[83] According to Article 18(1) of the amended Brussels I Regulation the consumer may bring actions either before the courts of the Member State in which the other party is domiciled or, 'regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled'. Conversely, proceedings may according to Article 18(2) of that Regulation be brought by the other party only 'in the courts of the Member State in which the consumer is domiciled'.

Although the freedom of contract is a fundamental right enshrined in Article 16 of the EU Charter, it is not possible for an individual to effectively contract away her or his status

---

[75] Even if Mr. Schrems also filed complaints with DPAs in Germany and Belgium, the case was handled by the Irish DPA.
[76] See Privacy Shield Decision (n 6) recital 15.
[77] See GDPR (n 7) recital 141 in the preamble, and vertical consistency with Article 47 of the EU Charter.
[78] *Schrems I* (n 1) paras 29-30.
[79] ibid para 65.
[80] *Schrems III* (n 1) para 52.
[81] See n 15. See also for instance, Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2019); and Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54(5) Common Market Law Review 1427.
[82] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (amended Brussels I Regulations) [2012] OJ L351/1. It could be mentioned that the amended Brussels I Regulations does not apply in Denmark.
[83] ibid art 17.

as 'consumer'.[84] However, the data subject may use a personal account for a wide range of online activities. In the *Schrems II* case, the Court explained that the user of social media, such as those provided by the Facebook business group, may retain the status of a 'consumer' even if the platform is used to form opinions or to promote economic interests.[85] More concretely, the ECJ explained that the legal framework for consumer disputes

> must be interpreted as meaning that the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement do not entail the loss of a private Facebook account user's status as 'consumer.[86]

Hence, Mr. Schrems could have taken legal actions in Austria against one or more European undertakings in the Facebook group to prevent the transfer of his personal data to the US.

Notably, the system set up for enforcement of private rights by the GDPR applies without prejudice to any other administrative or non-judicial remedy on which the data subjects may rely.[87] Even if the DPAs may in many instances facilitate the enforcement of data protection rights across the Union, the risk of ending up in litigations before administrative courts in foreign countries involving references for preliminary rulings may paradoxically make it more appealing to invoke consumer rights. On that note, Regulation 524/2013 regarding online dispute resolution in consumer cases provides a legal framework for easy access to justice that could apply also with regard to data protection.[88] Even if the possibility to lodge complaints about contractual terms regarding data processing to a consumer Ombudsman or organisation is good, online access to justice may be better.[89] In parity with the pressure put by the ECJ in *Schrems I and III* on firms to prevent data leaks, *Schrems II* signals that a high level of data protection is required by those who code applications for dispute resolution, rather than clarifies the relationship between EU legislation and an adequacy decision.

7 SOME CONCLUDING REMARKS

A century ago, justice was administrated mainly by local, provincial or national courts and tribunals. Gradually, however, more and more normative responsibilities were transferred to public administration and institutions such as Ombudsmen along with new forms of dispute resolution. We are now at the verge of a new paradigm of automated day-to-day legal decision

---

[84] Compare with *Facebook Insights* (n 10) and Case C-191/15 *Verein für Konsumentinformation v Amazon EU Sàrl* (*Amazon EU*) ECLI:EU:C:2016:612.
[85] *Schrems II* (n 1) paras 39-41. However, the case concerned the corresponding provision in the original Brussels I Regulation - Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1.
[86] *Schrems II* (n 1) para 41.
[87] Compare with *Planet49 GmbH* (n 31) para 33.
[88] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [2013] OJ L165/1.
[89] A consumer organisation should pursuant to Article 80(2) of the GDPR also be entitled to lodge complaints with national DPAs on behalf of data subjects - see Opinion of Advocate General de la Tour, Case C-319/20 *Facebook Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherbände – Verbraucherzentrale Bundesverband e.V*. ECLI:EU:C:2021:979.

making. However also algorithms and AI shall be used in a human-centric way and it must, therefore, be possible to hold natural and legal persons producing and using the systems accountable. Instead of procedural rules that the judiciary needs to follow, those who develop systems for automated decision-making need standards for what machines can and cannot do to humans. Furthermore, the role of the courts shifts from deciding individual cases on the facts to primarily review legal-technical regimes and ensure that there are remedies to challenge them. Preliminary rulings are particularly apt to promote a system of rule-based exchanges in cyberspace.

In the light of the aforementioned, the ECJ's preliminary rulings in *Schrems I* and *III* are commendable. It is impractical for data subjects to read the terms for use of each and every online service and in the wake of information fatigue the liability to protect data should be placed on the internet developers. Presumably, most people prefer some online privacy, and hopefully scholars that criticise the scope of the EU data protection regime will eventually realise that automated data protection may benefit people living in for instance developing countries as much as those being in Europe. In general, the fear of extraterritorial applicability is overexaggerated since the fact that a regime applies to legal entities in a third country does not necessarily imply that it can be enforced there. Indeed, that is the main reason why the European Commission can issue adequacy decisions. Having said that, the ECJ overstretched its competences in *Schrems I and III* by making digressions from the system-coherency that it must ensure pursuant to Article 7 of the TFEU. In response to the questions posed in the introduction to this article it must be said that an adequacy decision should be inapplicable when EU data protection legislation can be invoked; the transformation of individual complaints into systematic checks of adequacy decisions sits uncomfortably with the rule of law; and a data subject can in her or his capacity as a consumer challenge the terms for data processing including data transfers before national authorities and courts in the country where he or she is residing.

LIST OF REFERENCES

Cremona M and Scott J, EU law beyond EU borders (OUP 2019).
DOI: https://doi.org/10.1093/oso/9780198842170.001.0001

de Franceschi A and others (eds), *Digital Revolutions – New Challenges for Law* (C.H. Beck 2019).
DOI: https://doi.org/10.17104/9783406759048-1

Granmar C, 'Artificial Intelligence and Fundamental Rights from a European Perspective', in Granmar C and others (eds), *AI & Fundamental Rights* (iinek@law and informatics 2019).

— —, 'Global applicability of the GDPR in context' (2021) 11(3) International Data Privacy Law 225.
DOI: https://doi.org/10.1093/idpl/ipab012

Helberger N, Zuiderveen Borgesius F and Reyna A, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 Common Market Law Review 1427.

Howells G, Twigg-Flesner C and Wilhelmsson T, *Rethinking EU Consumer Law* (Routledge 2019).

Jackson K L and Goessling S, *Architecting Cloud Computing Solutions: Build Cloud Strategies that align* (Packt 2018).

Kuan Hon W, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Edward Elgar Publishing 2017).

Kuner C, 'Extraterritoriality and regulation of international data transfer in EU data protection law' (2015) 5(4) International Data Privacy Law 235.

Lenaerts K, Maselis I, and Guthman K, *EU Procedural Law* (OUP 2014).

Lessig L, *Code: And other Laws of Cyberspace, version 2.0* (Basic Books 2006).

Meltzer J P, 'After *Schrems II*: The Need for a US-EU Agreement Balancing Privacy and National Security Goals' (2021) 1 Global Privacy Law Review 83.

Millard C, *Cloud Computing Law* (OUP 2021).
DOI: https://doi.org/10.1093/oso/9780198716662.001.0001

Murphy M H, Assessing the implications of the Schrems II for EU-US data flows, (2021) 4 International and Comparative Law Quarterly 1.
DOI: https://doi.org/10.1017/S0020589321000348

Schrems M, *Kämpf um deine Daten* (Wien edition a GmbH 2014).

Schwartz P M, 'Global Data Privacy: The EU Way' (2019) 94 New York University Law Review 771.

Svantesson D J B, 'Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effects on U.S. Businesses' (2014) 50(1) Stanford Journal of International Law 53.

Tegmark M, *Life 3.0 – Being Human in the Age of Artificial Intelligence* (Vintage 2018).

Tosoni L, 'Article 4(16). Main Establishment' in Kuner C and others (eds), *The EU Data Protection Regulation (GDPR): A Commentary* (OUP 2020).
DOI: https://doi.org/10.1093/oso/9780198826491.003.0022

Wahl N and Prete L, 'The Gatekeepers of Article 267 TFEU: On Jurisdiction and Admissibility of References for Preliminary Rulings' (2018) 55(2) Common Market Law Review 511.

Wessel R A and Larik J, 'The EU as a Global Actor' in Wessel R A and Larik J (eds), *EU External Relations Law* (2nd edn, Hart Publishing, 2020).

Wetteroth D, *OSI Reference Model for Telecommunications* (McGraw-Hill Education 2001).