NORDIC JOURNAL OF EUROPEAN LAW

Volume 4
Issue 2 · 2021

LUND UNIVERSITY
FACULTY OF LAW

ISSN 2003-1785

NORDIC JOURNAL OF EUROPEAN LAW
ISSUE N 2 OF 2021

njel@jur.lu.se

http://journals.lub.lu.se/njel

Lund University

TABLE OF CONTENT

ARTICLES

REVIEWS

Editorial Note

It is with great pleasure that we present this issue of the *Nordic Journal of European Law* (NJEL). Like all issues of the NJEL, the current issue analysis a variety of matters within European law.

Most of the contributions of the current issue are articles developed from presentations given at the seminar '*The Consequences of Schrems II from Practical and Theoretical Perspectives*', sponsored by the Swedish Network for European Legal Studies and held at the Faculty of Law, Lund University on September 16, 2021. The seminal *Schrems II* case hence constitutes the foundation on this issue of the NJEL. By its judgment in *Schrems II*, the CJEU invalidated the EU-US Privacy Shield Framework as a basis for data transfers. At the core of ruling is the finding that third-country law must be assessed on a case-by-case basis to assure a degree of protection that is substantially equivalent to that provided for by EU law.

In this vein, the current issue contributes to develop a deeper understanding of the principles at play in the *Shrems II* case, as well as to foster further academic research within the area. Indeed, the saga around cross-border transfers under the GDPR is far from ended. Further research is expected, making the scattered picture of EU data privacy law more coherent.

On a separate note, we at the NJEL wish all our readers a happy new year!

The Editorial Board

A WEAPONIZED COURT OF JUSTICE IN *SCHREMS II*

JEFFERY ATIK,* XAVIER GROUSSOT†

The U.S.-EU conflict over the application of the General Data Protection Regulation (GDPR) to U.S.-based digital platform companies is marked by a startling legal development: the insertion of a constitutional court squarely into the heart of the dispute. The engagement of the EU's top court - the Court of Justice (CJEU) - in the Schrems I and Schrems II cases - has significantly inflamed the dispute. The CJEU has now twice struck down GDPR accommodations reached between the United States and the European Union. In doing so, the Court has rebuked both U.S. and EU officials. By transfiguring provisions of the GDPR with constitutional (that is, treaty-based) and human rights values, the Court has placed out of reach any accommodation that does not involve significant reform of U.S. privacy and national security provisions. Heated trans-Atlantic disputes involving assertions of extraterritorial extensions of regulatory power is an inappropriate place for a constitutional court like the CJEU to throw its declarative weight around.

1 INTRODUCTION

In two succeeding negotiations - first the Safe Harbour,[1] and then the Privacy Shield[2] - U.S. and EU officials reached agreement that qualifying U.S.-based data processors – such as digital platforms Google and Facebook - would enjoy the protection of the GDPR adequacy determinations by compliance with these accommodations. And twice - in actions brought by the same complainant, Max Schrems[3] - the CJEU struck down the Commission's underlying adequacy decisions,[4] as well as other aspects of the accorded frameworks. The absence of deference by the Court to the EU institution charged with the conduct of external relations is surprising; that said, the Court's assertion of the prerogative of re-assessing determinations by

* Professor of Law and Jacob Becker Fellow, Loyola Law School - Los Angeles and Guest Professor of Civil Law, Faculty of Law, Lund University.
† Professor of European Union Law at the Faculty of Law, Lund University.
A preliminary version of this article was presented at the seminar *The Consequences of Schrems II from Practical and Theoretical Perspectives* sponsored by the Swedish Network for European Legal Studies and held at the Faculty of Law, Lund University on September 16, 2021. We are grateful for the research assistance of Robert Miller.
[1] The Safe Harbour arrangements was the first mechanism permitting the export of personal data from the EU to the United States in compliance with the terms of the GDPR.
[2] The Privacy Shield arrangements permitted lawful transfers of personal data from the EU to the United States for processing by U.S.-based companies certified to be in compliance with the Privacy Shield principles under U.S. law.
[3] Max Schrems brought a series of actions with the Irish Data Protection Authority challenging the Safe Harbour and Privacy Shield. The ultimate questions in these actions were referred to the CJEU.
[4] The CJEU invalidated the Safe Harbour decision in 2015 in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650. The Safe Harbour regime was replaced by the Privacy Shield regime in August 2016. The Privacy Shield addressed some, but now all, of the defects identified by the CJEU in *Schrems I*. The CJEU invalidated the Privacy Shield regime decision on July 16, 2020 in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (*Schrems II)* ECLI:EU:C:2020:559.

EU administrative officials is a settled matter of EU law, squarely within the competence of the CJEU. It is less clear whether the Court's invocation of human rights bases for rejecting the finding of adequacy should escape external scrutiny. In *Schrems I*[5] and even more emphatically in *Schrems II*,[6] the Court strikes down accords with the United States on a basis that extends beyond mere non-conformance with the GDPR. The Court goes further - and adds EU constitutional (treaty-based) and human rights foundations to its rejection of the equivalency of the U.S. privacy / national security regimes.[7] And the Court demonstrates that a constitutional court is a blunt instrument indeed to deploy in a sensitive and significant debate between the trans-Atlantic political, economic and legal great powers. The European court may be right - but it is not necessarily right - in its world view of what human rights demands in the field of personal data privacy, and an assertion that it is the last word for the entire trans-Atlantic data space is as surprising as it is unhelpful.

There is good reason to expect a constitutional court - when faced with a measure that is pointedly extraterritorial - to take into account the interests of external actors. And a constitutional court should be prudent in projecting its constitutional reach, which should be more circumscribed than the intended reach of an ordinary regulatory measure. But this essay is not concerned with the correctness of the CJEU's decision, as an interpretive, constitutional or public international law matter. We rather make the call for awareness. The CJEU has either been insensitive to the concerns of American subjects and others with regard to the GDPR - or it has deliberately ignored them - by projecting a 'Europe First' response to the admittedly worrisome use of personal data by U.S.-based digital platforms.

The striking down of a moderating instrument resulting from negotiations between U.S. and EU officials - the Privacy Shield in *Schrems II* - by the Court can be described as a belligerent use of law - if not open 'lawfare'.[8] The EU was certainly free to act as a first mover in promulgating the GDPR; there had been no sign of legislative movement to be found within the halls of the U.S. Congress. But as a first mover, the EU legislative bodies did not intend to deprive the United States of room for manoeuvre. Indeed, the legislative/administrative/diplomatic acts of concording first the Safe Harbour and later the Privacy Shield demonstrate the desire of the Commission (at least) to enter into accommodation with the United States in the field of digital privacy. Not so the Court.

By striking down the two accommodations, the Court transformed what might have been a stimulating first action in a regulatory field into a rigid, unyielding demand. To us it appears that it is the Court, in its holdings in *Schrems I* and *Schrems II*, that converted a situation of legal conflict into an instance of legal belligerency.

Regulatory conflict is marked by (1) resistance, (2) unsustainability, (3) application of legal force and (4) pressure for de-escalation. The presence of intentionality, inflexibility and targeting indicate the belligerent use of law, arguable a form of 'lawfare.'[9] For the moment, it is difficult

[5] *Schrems I* (n 4).
[6] *Schrems II* (n 4).
[7] ibid paras 122 et seq, the CJEU extensively relying on Article 7, 8 and 47 of the EU Charter.
[8] See infra the discussion in sections 3.3. and 4.
[9] ibid.

to measure the resistance to the CJEU's latest move: *Schrems II*. American and European lawyers are hard at work to identify small and large reforms to the American privacy regime that could satisfy the Court's (rather vague) demand for equivalency of protection. General non-compliance by U.S. actors with the full force demands of GDPR is not easily observed.

The GDPR conflict with the United States is unusual in that the CJEU figures prominently. Indeed, there may not have been a dispute (at least at this point) had the Court not intervened. The entry on scene of a constitutional court - like the CJEU - may under certain conditions constitute an act of legal belligerency. Whether a court is an instrument of lawfare depends in part on what the court does - and in part on what it is capable of doing.

When a court elevates a contested regulatory feature into an incontestable constitutional norm it commits an act of extraterritorial aggression. And this, it appears, the CJEU has done in striking down successively the two EU-U.S. resolutions in *Schrems I* and *Schrems II*.

2 INTERNAL AND EXTERNAL VIEWS OF SCHREMS II

GDPR contained a conciliatory feature - a permissive equivalency test - that could have served to adjust the regulation's external effects. And through a series of adjustments (and smoke and mirrors as well), the United States was able to persuade the Commission that the U.S. privacy regime provided adequate (though not identical) protections to EU data subjects when compared to those provided them by the GDPR.[10]

An adequacy determination could be many things. It could simply be a political expediency, whereby real conflict is swept away, providing comfort to both domestic and foreign constituencies. Equivalency can be a technical exercise, where resort to different means is assessed to determine if they achieve the same desired end of legal protection. In both these cases, the first and ordinary equivalency determination is generally undertaken by an administrative (that is, executive) agency. Equivalency determinations are not ordinarily suited to judicial resolution.

2.1 SUSPICIOUS MINDS: EXTRATERRITORIALITY CONFLICT IN THE TRANS-ATLANTIC SPACE

Courts have generally played minor roles in past trans-Atlantic conflicts involving the asserted improper extraterritorial reach of one party's regulation. During the antitrust conflicts of the 1960s and 1970s, courts were given the unpleasant task of managing clawback actions that were intended to neutralize the undesired extensions of effects-based jurisdiction. One observed little judicial enthusiasm on either side of the Atlantic for the instrumental resort to courts as battlegrounds over whether U.S. Sherman Act actions should or should not reach London-based cartels. Rather, courts understood that comity, as a general principle, required a degree of legal flexibility.

[10] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.

In the 1996 Helms-Burton controversy, where the United States threatened to expose European operators of confiscated property in Cuba to harsh compensation claims by elements of the U.S.-based Cuban diaspora,[11] courts played no role at all. Helms-Burton had a safeguard built in - no legal actions under the Act were available so long as the President maintained a waiver.[12] The U.S. legal system was implicated by Helms-Burton: the essence of the threat was unleashing private litigants against European corporate interests in order to bolster adhesion to the U.S. economic embargo against Cuba. (In an act of cynical manipulation, Helms-Burton filled the heads of U.S. citizen granddaughters and grandsons of the pre-revolutionary Cuban moneyed class with delusions of recovering significant wealth from those European companies.) The Europeans resisted Helms-Burton, politically and legislatively. An EU regulation implemented a claw-back should any Helms-Burton recovery take effect. But to date, Helms-Burton has not been tested by any court, U.S., European or Canadian, given the gapless continuity of presidential waivers.

It has been a relentless feature of extraterritoriality conflicts that the offending party asserts serious internal effects of external behaviour that justify reach. And so it has been the case with the Europeans in justifying the reach of the GDPR. The entry into effect of the GDPR had been well anticipated by both American and European interests. The somewhat sophist notion of 'export' of personal data made clear the EU's intention to subject American digital giants to EU rules. Yet hard-wired into the GDPR was a mechanism to relieve some of the inevitable pressure: the GDPR, by its terms, exempted from the 'export' prohibition any data processing that occurred in countries with data protections 'equivalent' to those found in the GDPR.[13]

2.2 IDENTIFYING DISCRETION WITHIN SCHREMS II – INTERNAL VIEW

We begin with a brief recapitulation of the internal view of the *Schrems II* decision - that is, an account that would be adopted by an EU constitutional lawyer. We look at the sources of law utilized by the CJEU and at the Court's exercise of authority in reaching its judgment. We will stipulate that the Court reached a 'correct' decision when viewed from this internal perspective. There is little to gain from contesting the Court's judgment as a matter of EU law. Rather we will explore whether there existed a range of alternative determinations that the Court could have reached that would have avoided the resultant trans-Atlantic conflict. That is, we will describe (as well as we are able) the field of discretion open to the Court. We conclude – regardless of the correctness of the CJEU's judgment as a matter of EU law – the Court was not compelled to rule as it did and so could have adopted a more conciliatory stance.

---

[11] See U.S.C ch 69 A § 6021 et seq.

[12] See for development, Antonella Troia, 'The Helms-Burton Controversy: An Examination of Arguments that the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 Violates US Obligations Under NAFTA' (1997) 23 Brooklyn Journal of International law 603.

[13] European Commission, 'Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 11 December 2021.

The terms of the regulation - the GDPR - are of course binding on the Court. Absent conflict between the GDPR and some higher order EU law (such as a conflicting treaty norm), the Court is obliged to give effect to GDPR's terms. Processing of personal data requires either consent[14] or compliance with GDPR provisions. Any data transfer - internal or export - must comply with the terms of GDPR Article 6.[15] Some transfers must comply with the stricter requirements of GDPR Article 9.

But the relevant term underlying the Court's holding striking down the Privacy Shield arrangements with the United States in *Schrems II* involves the 'adequacy' determination found in GDPR Article 45.[16] Article 45(1) provides:

> A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

GDPR further outlines both substantive and procedural considerations that underlie any adequacy determination. Among the examined substantive features of the export country's legal system (here, the U.S. legal system) are its adherence to the rule of law, human rights and fundamental freedoms as well as any counterpart legislation, regulation or case-law. Among the procedural considerations is the existence of 'independent supervisory authorities'[17] charged with enforcing data privacy rules.

Again, our project in this section is to discuss zones of discretion available to the CJEU. The first involves the review the Court was compelled to apply to an extant determination by the Commission that the United States did satisfy the 'adequate level of protection' required by GDPR Article 45. It is beyond the scope of this essay to take a deep dive into the deference the Court could or should afford a Commission action either generally or in this specific instance.[18] But we imagine that the Court had a sound legal basis - had it chosen to do so - to limit its review of the Commission's adequacy decision.

Further, on a searching review of the Commission's action, the Court faced terms endowed with substantial ambiguity, which created opportunity for the authoritative interpreter (here the Court). The Court was free to give meaning to terms such as 'adequate' or 'independent' (with regard to the third country supervisory authorities) as it saw fit - and in so doing effect the resultant consequences of the Court's (as opposed to the Commission's) meaning.

---

[14] 'Consent. General Data Protection Regulation (GDPR)' (*Intersoft Consulting*,) <https://gdpr-info.eu/issues/consent/> accessed 11 December 2021.

[15] 'Art. 6 GDPR – Lawfulness of Processing. General Data Protection Regulation (GDPR)' (*Intersoft Consulting*) <https://gdpr-info.eu/art-6-gdpr/> accessed 11 December 2021.

[16] *Schrems II* (n 4) paras 168-169, para 177, paras 181-188 and paras 198-203.

[17] Insert reference to Court's assessment of U.S. compliance with independent supervisory authorities requirement.

[18] See in general on discretion given to the European Commission, Damien Geradin and Nicolas Petit, 'Judicial Review in EU Competition Law: A Quantitative and Qualitative Assessment' (2010) TILEC Discussion Paper No 2011-008, and Joana Mendes, *Executive Discretion and the Limits of EU Law* (OUP 2019).

But more than the resolution of ambiguity is demanded with regard to the adequacy decision of the Commission. The adequacy decision is a process and leads to a result. When the Court reviews the adequacy decision of the Commission, it goes beyond mere interpretation of a legislative term.

We further note the sources available (and utilized) by the CJEU in reaching its judgment in *Schrems II*. In addition to the provisions of *Schrems II,* the Court had direct access to treaty provisions, Charter provisions, and general principles in its review - and indirect access (as general principles) to the wider corpus of ultra-Charter international human rights law.[19] This approach is common not only to the recent case law of the CJEU on the GDPR[20] but also to the whole approach of the CJEU in the cases concerning digitalization in the processing of personal data such as *Privacy International*[21] and *La Quadrature du Net*.[22] This also confirms the view that the CJEU has played a major role in shaping data protection in to a proper fundamental right.[23] Moreover, GDPR Article 45 expressly directs an effectiveness evaluation of the rule of law, human rights and fundamental freedom within the United States.[24]

The demands of the 'rule of law' or 'human rights' or 'fundamental freedom' are fluid, to say the least.[25] There can be no doubt that the CJEU is an authorized and respected juridical voice in contributing meaning to these categories of legal norms. It is precisely because the CJEU enjoys the status of a world-class articulator of these norms[26] that it enjoys discretion in its application of these norms. Since *Schrems I,* the Court is keen to link the protection of EU Charter to the rule of law problematic defines as *État de droit*[27] and thus propelling a substantive rule of law in the legal order of the European Union.[28] We suggest that the Court could have found in its evaluation of the U.S. data privacy regime compliance with the GDPR's effectiveness mandate without betraying a cogent adherence to the rule of law, human rights and fundamental freedom. Here too was present discretion that could have been exercised in a different way.

---

[19] *Schrems II* (n 4) and (n 8).
[20] ibid.
[21] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (Privacy International)* ECLI:EU:C:2020:790.
[22] 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. See in this volume, for an assessment of the negative reaction of the French national supreme court to the CJEU answer, Araceli Turmo, 'National Security Concerns as an Exception to EU standards on Data Protection' (2021) 4(2) Nordic Journal of European Law, 86. According to her, 'The French Government had in fact encouraged the French supreme court to go down the same path in reaction to *La Quadrature du Net*, in order to preserve French regulatory provisions allowing the indiscriminate gathering and retention as well as relatively unrestricted access to this metadata by security and intelligence services'.
[23] Susanna Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021), 11.
[24] *Schrems II* (n 4).
[25] Xavier Groussot and Gunnar Thor Petursson, 'Je t'aime moi non plus: Ten Years of Application of the EU Charter of Fundamental Rights' (2022) 59(1) CMLRev (forthcoming).
[26] ibid.
[27] *Schrems I* (n 4) para 95.
[28] See Paul Craig, 'Formal and Substantive Concepts of the Rule of Law: An Analytical Framework' [1997] Public Law 467, and Xavier Groussot and Johan Lindholm 'General Principles: Taking Rights Seriously and Waving the Rule-of-Law Stick in the European Union' in Katja Ziegler and others, *Research Handbook on General Principles in EU law: Constructing Legal Orders in Europe* (Edward Elgar 2022) (forthcoming).

At this point, we cannot resist making a comparative comment. U.S. constitutional principles require courts - where they enjoy discretion - to exercise their discretion in a manner that supports both the determinations of the administrative agencies they are reviewing (*Chevron* doctrine)[29] and in a manner consistent with international legal obligations (*Charming Betsy* doctrine)[30] that arguably would have included the Privacy Shield arrangements between the EU and the United States.

In concluding our remarks here on the internal correctness of the Court's judgment in *Schrems II*, the telling inquiry is not whether the Court was correct in the judgment it reached - but rather would the Court have been correct in reaching an alternative disposition of the matter. If an alternative judgment were available to the Court that would have preserved the Privacy Shield, it then becomes a matter of external scrutiny whether the Court should have acted differently. We suggest that the Court had not been legally compelled to reach the conclusion it reached in *Schrems II* - without in our so doing asserting any internal legal error in its judgment.

2.3 IDENTIFYING DISCRETION WITHIN *SCHREMS II* – EXTERNAL VIEW

We restate our view that the CJEU is presumptively correct in its holding in *Schrems II* as a matter of internal EU law. This would be true, of course, of any judgment of the CJEU with regard to a question of EU law and results from the primacy of the Court within the EU legal system. The inherent correctness of the CJEU in *Schrems II* does not, however, insulate it from critique or disregard from external vantages, at least with respect to definitions and applications involving those categories of norms that are located in shared legal space. It is open season for the Americans and others to challenge the Court's resort to rule of law, human rights law and fundamental freedoms, as the CJEU is far less privileged in these domains than it is within the EU law closure.

There are certainly many areas of rule of law or human rights or fundamental freedom analysis that have been fleshed out by courts and tribunals throughout the world. But within the specific domain of the protection of personal data, there is thin law at best. Indeed, the very best positive law in this field is the GDPR and other European legal initiatives. But Europe, as the sole or primary occupant of this specific legal domain, can hardly claim that its proprietary approaches deserve global (or universal) recognition as constituent features for human rights law. There is certainly a first mover advantage in many fields of international law, but Europe's pioneering foray into data privacy rights does not make the GDPR a *de facto* standard against other approaches (or non-approaches) adopted by other nations.

What then might international human rights law (or rule of law or fundamental freedoms) demand of the United States with regard to the protection of personal data? At the moment,

---

[29] 'If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress...if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute' - *Chevron U.S.A. v. Natural Res. Def. Council*, 467 U.S. 837, 104 S. Ct. 2778 (1984).

[30] '[A]n act of Congress ought never to be construed to violate the laws of nations if any other possible construction remains' - *Murray v. Schooner Charming Betsy*, 6 U.S. 64 (1804).

there is no recognition of any such obligation by the U.S. Congress. Not only is there no relevant legislation, there are no visible legislative proposals in the pipeline. A few states - notably California - have been inspired by Europe's GDPR to adopt state-level data protection regimes, but most states have been as silent as the federal government itself. It is of course harder to read Congressional inaction than action, but it appears that the current state of American law and practice is one of non-recognition of any obligation to protect interests in personal data. This may, of course, change.

There may, however, be a Trans-Atlantic view (in contrast to either the European regulatory or U.S. *laissez-faire* stances) that deserves recognition, and that is the law expressed by the now-discarded Privacy Shield! The United States, through the act of negotiating a framework for trans-Atlantic data traffic, implicitly conceded a good part of the GDPR's international legitimacy. This concession may have been driven more by the realities of power (think Brussels Effect)[31] than by recognition of the intrinsic legitimacy of the European policy choices. We assert that it would be easier to claim the Privacy Shield represented the stance of international human rights law than the unadulterated GDPR itself.

3 LOCATING *SCHREMS II* ON THE SCALE OF BELLIGERENCY

3.1 THE CONFLICT / COORDINATION / COOPERATION SPECTRUM

The GDPR conflict between the European Union and the United States is first a legal conflict. The field describing the multiple exercise of what international lawyers call prescriptive jurisdiction - the application of law to regulate the conduct of a legal person - is known as private international law in most legal systems, although common lawyers recognize the area with the more evocative name 'conflict of laws'. But the GDPR conflict is also an economic and perhaps cultural conflict. There is a strand of conflict of law classification that it considers a predicament to be 'no true conflict' where a legal subject can comply fully with the demands of one relevant legal system without violating the demands of the counterpart legal system.

The 'no true conflict' scenario includes the frequent situation where one state proscribes behaviour that the other state does not address. Using this test, GDPR presents 'no true conflict'. Roughly speaking the GDPR constrains the ability of Google or Facebook to export personal

[31] See in general Anu Bradford, *The Brussels Effect: How the European Union Rule the World* (OUP 2020). In her book, she shows the great power of EU law to influence the regulation of legal standards outside Europe. Her main argument is that EU law made in Brussels can set the legal standard of protection worldwide in many law fields such as competition law, health law, consumer safety, data privacy and artificial intelligence. The 'Brussels Effect' reveals the EU's unique power to influence global corporations and set the rules of the game while acting alone what she calls a 'unilaterally regulatory globalization'. EU law, due to its regulatory and legal strength, acts here as a soft power. The situation is comparable to the so-called 'California Effect 'where the Californian environmental standards can influence the rest of the US legislation due to the strong market power of the State of California in the US federation'. According to Bradford, four conditions are necessary to ensure the effect: 1) the existence of a very large economic market with enforcement power 2) a regulatory capacity with a preference to enact stricter rules 3) specific areas/policies used as regulatory targets 4) the need of non-divisible legal standards for the companies. EU is seen as a soft power which can influence without coercion the world legal standards. This regulatory and legal expansion is clearly connected to the existence of the *lex mercatoria*.

data from the EU for processing in the United States; the ordinary operation of these platforms involves the processing of personal data as that notion is defined in the GDPR. Google or Facebook could fully comply with the GDPR export limitations by desisting from any data export. By so doing, Google or Facebook would not violate any conflicting U.S.-based legal mandate. The problem of course is that Google and Facebook wish to export EU-based personal data.[32] Regulatory conflicts can be resolved. There is a spectrum that runs from true conflict (where the legal subject is caught between conflicting demands) to complete elimination of conflict through cooperation, such as by resort to a mirror-image (uniform) rule or the construction of a common rule shared within a higher legal space superimposed on two otherwise independent sovereign regimes. A fully cooperative resolution may more closely match the regulatory imperatives of one state than the other. At one extreme, the 'cooperative' solution might be a complete capitulation of one state to the regulatory choices of the other.

3.2 COOPERATION AND COORDINATION IN REGULATORY CONFLICTS

There are a variety of cooperative techniques available to the EU and the United States to resolve the GDPR conflict. Notwithstanding Europe's assertion of a first-mover advantage in the field of the protection of personal data rights, the United States and Europe could work toward eliminating conflicts and inconsistencies in this area. This might take the form of harmonization, where both the United States and Europe would adjust their current regulatory positions according to a common design. Under certain conditions, regulatory convergence can arise spontaneously, gradually resolving past conflict, as occurred in the field of corporate payments to foreign public officials.

As a formal alternative, the EU and the United States could have elevated the protection of personal data to a bilateral, multilateral, or global instrument. A cooperative promotion of a global standard based on a common EU - U.S. position with regard to the protection of personal data would likely attract the adhesion of many other countries (although perhaps not China).

And finally, data protection may be an area ripe for what we have described elsewhere as 'trans-Atlantic bicameralism',[33] where the first initiative in a particular regulatory space (here the GDPR) is understood to be a functional proposal, to be accepted, rejected or amended by the trans-Atlantic counterparty. The next move, under this modality, would be for the United States to enact legislation adopted some or all of the GDPR (as it sees fit), with any remaining conflict eliminated through a process of reconciliation. Europe then would amend GDPR accordingly.

Cooperation is not an inevitable result, of course. The first-mover advantage can yield enduring benefits to the state that occupies a vacant regulatory space that touches multiple jurisdictions. Having enacted GDPR earlier than the emergence of any other data privacy regime, the EU both occupied the field and set the standard for all states which follow. The GDPR was

[32] See also many litigations of the CJEU concerning Google and Facebook. See, eg, recently the pending Case C-329/20 *Facebook Ireland,* and Opinion of Advocate General de la Tour (ECLI:EU:C:2021:97) in this case concerning consumer protection and Article 80 GDPR.

[33] Jeffery Atik and Xavier Groussot, 'The Draft EU AI Regulation: Strategic Bicameralism in the Shadow of China' (2021) 72 EU Law Live Weekend Edition 2.

designed to be global standard - and its insistence of adequacy and equivalency were designed to puncture less robust protections.

Coordination is a regulatory state intermediate between cooperation and conflict, where the first-movant preserves adequate policy space for alternative approaches. Follow on actors can adopt a variety of approaches where coordination remains available. Yet this is not the case for the GDPR, other than in the solution where data processing is fragmented between intra-European and extra-European spaces.

3.3 REGULATORY CONFLICT

In its native state, the GDPR likely introduced a conflict with the United States.[34] The CJEU's judgments in *Schrems I* and *Schrems II* have inflamed that conflict. We argue that law can be used belligerently.[35] This is a notion that grows out of the lawfare tradition that identifies an instrumentalized resort to law in order to achieve extra-legal goals, including policy dominance in our view.[36] Lawfare is a nascent (often contested)[37] terminology that should in our view deserve more academic attention.[38] The concept of lawfare fits the issue of regulatory conflicts revealed by the CJEU case law,[39] where the EU court tests the adequate level of protection required by Article 45 of the Charter in light of the EU Charter.[40] *Schrems I* and *Schrems II* constitute in fact litigations where there is no consensual issue available to solve the regulatory conflicts due to the extensive interpretation of the fundamental right enshrined in the EU

[34] See Bradford (n 31).

[35] David Kennedy, *Of War and Law* (Princeton University Press 2006). See also Orde F Kittrie, *Lawfare: Law as a Weapon of War* (OUP 2016); Congyan Cai, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (OUP 2019).

[36] Charles J Dunlap Jr., 'Does Lawfare Need and Apologia?' (2010) 43 Case Western Reserve Journal of International Law 121. The term 'lawfare' is employed in the field of international law by US and Chinese scholars since the last two decades. And it has now been used for the very first time in Europe on the 15th of June 2020 by a leading scholar in European Union external relation law and governance - see Steven Blockmans, 'Why Europe Should Harden Its Soft Power to Lawfare' (*CEPS blog*, 15 June 2020) <https://www.ceps.eu/why-europe-should-harden-its-soft-power-to-lawfare/> accessed 11 December 2021.

[37] See Wouter G Werner, 'The Curious Career of Lawfare' (2010) 43 Case Western Reserve Journal of International Law 61. See also Leila Nadya Sadat and Jing Geng, 'On Legal Subterfuge and the So-Called "Lawfare' Debate"' (2010) Case Western Reserve Journal of International Law 153. As put by them: 'There are many nuances to the term, though lawfare is generally defined as a tactic of war where the use of law replaces the use of weapons in the pursuit of a military objective. Lawfare proponents increasingly claim that adversaries of the United States are manipulating the rule of law to undermine democracy and national security'. See also Scott Horton, 'The Dangers of Lawfare' (2010) 43 Western Reserve Journal of International Law 163. For him, the term of lawfare is ideologically charged.

[38] There is in our view a need to build strong theoretical/conceptual foundations of lawfare since it reveals the real nature of our time, a time of big politics. This is the zeitgeist of our time. See for a recent use of the concept of lawfare in the context of the backsliding of the rule of law in Europe, Jeffery Atik and Xavier Groussot, 'Constitutional attack or political feint? - Poland's resort to lawfare in Case K 3/21' (*EU Law Live,* 18 October 2021) <https://eulawlive.com/op-ed-constitutional-attack-or-political-feint-polands-resort-to-lawfare-in-case-k-3-21-by-jeffery-atik-and-xavier-groussot/> accessed 11 December 2021.

[39] See in *Schrems II* (n 4) paras 168-177.

[40] *Schrems II* (n 4 and n 16).

Charter, in particular the right to data protection as defined in Article 8 of the EU Charter.[41] These litigations show, arguably, that there is no neutrality of the CJEU in assessing the (euro-)rights are issue.[42]

Extraterritorially effective law is peculiarly objectionable when the enacting state has power - and there can be no mistaking the exercise of European power in the GDPR controversy. (The general exercise of European regulatory power is popularly known as the 'Brussels Effect').[43] A powerful state can impose its legal power by adopting a law suited to its interests and projecting its effects outside its borders. This may be a fair characterization of what the EU has done with the GDPR even before its hardening by the CJEU in *Schrems I* and *Schrems II*.

Conflict results when one partner makes law and precludes the other from freely making alternative regulatory choices. There are several markers of regulatory conflict that we can observe. The first is resistance. There was observed resistance to the GDPR by U.S. interests long before the regulation came into effect. And it remains an open question how deep compliance by U.S. firms with GDPR may be in practice; non-compliance is after all a form of resistance. And the energetic response by U.S. officials in negotiating the Safe Harbour and Privacy Shield arrangements with an eye to denaturing the more ambitious features of the GDPR further signals an underlying resistance.

4 A WEAPONIZED CJEU

4.1 THE BELLIGERENT USE OF LAW

One of the given premises of this article is that the CJEU decided *Schrems II* correctly as a matter of European law. That is, the question it was called upon to answer by the referring Irish High Court was within its authority (competency) and that its answer (the judgment itself) was supported by appropriate source law, including its resort to Charter and other treaty provisions as well as relevant general principles, including fundamental freedoms and other human rights notions.

We have further asserted that the CJEU might have reached equally correct (but different) conclusions, consistent with EU law including its higher law, that would have better contributed to locating a cooperative solution to the legal conflict arising within the concurrent jurisdiction occupied by both the EU and the United States.

We now propose that the judgment of the CJEU in *Schrems II* constitutes a belligerent use of law. And to do this, we now need to explore what we see to constitute a belligerent use of law. We use this phrase - belligerent use of law - to invoke at least part of the 'lawfare' tradition

[41] See for development Larry Yackle, *Regulatory Rights: Supreme Courts Activism, The Public Interest and the Making of Constitutional law* (University of Chicago Press 2007). See also for contrasting the GDPR with the proposed EU Regulation on Artificial Intelligence, Atik and Groussot, 'The Draft EU AI Regulation' (n 33).
[42] Lindroos-Hovinheimo (n 23) 27. The author considers the impossibility of neutrality in the situation of balancing of rights.
[43] See Bradford (n 31).

- which categorizes certain legal uses that are improperly instrumentalized to serve purposes beyond the ordinary objects of law.[44] In our view, an extraterritorial conflict arising from the predicament of concurrent jurisdiction is ripe for this kind of abuse.

Law-making inevitably involves a projection of power by the law-making state. It is first and foremost an internal exercise of power over the subjects of that state. But it also, to a lesser or greater degree, constitute an assertion of power outside the Westphalian territorial bounds.[45] International law tolerates the extension of a law's effect beyond the territorial limits of the imposing states under certain conditions. Comity, as an independent mediating principle, counsels moderation in any extraterritorial extension as well as consideration of the regulatory interests of any other state co-occupying a particular regulatory space. As such, there must be additional elements that constitute a particular exterritorial extension 'belligerent' to avoid the term simply serving as a pejorative equivalent.

Intention can and should play a role in defining when a use of extraterritorial law is properly described as belligerent. Extraterritorial effect is often an inadvertent feature of regulatory design, an unintended spillover. Or an extraterritorial reach is intended to eliminate or reduce simple evasion or circumvention by actors presumptively subject to the regulation. The mere fact of extraterritorial effect cannot, in itself, be fairly described as belligerent.

Where a state imposing a regulatory scheme with extraterritorial effect that it intends to serve as a global standard (as opposed to a mere territorial approach among alternate possible approaches) this changes. Imposing a particular regulatory design on others deprives those others from appraising the regulatory space and selecting alternate approaches. When this is done intentionally, the end result extends beyond maximizing the legal effectiveness of one's own regime. Intentionally imposing one's regulatory responses achieves political ends, not legal ends.

The second indicator of belligerency is inflexibility. An unwillingness to adjust the projected regulatory approach to the needs and concerns of others suggests the presence of an aggressive intent. As we will note in the next section, supporting particular legal choices on a country's constitutional vision necessarily produces inflexibility. The degree of flexibility may not be apparent - as cultivating an illusion of strong commitment to a regulatory approach may bring a strategic advantage. But removing an extraterritorial legal regime from one of ordinary law to one founded on constitutional principles produces real rigidity. It is very difficult for a state that uses constitutional justifications for its policy designs to alter those designs. In the case of *Schrems II* - again as we will argue below - it is the CJEU that transforms the demands of a piece of ordinary legislation - the GDPR - into an uncompromising constitutional demand.

A third indicator is targeting regulatory subjects that are located extraterritorially. If the regulatory targets are asymmetrically distributed, disregard of the regulatory choices of the co-habiting states is more problematic.

---

[44] See generally on the issue of instrumentalization of law, Brian Z Tamanaha, *Law as a Means to an End: Threat to the Rule of Law* (CUP 2006).

[45] For a discussion on power, see, eg, David Dyzenhaus, 'Lawyers for the Strongman' (*aeon*, 12 June 2020) <https://aeon.co/essays/carl-schmitts-legal-theory-legitimises-the-rule-of-the-strongman> accessed 11 December 2021. The author discusses *inter alia* the use of law by lawyers like Carl Schmitt.

Where these features are present - intention, inflexibility and targeting - extraterritorial extension of a regulatory program can be described as hostile or belligerent. Belligerency suggests a war-like state - but does not necessarily mean that the state which makes belligerent use of law is acting wrongfully. This ultimate consideration requires further inquiry as to whether the resort to the belligerent use is justified - and whether the belligerent use of law involves legitimate means - additional features that will be considered in the following sections of this article.

4.2 A CONSTITUTIONAL COURT AS AN INSTRUMENT FOR TRANS-ATLANTIC REGULATORY CONFLICT

The CJEU cannot be critiqued for responding to the reference in Max Schrems' case before the Irish authorities.[46] Clearly the referring court required guidance from the CJEU to assess Mr. Schrems claim that the Regulation implementing the Privacy Shield arrangements with the United States were outside of the bounds of EU law.[47] The Court was likely compelled to enter the fray. Yet the Court need not have acted as it did in reaching its judgment in *Schrems II*. As we argue in the prior section, there was ample discretionary space for the Court to have reached a differing result. And further, there was ample alternative grounds for the Court to have reached the same result it did.

There is an inherent escalation of an international legal conflict whenever a constitutional court enters play. And the escalation is significantly enhanced when a constitutional court rests its judgment on constitutional or international law grounds.

In *Schrems II* the Court was asked to review the adequacy decision of the Commission that supported the Privacy Shield and its implementation in EU law.[48] Article 45 of the GDPR does dictate the Commission to consider the presence of the Rule of Law, observation of international human rights and the respect for fundamental freedoms. Yet the Court chooses to disregard the Commission's assessment of these and other factors in concluding that the United States provided 'adequate' protection to the data privacy concerns of EU citizens.[49]

We move now from what could have been to what happened in *Schrems II*. The CJEU inserted itself into the trans-Atlantic conflict over the asserted extraterritorial effects of the GDPR in *Schrems II*.[50] In invalidating the Privacy Shield arrangements based on its assessment of the adequacy of data protections provided by the U.S. certified data processors on a mix of human rights and fundamental freedoms principles, the Court not only struck a blow for maintaining the European notion of data privacy, it locked the EU into a position from which few concessions could be made.[51]

---

[46] See in this volume, for an in depth analysis of the national proceeding, Graham Butler, 'Lower Instance National Courts and Tribunals in Member States, and Their Judicial Dialogue With the Court of Justice of the European Union' (2021) 4(2) Nordic Journal of European Law, 19.
[47] ibid.
[48] See *Schrems II* (n 4, n 7 and n 16).
[49] ibid.
[50] ibid.
[51] ibid.

Entry by a constitutional court and recourse by a court to constitutional and international law grounds for a determination rejecting an agreed solution to a conflict involving concurrent jurisdiction the court imposed rigidities that the executive arm (here the Commission) cannot easily relax. In so doing, the Court diminishes the prospect of any cooperative solution. Accommodation or coordination becomes more complex and costly to achieve. And an enduring conflict - with attendant suspicions, hostility and recriminations - is likely to result.

In *Schrems II*, the Court held that a key element of the Privacy Shield, resort to standard contract clauses, had to ensure data subjects a level of protection essentially equivalent to that provided by the GDPR and the EU Charter of Fundamental Rights.[52] The GDPR is ordinary law, a regulation promulgated by the legislative/administrative organs of the EU, whereas the Charter is constitutional in rank.[53]

It is very difficult, if not impossible, to bargain with the CJEU. This is true for the U.S. side in any post-*Schrems II* negotiations. It is also true for the Commission who cannot suggest potential conciliatory approaches without again risking the embarrassment of having its work tossed out by the CJEU. Having inserted itself twice in the muddle and having declared that any resolution of the conflict must meet an uncertain constitutional evaluation, the Court has significantly limited the room for manoeuvre for the Commission (which is, of course, generally charged with the conduct of external affairs).

The United States now faces the EU as both an unreliable and inflexible adversary in reaching any accommodation of the GDPR's demands with regard to U.S.-based data processing. The Court's action - striking down prior agreements reached with the Commission - make it difficult to take the Commission's proposals (or concessions to U.S. proposals) seriously, even when tendered in good faith. And to the degree that Court has established - as it seems it has - that ultimate appraisal of U.S. data protections will be measured against Charter standards (with the CJEU the ultimate specifier of what those standards are) sharply reduces the space for compromise or conciliation.

4.3 'JUST WAR' LIMITS ON THE BELLIGERENT USE OF LAW BY A CONSTITUTIONAL COURT

We have made two principal assertions at this point. The first is that the Court could have minimized its effect on the U.S.-EU bargain, either from exercising its discretion to provide for a more cautious outcome, or - while preserving the outcome it reached - by basing its judgment on ordinary law (ie, GDPR) grounds as opposed to far more rigid constitutional (eg, Charter and human rights) grounds. The second assertion is that the Court has acted belligerently by intervening in the trans-Atlantic dialogue over the proper extraterritorial extension of EU regulatory policy and imposing a purely European judgment that did not take into account U.S. interests.

---

[52] *Schrems II* (n 4).

[53] See the text of Article 6 TEU and Article 289 TFEU.

We now address whether there should be limits on a constitutional court to propel its constitutional and human rights vision into a zone where comity is understood to play a role. We have termed the CJEU's role in the trans-Atlantic dispute over the proper scope of data protection belligerent. By this we intend to characterize the Court's action as aggressive and unilateral. In so doing we deliberately invoke at least some of the 'lawfare' literature that describes the improper use of law to achieve strategic outcomes.[54]

The CJEU's judgment in *Schrems II* may contribute to achieving Europe's goal of converting what nominally is a European approach into the de facto global standard for the protection of personal data. *Schrems II* vaults the undiminished GDPR as an unavoidable constraint on any global actor in the digital space. And - if the effect of *Schrems II* is to make satisfaction of GDPR's adequacy requirement or the Charter's equivalency requirement elusive, the CJEU may have shut down the possibility of any export of EU-sourced personal data - a result that goes beyond the clear design of the GDPR (which anticipates the export of personal data under certain conditions).

We suggest that the law of war may provide limits to what the CJEU or any constitutional court might do, inspired by counterpart limits within the law of war tradition.[55] Before doing so, we recall that scenarios involving concurrent jurisdiction - from the case of the *Lotus* onward - require a comity analysis and not a bull-headed insistence by a court that its internal views dominate the interests of the counterparty.[56]

In its traditional structure, the law of war divides between *jus ad bellum* (which addresses the justness of engaging in war) and *jus in bello* (which sets the limits on just means in armed conflict). This is a useful model for exploring possible limits on lawfare conducted by a constitutional court such as the CJEU. Let us first engage in an exploration of the circumstances where resort to lawfare may be considered just.

In a regulatory conflict that arises between two states enjoying concurrent jurisdiction, the ordinary expectation would be a joint and cooperative search for an arrangement that satisfies in part the expectations of each. A peaceful outcome results from what is an essentially political (diplomatic, if you will) process, involving political institutions. Resolution of regulatory conflicts need not, and in most cases should not, feature the intrusion of a judicial body from one of the contesting parties. There are compelling reasons sourced in institutional competence, access to information and pragmatics that make judicial intervention undesirable.

Of course, there are sound justifications for the entry of a court where legal interests are disregarded. Again, whether the Commission disregarded the rights of EU citizens in their personal data is beyond our evaluation. But the internal legal conditions that legitimates a court's

---

[54] See Kennedy (n 35) and Kittrie (n 35). Kittrie considers that lawfare is traceable to Hugo Grotius and his book *Mare Liberum*, published in 1609. In this book, he argues that under 'the Law of Nations the sea is common to all', 'that through it the Dutch accomplished what their naval and military forces could not, and they thereby "solidified the concept of freedom of the seas"'. That was to the benefit of the Dutch Indian Companie, which financed Grotius research. Though history, many examples can be found where the law is strategically used to achieve 'security objectives'.

[55] ibid.

[56] The Case of the S.S. 'Lotus' (France v. Turkey)*, 7 Sept. 1927, PCIJ, Ser. A., No. 10, 1927*. See for a discussion on cooperation, Wolfgang Friedmann, *The Changing Structure of International Law* (Columbia University Press 1964), 63.

intrusion can simultaneously represent an aggressive wrecking of a political solution that inflicts harm on at least one party - and perhaps both.

And so a potential *jus ad bellum* norm would caution a constitutional court in an ongoing conflicted concurrent jurisdiction scenario to refrain from engaging what might be idiosyncratic principles (or idiosyncratic interpretation of principles) unless there was some justificatory threat from the rival jurisdiction. We are open to the possibility that this might in fact be the case regarding the protection of personal data given the evident disinterest in the U.S. Congress to engage the policy space. Much as self-defence is long understood to justify resort to war, so too might certain provocations (or perhaps regulatory irresponsibility) justify a constitutional court from asserting its values without regard to comity considerations.

A justified war cannot be fought without limits as to means. *Jus in bello* operates independently of *jus ad bellum*. Again, by analogy, even were the intervention by the CJEU in this dispute to be fully justified, it does not follow that the means the Court utilizes are necessarily justified.

Two notions dominate the law of war as to just means: discrimination and proportionality. Discrimination addresses the requirement that force be confined to lawful targets; in its negative form, discrimination requires that force not be directed as a broad category of protected targets of the adversary (civilians, hospitals, combatants *hors combat*, etc.). A norm of discrimination in a 'lawfare' context might require recognition of certain core values (the U.S. Second Amendment, perhaps, to make a grotesque example) even when those values are not shared in the constitutional or fundamental freedom tradition of the intervening court. But there is little here to suggest that the CJEU was striking any core value of the United State in denying effect to the Privacy Shield.[57]

Proportionality, as an analogue concept, may have more purchase in the case of lawfare.[58] Proportionality here would involve a balancing of interests between the objective of the imposed law (here the protection of the interests of EU citizens sharing personal data) and the legitimate harm to U.S. interests.[59] In principle, some weight should be given to the *laissez-faire* regulatory stance of the United States. It may reflect a considered policy judgment that is entitled to some regard. Merely securing the profits (or worse, dominant positions) of Google or Facebook is another matter. These palpable interests may not be entitled to legal protections (outside of, perhaps, the currently moribund WTO regime).

---

[57] See *Schrems II* (n 4).

[58] See in this volume, Ester Herlin-Karnell, 'EU Data Protection and the Principle of Proportionality' (2021) 4(2) Nordic Journal of European Law, 66. According to her, 'many scholars have, of course, been interested in proportionality for a long time and there are very good reasons for such an extensive interest in the contours of proportionality'. In this article, we are linking the concept of proportionality to the nascent concept of lawfare.

[59] ibid. According to her: 'The notion of proportionality is of course a golden rule in EU law. The principle of proportionality in EU law is taken to mean balancing the means and ends, in which the notion of appropriateness constitutes the golden thread for deciding on the desirability and need for EU action. Thus, proportionality is a classic in EU law and is one of the most crucial general principles, one which is used both as a sword and as a shield, usually in the context of to what degree the Member States could derogate from their EU law obligations. But it also constitutes one of the leading principles for deciding on whether EU legislative competence is warranted'.

In EU law, the requirements of proportionality and discrimination can be viewed as ideologically loaded (non-neutral) concepts[60] as it resorts from a general analysis of their use through time in the CJEU case law; their use sometimes leading to broad discretion, sometimes not.[61] Looking at their jurisprudential and historical application by the Luxembourg Court, litigations on proportionality and discrimination do often reflect the various policy approaches taken by the CJEU[62] in a specific period of times that crystalize the understanding of the Court's activity as centralized/uniting or decentralized/diversifying.[63] Whereas these two constitutional principles/requirements can both foster centralization and decentralization in the EU legal order, in recent years, perhaps due to the impact of the many crises in Europe,[64] the CJEU case law exhibits strong elements of centralization and effectiveness that influence the level of discretion and tend to limit it in turn.[65]

To some degree, the requirements of discrimination and proportionality have a greater procedural effectiveness than substantive effectiveness. Battlefield liability results from command failures to consider the demands of discrimination or proportionality, rather than decisions that prove to have violative effects. Here the model would have asked the CJEU to reflect on whether the judgment reached in *Schrems II* unlawfully touched core interests of the United States (failure to discriminate) or whether its protection of European interests was outweighed to the burden the decision imposes on U.S. interests (proportionality). It may be that the CJEU's action could be defended as a substantive matter; its failure to fully reflect on effects on U.S. interests might condemn the judgment regardless.[66]

5 CONCLUSION

The CJEU, in *Schrems II*, could have taken a more conciliatory stance. It likely had the discretion to avoid striking down the Privacy Shield arrangements. And – even if it had been determined to invalidate the Privacy Shield, it could have confined the grounds to ordinary law. Instead, the CJEU acted as a magnificent constitutional court, exercising its authority over other EU institutions and resting its judgment importantly on Charter (that is, constitutional) grounds. In our view, the CJEU came crushingly into a conflict, as opposed to deftly avoid it. And within

---

[60] Joxerramon Bengoetxea, 'Rethinking EU Law in the Light of Pluralism and Practical Reason', in Miguel Maduro and others (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (CUP, 2014) 145, 147. Bengoetxea refers to ideological coherence as being characterized by the values of the body politic as stated in and interpreted from the constitution.

[61] Gunnar Thor Petursson, *The Proportionality Principle as a Tool for Disintegration in EU Law – of Balancing and Coherence in the Light of the Fundamental Freedoms* (PhD Dissertation, Lund University 2014), see in particular ch 10, 235 et seq.

[62] Xavier Groussot, *General Principles of Community Law* (Europa Law Publishing 2006), see ch 3, 126 et seq.

[63] ibid.

[64] See generally on the issues of legality and crises, David Dyzenhaus, *The Constitution of Law: Legality in a Time of Emergency* (2nd edn, CUP 2013).

[65] Xavier Groussot and Anna Zemskova, 'The Rise of Procedural Rule of Law in the European Union - Historical and Normative Foundations' in Antonina Bakardjieva-Engelbrekt and others (eds), *The Rule of Law in EU: Thirty Years after the Fall of the Berlin Wall* (Hart Publishing 2021) 267.

[66] *Schrems II* (n 4).

the conflict – an extraordinarily important conflict with the United States – the CJEU has acted belligerently.

Constitutional values of one party are ill-suited to satisfactorily resolve a legal conflict between two parties. A constitutional court, such as the CJEU – that sees its own law and not that of the counterparty to the conflict – makes reconciliation and resolution far less likely. Europe may 'win' this contest with the United States – and the CJEU's judgment in *Schrems II* may contribute to its policy success. But such a 'win' reflects the exercise of power more than law.

LIST OF REFERENCES

Atik J and Groussot X, 'The Draft EU AI Regulation: Strategic Bicameralism in the Shadow of China' (2021) 72 EU Law Live Weekend Edition 2.

— —, 'Constitutional attack or political feint? -Poland's resort to lawfare in Case K 3/21' (*EU Law Live,* 18 October 2021) <https://eulawlive.com/op-ed-constitutional-attack-or-political-feint-polands-resort-to-lawfare-in-case-k-3-21-by-jeffery-atik-and-xavier-groussot/> accessed 11 December 2021.

Bengoetxea J, 'Rethinking EU Law in the Light of Pluralism and Practical Reason' in Maduro M and others (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (CUP 2014). DOI: https://doi.org/10.1017/cbo9781139236041.009

Blockmans S, 'Why Europe Should Harden Its Soft Power to Lawfare' (*CEPS blog*, 15 June 2020) <https://www.ceps.eu/why-europe-should-harden-its-soft-power-to-lawfare/> accessed 11 December 2021.

Bradford A, *The Brussels Effect: How the European Union Rule the World* (OUP 2020). DOI: https://doi.org/10.1093/oso/9780190088583.001.0001

Butler G, 'Lower Instance National Courts and Tribunals in Member States, and their Judicial Dialogue with the Court of Justice of the European Union' (2021) 4(2) Nordic Journal of European Law 19.

Cai C, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (OUP 2019).
DOI: https://doi.org/10.1093/oso/9780190073602.001.0001

Chander A, 'Is Data Localization a Solution for Schrems II? Journal of International Economic Law', September 2020.

T Christakis, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers'. European Law Blog, November 2020.

Craig P, 'Formal and Substantive Concepts of the Rule of Law: An Analytical Framework' [1997] Public Law 467.

C Docksey, 'Schrems II and Individual Redress - Where There's a Will, There's a Way. Lawfare, October 13, 2020.

Dunlap C J, 'Does Lawfare Need and Apologia?' (2010) 43 Case Western Reserve Journal of International Law 121.

Dyzenhaus D, *The Constitution of Law: Legality in a Time of Emergency* (2nd edn, CUP 2013).

H Farrell and A Newman, 'Schrems II Offer an Opportunity - if the U.S. Wants to Take It'. Lawfare, July 28, 2020.

Friedmann W, *The Changing Structure of International Law* (Columbia University Press 1964).

Geradin D and Petit N, 'Judicial Review in EU Competition Law: A Quantitative and Qualitative Assessment' (2010) TILEC Discussion Paper No 2011-008.
DOI: https://doi.org/10.2139/ssrn.1698342

Groussot X and Lindholm J, 'General Principles: Taking Rights Seriously and Waving the Rule-of-Law Stick in the European Union' in Ziegler K and others, *Research Handbook on General Principles in EU law: Constructing Legal Orders in Europe* (Edward Elgar 2022) (forthcoming).

Groussot X and Petursson G T, 'Je t'aime moi non plus: Ten Years of Application of the EU Charter of Fundamental Rights' (2022) 59(1) CMLRev (forthcoming).

Groussot X and Zemskova A, 'The Rise of Procedural Rule of Law in the European Union - Historical and Normative Foundations' in Bakardjieva-Engelbrekt A and others (eds), *The Rule of Law in EU: Thirty Years after the Fall of the Berlin Wall* (Hart Publishing 2021).

Herlin-Karnell E, 'EU Data Protection and the Principle of Proportionality' (2021) 4(2) Nordic Journal of European Law 66.

Horton S, 'The Dangers of Lawfare' (2010) 43 Western Reserve Journal of International Law 163.

Kennedy D, *Of War and Law* (Princeton University Press 2006).

Kittrie O F, *Lawfare: Law as a Weapon of War* (OUP 2016).

Lindroos-Hovinheimo S, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021).
DOI: https://doi.org/10.1017/9781108781381

Mendes J, Executive Discretion and the Limits of EU Law (OUP 2019).

Petursson G T, *The Proportionality Principle as a Tool for Disintegration in EU Law – of Balancing and Coherence in the Light of the Fundamental Freedoms* (PhD Dissertation, Lund University 2014).

K Propp and P Swire, 'After Schrems II: A Proposal to Meet the Individual Redress Challenge'. Lawfare, August 13, 2020.

Sadat L N and Geng J, 'On Legal Subterfuge and the So-Called "Lawfare" Debate' (2011) Case Western Reserve Journal of International Law 153.

Tamanaha B Z, *Law as a Means to an End: Threat to the Rule of Law* (CUP 2006).
DOI: https://doi.org/10.1017/CBO9780511511073

Troia A, 'The Helms-Burton Controversy: An Examination of Arguments that the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 Violates US Obligations Under NAFTA' (1997) 23 Brooklyn Journal of International law 603.

Turmo A, 'National Security Concerns as an Exception to EU standards on Data Protection'4(2) Nordic Journal of European Law 86.

Werner W G, 'The Curious Career of Lawfare' (2010) 43 Case Western Reserve Journal of International Law 61.

Yackle L, *Regulatory Rights: Supreme Courts Activism, The Public Interest and the Making of Constitutional law* (University of Chicago Press 2007)
DOI: https://doi.org/10.7208/chicago/9780226944739.001.0001

LOWER INSTANCE NATIONAL COURTS AND TRIBUNALS IN MEMBER STATES, AND THEIR JUDICIAL DIALOGUE WITH THE COURT OF JUSTICE OF THE EUROPEAN UNION

GRAHAM BUTLER*

The vast majority of cases that are submitted to the Court of Justice of the European Union (the Court) through the preliminary reference procedure that is contained in Article 267 TFEU come from lower instance national courts and tribunals in EU Member States. As a result, it is not always appellate courts, or higher instance national courts and tribunals, such as courts of final appeal, which make orders for reference. Judicial dialogue between national courts and the Court through this Article 267 TFEU procedure is notable for its particular quality of it being open to receiving orders for reference, for an interpretation of EU law from national courts and tribunals – of any instance – from first instance, to final instance. But can this judicial dialogue between lower instance national courts and tribunals and the Court be impeded by national courts' more senior national Brethren, with appeals being allowed against orders for reference within national legal orders? The case law of the Court on such an issue has been progressive, in that it developed slowly over time, and the Court, by 2021, becoming increasingly assertive. As will be analysed in this article, the Court's approach to the arising issue has clearly been an attempt to balance the interests of judicial dialogue on the one hand, and national rules on the other. Yet, with the Court's broader case law tightening the understanding of who constitutes the European judiciary, and ensuring that all national courts and tribunals remain independent from executive interference in EU Member States, the article commends recent developments, but makes the further plea for an affirmative judgment of the Court to not permit, as a matter of EU law, appeals against orders for reference made by lower instance national courts and tribunals in EU Member States, in the name of preserving judicial dialogue through the preliminary reference procedure.

1 INTRODUCTION

The importance of the preliminary reference procedure to the functioning of the EU legal order, and the effectiveness of EU law, is well-known.[1] It has been described as everything from its indispensability, to being the 'crown in the jewel' in having a functioning EU legal

* Associate Professor of Law, Aarhus University, Denmark.

[1] See, *inter alia*, Anthony Arnull, 'The Past and Future of the Preliminary Rulings Procedure' in Mads Andenas and John A Usher (eds), *The Treaty of Nice and Beyond: Enlargement and Constitutional Reform* (Hart Publishing 2003); Xavier Groussot, 'Spirit Are You There? – Reinforced Judicial Dialogue and the Preliminary Ruling Procedure' (2008) 4 Europarättslig tidskrift 934; Clelia Lacchi, 'Multilevel Judicial Protection in the EU and Preliminary References' (2016) 53 Common Market Law Review 679; Koen Lenaerts, 'Form and Substance of the Preliminary Rulings Procedure' in Deirdre Curtin and Tom Heukels (eds), *Institutional Dynamics of European Integration: Essays in Honour of Henry G. Schermers, Volume II* (Martinus Nijhoff Publishers 1994); Allan Rosas, 'The Preliminary Rulings Procedure' in Dennis Patterson and Anna Södersten (eds), *A Companion to European Union Law and International Law* (John Wiley & Sons, Inc 2016).

order. But it only does so because judicial dialogue is with *all* national courts and tribunals, and not just those of higher instance. Article 267 TFEU, in theory and in practice, protects and preserves judicial dialogue for all national courts and tribunals. But to what extent do lower instance national courts and tribunals, to whom potential appeals against their actions may lie, have their judicial dialogue with the Court protected by that very same Court?

The overwhelming majority of the cases on the docket of the Court[2] are those that are referred to it by national courts and tribunals in EU Member States through the preliminary reference procedure that is provided for in Article 267 TFEU. It constitutes the formal means of judicial dialogue in the EU. Why specific cases reach the Court through this procedure is something of a mystery, and each case through the procedure is subject to its own factual context. This said, the preliminary reference procedure makes a distinction between 'higher' and 'lower' instance national courts and tribunal, given the very language of Article 267 TFEU. There are a whole host of reasons for why a national court or tribunal of a Member State *may* refer, if they 'consider […] that a decision on the question is necessary to enable it to give judgment'.[3] This is in regard to lower instance national courts and tribunals.[4] But this '*may*' quickly turns into a '*shall*', for higher instance national courts and tribunals, when the latter's ruling there can be no appeal from.

Article 267 TFEU provides for this judicial dialogue between national courts and tribunals and the Court, and it states,

> The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning:
> (a) the interpretation of the Treaties;
> (b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union;
> Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court to give a ruling thereon.
> Where any such question is raised in a case pending before a court or tribunal of a Member State against whose decisions there is no judicial remedy under national law, that court or tribunal shall bring the matter before the Court.
> If such a question is raised in a case pending before a court or tribunal of a Member State with regard to a person in custody, the Court of Justice of the European Union shall act with the minimum of delay.

Whilst facilitating judicial dialogue to enable the Court 'to give a ruling', there are many unanswered questions regarding Article 267 TFEU: what is a court of a Member State? What is a tribunal of a Member State? What does 'of a Member State' mean? Are national courts and tribunals obligated to make a reference for a preliminary ruling? What is a court or

[2] In this article, 'the Court' refers to the Court of Justice within the institution of the Court of Justice of the European Union.

[3] Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/47, art 267(2). It is a different matter, however, for national courts and tribunals 'against whose decisions there is no judicial remedy under national law, that [such] court or tribunal shall bring the matter before the Court', as per Article 267(3) TFEU.

[4] In this article, 'lower instance national courts and tribunals' is understood as bodies to which are not those considered as those falling into Article 267(3) TFEU.

tribunal 'against whose decisions there is no judicial remedy'? What questions can be referring under the procedure? At what stage of a national procedure can questions be referred to the Court? What is to be contained in the reference made by a national court or tribunal?

Guidance of how to answer such (and further) questions under Article 267 TFEU has been considered in the case law.[5] In every case, the determining factors that motivate a national court or tribunal to make an order for reference under Article 267 TFEU may differ, but the very *decision* of a national court or tribunal to make a reference is not always welcome by the parties before national courts and tribunals. Therefore, the natural question arises: can a decision of a national court or tribunal of lower instance, who makes an order for reference under Article 267 TFEU to the Court, be appealed within the national legal order to a higher instance national court? Furthermore, if such decisions are appealed, what is the scope of the powers of the higher instance national courts and tribunals? And does EU law limit the effects of appeals made to higher instance national courts and tribunals against orders for reference made by lower instance national courts and tribunals?

The Court's jurisprudence on how to deal with the different instances in Member States, and the status of the preliminary reference procedure, as will be demonstrated in this article,[6] has varied over time. Whilst the current case-law veers on the side of preventing higher instance national courts and tribunals from interfering in lower instance national courts and tribunals, the case-law has not fully dispelled the underlying problem of the potential for lower instance national courts and tribunal's decisions to refer being subject to a national appeal process, and the wider chilling-effect it could have.[7] This article makes the case that national courts and tribunals, of lower instance – that *may* make a preliminary reference – should retain as broad a discretion as conceivably possible to make orders for reference under Article 267 TFEU, thus having unfettered discretion in engaging in judicial dialogue with the Court. In doing so, this position promotes even wider use of EU law, ensuring that it remains effective, so that actors do not have to engage in long, protracted legal disputes in national courts and tribunal, in the mere hope that higher instance, or final instance national courts and tribunals, make orders for reference.

This article is structured as follows. Section 2 reflects on the history of the issue of judicial dialogue between lower instance national courts and tribunals with the Court, and how appeals against orders for reference were handled. As demonstrated, whilst the Court initially waivered on how to handle the issue of appeals brought against decisions of lower instance national courts and tribunals making orders for reference, it ultimately settled on a compromise between the effectiveness of EU law, and making allowances for national rules.

---

[5] For the most comprehensive, and authoritative single source of analysis on many of the issues arising under Article 267 TFEU, see, Morten Broberg and Niels Fenger, *Broberg and Fenger on Preliminary References to the European Court of Justice* (3rd edn, OUP 2021)., and previous editions (1st edn in 2010, and 2nd edn in 2014).

[6] Elsewhere, previously, in the context of the *Schrems II* case, the Court passed on an opportunity presented to it on curtailing appeals. See, Graham Butler and John Cotter, 'Just Say No! Appeals Against Orders for a Preliminary Reference' (2020) 26 European Public Law 615.

[7] For earlier consideration of the arising issues as Community law, later Union law, once stood, see, David O'Keeffe, 'Appeals Against an Order to Refer under Article 177 of the EEC Treaty' (1984) 9 European Law Review 87. Subsequent writing has also analysed the case-law as it has developed. See, Michal Bobek, 'Cartesio: Appeals against an Order to Refer under Article 234(2) EC Treaty Revisited' (2010) 29 Civil Justice Quarterly 307; Morten Broberg and Niels Fenger, 'Preliminary References as a Right – but for Whom? The Extent to Which Preliminary Reference Decisions Can Be Subject to Appeal' (2011) 36 European Law Review 276.

Firstly, it settled on proceeding with cases that were validly submitted to the Court through the preliminary reference procedure, notwithstanding a national appeals procedure; whilst secondly, it did not state that appeals being brought against decisions to make orders were contrary to Article 267 TFEU. This, is categorised as the 'old case law'.

Next, section 3 moves on to analyse what is called what is branded the 'new case law'. Here, two cases from the Court come into sharp focus, given they affirmatively moved on from prior jurisprudence. Firstly, in *Cartesio*,[8] the Court decided to try and limit the effects of any decisions of higher instance national courts and tribunals against decisions of lower instance national courts and tribunals that involved making an order for reference through Article 267 TFEU. Whilst the *Cartesio* judgment was thus a firmer strengthening of judicial dialogue between lower instance national courts and tribunals and the Court, that the Court had taken in the 'old' case law, the Court however, still, did not rule out the possibility of appeals being made in national legal systems against decisions regarding orders for reference. Secondly thereafter, in *IS*, the Court built on *Cartesio*, by going even further. This time, the Court appeared to take a stronger position than it ever had. Here, it stated that lower instance national courts and tribunal ought to invoke the primacy of EU law, specifically the primacy of Article 267 TFEU against decisions of higher instance national courts and tribunals, to ensure that its judicial dialogue between lower instance national courts and tribunals and the Court is preserved. However, again, still, the Court did not rule out the possibility of appeals being made in national legal systems against decisions regarding orders for reference.

Penultimately, section 4 considers the case for clarity, in which, in the view of this author, the Court ought to go even further than it has in *Cartesio* and *IS*, and affirmatively rule out the mere possibility of appeals, whilst lower instance national courts and tribunals are engaged in judicial dialogue with the Court through the preliminary reference procedure. Conclusively, section 5 rounds out the argument, by putting the issue in a broader context.

2 APPEALS AGAINST DECISION TO REFER, AND THE OLD CASE LAW

2.1 THE ORIGINAL POSITION

Early in the Court's jurisprudence, it decided that if an appeal against an order for reference by a lower instance national court or tribunal was brought to a higher instance national court or tribunal, the pending case on the docket of the Court would continue to proceed. Whilst the Court was operational since 1952 hearing a range of direct actions, it was not until 1961 when the Court received its first ever case through the preliminary reference procedure, then located in Article 177 EEC (now Article 267 TFEU) in *De Geus en Uitdenbogerd v Bosch and Others* (*De Geus v Bosch*).[9] The case had been submitted to the Court by a lower instance national court or tribunal, the *Gerechtshof's-Gravenhage* (Court of Appeal, The Hague). But within the Dutch judicial system, the decision of the Court of Appeal to refer questions to the Court was appealed to a higher instance national court or tribunal.

[8] Case C-210/06 *CARTESIO Oktató és Szolgáltató bt (CARTESIO)* ECLI:EU:C:2008:723.
[9] Case 13/61 *De Geus en Uitdenbogerd v Bosch and Others* (*De Geus v Bosch)* ECLI:EU:C:1962:11.

Going first in adjudicating on the arising issue, Advocate General (AG) Lagrange rejected the view that just because a decision of a lower instance national court to make an order for reference had been appealed, that this would result in the Court having to suspend proceedings before it, until such appeal proceedings at national level had ended.[10] Using its own reasoning, the Court in essence agreed with AG Lagrange. The Court stated,

> Just as the Treaty does not prevent the national [higher instance national court or tribunal] from taking cogni[s]ance of the petition but leaves the determination of its admissibility to the national law and the decision of the national judge, […] *the Treaty makes the jurisdiction of this Court dependent solely on the existence of a request for a preliminary ruling within the meaning of Article [267 TFEU]*. And it does so without requiring this Court to discover whether the decision of the national judge has acquired the force of *res judicata* under the national law.[11]

De Geus v Bosch was therefore a strong endorsement of the rights of lower instance national courts and tribunals within the EU legal order, and ensuring they could have judicial dialogue with the Court. Evidently therefrom, whilst the case was on the docket of the Court, referred to it from a national court or tribunal – of whatever instance – the case remained live.

Whilst the judgment in *De Geus v Bosch* was not directly criticising the decision of one of the parties in the national proceedings to appeal the decision to refer, nor preventing the higher instance national court or tribunal from acting in any way, the Court's position was reasonably clear for its time in the early years of the EU legal order: whilst a case was before it through the preliminary reference procedure, it would proceed in answering the questions put to it. The Court did not, consequently, delve into the intricacies of the underlying national legal system, and how appeals against such decision to make an order for reference, in the '*may*' refer scenario envisaged by Article 267 TFEU, would be handled by higher instance national courts and tribunals.

That said, whilst *De Geus v Bosch* was a favourable judgment for lower instance national courts and tribunals, it did not appear to rule out the possibility of having appeals brought against the decisions of lower instance national courts and tribunals to make orders for reference. In that sense, the judgment in *De Geus v Bosch* paid due deference to national rules. Instead, the Court merely confirmed itself to the specificities of the case at hand – an act of judicial minimalism – and continue with the case on its docket, given it is duly seized of the matter by the referring national court or tribunal.

2.2 THE SECOND POSITION

Subsequently, the Court changed its mind on the position it took in *De Geus v Bosch*, at least initially. It then held that if an appeal was brought to a higher instance national court or tribunal against a decision of a lower instance national court or tribunal to make an order for reference, the pending case on the docket of the Court would be suspended. Thus, the position of the Court in *De Geus v Bosch* was short-lived, at least initially.

[10] For his full reasoning, see, Opinion of Advocate General Lagrange, Case 13/61 *De Geus v Bosch* ECLI:EU:C:1962:3, page 59.
[11] *De Geus v Bosch* (n 9), page 50 (emphasis added).

On the next occasion in which the Court was faced with the same scenario, this time in *Chanel v Cepeha*, which was a referral from the *Arrondissementsrechtbank Rotterdam* (District Court of Rotterdam), the Court had a change of heart over the effect of the case on its docket whilst an appeal against the decision of the lower instance national court or tribunal's to make an order for reference was being heard.[12] Moreover, it is a case where the influence of the AG might be seen to be particularly prominent.[13] AG Roemer in *Chanel v Cepeha* took a different view to that of his former colleague – AG Lagrange – and the judgment of the Court in *De Geus v Bosch*. For AG Roemer, instead, the appeal against the decision of the District Court of Rotterdam to the Court of Appeal in The Netherlands[14] ought, in fact, to result in the proceedings before the Court not proceeding, and the case be stayed on the Court's docket. AG Roemer stated,

> I propose that the Court issue an order declaring that for the moment it cannot give a ruling on the questions submitted to it; it may only do so when the [higher instance national court] has given judgment on the appeal brought against the decision to make the reference.[15]

For him, the Court 'cannot simply ignore the situation',[16] and, the 'necessary result must be a stay of proceedings on the reference until a decision has been given at the national level with regard to whether the interpretation requested is of importance in deciding the case or not'.[17]

Remarkably, the Court in *Chanel v Cepeha* agreed, issuing a very brief order, stating, that '[j]udgment in the present case is suspended pending notification to the Court that the appeal has been decided'.[18] No reasons were given by the Court for its position, other than that it was deciding so '[i]n the circumstances of the case', and no further reasoning was provided for why it had turned its back on its decision in *De Geus v Bosch* so swiftly.

Just over a year later, the Court delivered a second order in *Chanel v Cepeha*. Following a communication from the referring lower instance national court or tribunal – the District Court of Amsterdam – that the higher instance national court or tribunal had amended the judgment of the lower instance national court or tribunal. Therefore, the referring court stated that 'the reference for interpretation has lost its purpose'.[19] The Court, accordingly, removed the case from its docket. No further explanation was given for the Court's action, or any other reasoning in its first order. Whilst problematic for its lack of reasoning, it was

---

[12] Case 31/68 *SA Chanel v Cepeha Handelsmaatschappij NV (Chanel v Cepeha)* ECLI:EU:C:1970:52, page 405.
[13] On the role played by AGs at the Court, see, Graham Butler and Adam Łazowski (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).
[14] By coincidence, the higher instance national court in *Chanel v Cepeha*, was the Court of Appeal in The Hague, was the same national court in the *De Geus v Bosch* case, whose own decision was subject to an appeal to an even higher instance national court.
[15] Opinion of Advocate General Roemer, Case 31/68 *SA Chanel v Cepeha Handelsmaatschappij NV*, ECLI:EU:C:1969:18, page 412.
[16] ibid, page 409.
[17] ibid.
[18] Order of the Court in Case 31/68 *SA Chanel v Cepeha Handelsmaatschappij NV* ECLI:EU:C:1969:21.
[19] *Chanel v Cepeha* (n 12), page 405.

particularly striking that no explanation was offered at all given this was an affirmative U-turn on prior case law.[20]

2.3 A RETURN TO THE ORIGINAL POSITION

Notwithstanding the fact that the Court had already changed its mind without explanation, its change of mind in *Chanel v Cepeha* was not, in fact, long lasting. Rather, in *BRT v SABAM* thereafter, the Court went back to its prior position that it had in *De Geus v Bosch*.

In *BRT v SABAM*, a referral to the Court under Article 267 TFEU from the Tribunal of First Instance in Brussels (*Tribunal de première instance de Bruxelles* or *Rechtbank van eerste aanleg te Brussel*), the defendant notified the Court that it had appealed the decision of the national court in which it made the order for reference. The appeal was brought to a higher instance national court or tribunal in Belgium, and accordingly, the defendant pleaded that the Court should suspend the proceedings, whilst national appeal proceedings were ongoing. In effect, the defendant was seeking an order of the Court, akin to what the Court had done in *Chanel v Cepeha*, pending the outcome of the appeal at national level.

The Court was informed by the referring lower instance national court or tribunal, after the submissions of the defendant, with some hesitation about its position, that it 'does not wish [that] the Court…suspend the examination' of the questions referred, in turn, effectively, asking the Court to take the approach that it had initially taken in *De Geus v Bosch*. In *BRT v SABAM* therefore, AG Mayras therefore had a task on his hand: state the Court follow its revised *Chanel v Cepeha* position, unexplained as it was; or instead revert back to its initial position in *De Geus v Bosch*.

AG Mayras had the courage to recommend the Court revert to its original position of *De Geus v Bosch*. For him, avoiding national procedural questions was of particular importance, noting that if the Court were to consider matters that were before higher instance national courts and tribunals, accounting for technical matters of national court, the Court would be 'exceed[ing] jurisdiction and encroach[ing] upon that of the [national] courts, since [the Court would] be forced to appraise the effects of the appeal against the order for reference in accordance with the rules of the national law'.[21] He continued,

> Article [267 TFEU] establishes direct cooperation between the Court of Justice and the national courts of the Member States which can make use of the power to refer to it, for preliminary rulings, any question of interpretation of Community law which they consider necessary for the solution of disputes brought before them.[22]

Thus, for AG Mayras, not only was a division of powers between national courts and tribunal and the Court important, but also the importance of judicial dialogue between all national

[20] For analysis on U-turns, see, Mirka Kuisma, *Confronting Realities with the Legal Rule: On Why and How the European Court of Justice Changes Its Mind* (PhD dissertation, University of Turku 2021); David T Keeling, 'The Rehabilitation of Trade Marks, the Demise of the Doctrine of Common Origin, and the Overruling of Prior Case Law: Opinion of Advocate General Jacobs in HAG II' in Graham Butler and Adam Łazowski (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).

[21] Opinion of Advocate General Mayras, Case 127/73 *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior (BRT v SABAM)* ECLI:EU:C:1974:11, page 69.

[22] ibid.

and courts and tribunals and the Court under Article 267 TFEU. His convincing argument held sway in the Court. In its judgment, the Court disavowed *Chanel v Cepeha*, but without stating so, nor stating that it was to return to its *De Geus v Bosch* position. Instead, it simply stated that the case 'continues as long as the request of the national court has neither been withdrawn nor become devoid of object',[23] and that 'as the preliminary questions of the [national court] have been duly referred to the Court[,] the latter is bound to give a reply'.[24]

De Geus v Bosch and *BRT v SABAM* were therefore to be seen as the affirmative position of the Court on the question on the effect of appeals made in national legal orders, and the effect they had on proceedings before the Court by the lower instance national court or tribunal who made orders for reference. However, given that *BRT v SABAM* was a reversion to the Court's original position, it would take subsequent jurisprudence to test whether the Court had settled on this position, or whether it would again change its mind, accounting again for the complete absence of reasoning of its decision in *Chanel v Cepeha*.

Much later in *Rheinmühlen-Düsseldorf I*, a referral from the *Bundesfinanzhof* (Federal Fiscal Court) in Germany, the referring national court or tribunal asked a very pointed question to the Court on the intricacies of the preliminary reference procedure then contained in Article 177 EEC (now Article 267 TFEU). It asked,

> [W]hether the second paragraph of Article 177 gives "to a court or tribunal against whose decisions there is a judicial remedy under national law a completely unfettered right to refer questions to the Court of Justice [or …]
> [D]oes it leave unaffected rules of domestic law to the contrary whereby a court is bound on points of law by the judgments of the courts superior to it?[25]

The pointedness of the case most likely lay because of the inconsistent case law that had come out of the Court on these issues, in which a lower instance national court or tribunal – the *Hessisches Finanzgericht* (Fiscal Court of Hesse), and a higher instance national court or tribunal – the *Bundesfinanzhof*, were unsure of where the law stood, and the effect of orders for reference on the docket of the Court, which still had proceedings in national courts and tribunals. In this specific instance, the lower instance national court had itself made its own order for reference to the Court in *Rheinmühlen-Düsseldorf II*,[26] which was pending simultaneously.

The two *Rheinmühlen-Düsseldorf* cases thus offered the Court to clarify matters, and add more insight in the role of lower instance national courts and tribunals and the preliminary reference procedure. In a joined Opinion for both cases, AG Warner concurred with the Court's original position,[27] that higher instance national courts and tribunals, and the national

---

[23] Case 127/73 *BRT v SABAM* ECLI:EU:C:1974:6 para 9.
[24] ibid para 24.
[25] Case 166/73 *Rheinmühlen-Düsseldorf v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (*Rheinmühlen-Düsseldorf I*) ECLI:EU:C:1974:3.
[26] Case 146/73, *Rheinmühlen-Düsseldorf v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (*Rheinmühlen-Düsseldorf II*) ECLI:EU:C:1974:12. Despite this case being lodged by the lower instance national court first (Case 146/73), compared to that of the higher instance national court second (Case 166/73), the case lodged first was adjudicated upon later than the case lodged second, hence the case lodge first is known as *Rheinmühlen-Düsseldorf II*, and the case lodged second is known as *Rheinmühlen-Düsseldorf I*.
[27] And also, therefore, the Opinion of AG Lagrange in *De Geus v Bosch* (n 10), and AG Mayras in *BRT v SABAM* (n 21).

laws and rules of Member States, could not interfere in the judicial dialogue between lower instance national courts and tribunals and the Court. For him, there were three principal reasons for his position,

> First, and most obviously, it involves empowering the Member States to qualify by national legislation the terms of the Treaty.
> Secondly it opens the way for the Treaty to apply differently in different Member States. One Member State might circumscribe the discretion of its lower Courts to refer questions to this Court more tightly than another. This, clearly, could injure both the uniform application of Community law and its balanced development.
> Thirdly it means that, in deciding upon the admissibility of particular references, this Court must be faced with an impossible choice. It must either embark upon the interpretation and application of provisions of national law, including procedural ones — which is not its role — or it must ignore those provisions and thus allow to subsist a situation in which a reference may be admissible in Community law but inadmissible in national law.[28]

The strong position of AG Warner meant the Court was almost compelled to respond with an equally forceful position on the nature and scope of the preliminary reference procedure, and its dialogue that it enjoyed with lower instance national courts and tribunals. This was in particular because AG Warner had grilled the Court in his Opinion, noting the Court's position had been inconsistent, or worse, not sufficiently clear.[29]

The Court did not disappoint for the time, at least in *Rheinmühlen-Düsseldorf I*. There, it stated that 'every national court or tribunal without distinction to refer a case to the Court for a preliminary ruling when it considers that a decision on the question is necessary to enable it to give judgment',[30] and that,

> […] national courts have the *widest discretion* in referring matters to the Court of Justice [… and] that a rule of national law whereby a court is bound on points of law by the rulings of a [higher instance national] court cannot deprive the [lower instance national] courts of their power to refer to the Court questions of interpretation of Community law involving such rulings.[31]

The Court further went out of its way to offer consequentialist logic on what would happen if the preliminary reference procedure was undermined by higher instance national courts and tribunals. The Court thus opined,

> If [lower instance national] courts were bound [by higher instance national courts] without being able to refer matters to the Court, the jurisdiction of the latter to give

[28] Opinion of Advocate General Warner, Case 146/73 *Rheinmühlen-Düsseldorf II* and Case 166/73 *Rheinmühlen-Düsseldorf I* ECLI:EU:C:1973:162.
[29] On the role that *UK* Advocates General, like AG Warner, made to EU law whilst they were within the Court until 2020, see, Butler and Łazowski (n 13).
[30] *Rheinmühlen Düsseldorf I* (n 25) para 2.
[31] ibid para 4 (emphasis added).

> preliminary rulings and the application of Community law at all levels of the judicial systems of the Member States would be compromised.[32]

In other words, lower instance national courts and tribunals retained rights under Article 267 TFEU that no higher instance national courts and tribunal could take away. This was not withstanding the fact that the Court did not rule out the possibility for appeals to be brought against decisions of lower instance national courts and tribunals to make orders for reference.

By contrast, in *Rheinmühlen-Düsseldorf II*, less convincingly, whilst the Court did not say that orders for preliminary references from lower instance national courts could not be the subject of an appeal, it did point out that regardless of an order being appealed, the Court would, '[n]evertheless, in the interests of clarity and legal certainty […] abide by the decision to refer, which must have its full effect so long as it has not been revoked'.[33] However, it went on to say that, 'Article [267 TFEU] does not preclude a decision of such a court referring a question to this Court for a preliminary ruling from remaining subject to the remedies normally available under national law'.[34] Whilst *Rheinmühlen-Düsseldorf II* was nonetheless favourable towards lower instance national courts and tribunals like in *Rheinmühlen-Düsseldorf I*, in principle, it paved the way for caveats to be made.

Thus, *De Geus v Bosch*, *BRT v SABAM*, *Rheinmühlen-Düsseldorf I*, and *Rheinmühlen-Düsseldorf II* was in the direction of offering protection to lower instance national courts and tribunals from higher instance national courts and tribunals (and perhaps, even the national rules in Member States), in ensuring their dialogue with the Court through Article 267 TFEU. Collectively, whilst all being building blocks in their own right on the nature of the preliminary reference procedure, on the issue of appeals, these cases can be considered the 'old case law', given that, whilst still being valid, the Court has later developed its case law quite considerably, and do not reflect current thinking and practice.

3 APPEALS AGAINST DECISIONS TO REFER, AND THE NEW CASE LAW

Whilst these earlier judgments became settled law for some time, there was clearly caveats in the Court's jurisprudence that paved the way for potential exploitation if appeals were brought against orders for reference to higher instance national courts and tribunals. For example, what if national law allowed for higher instance national courts and tribunals to overturn such decisions of lower instance national courts and tribunals? Or amend the text of the order for reference that the lower instance national court or tribunal had submitted to the Court? The perceived position, given this 'old case law', was that the Court would not necessarily get involved in national procedural matters, as long as it was the referring national court or tribunal itself that was engaged in the judicial dialogue.

But this position was by no means certain. For example, academic literature had different perspectives. For example, one view was that 'no rule of national law can fetter the

[32] *Rheinmühlen Düsseldorf I* (n 25) para 4.
[33] *Rheinmühlen-Düsseldorf II* (n 26) para 3.
[34] ibid.

discretion of a lower court to make a reference'.[35] Elsewhere was the position that appeals of references made by lower instance national courts and tribunal were allowed.[36] Such positions was justified at the time, though it might have been plausibly suggested that the views of such authors filled in the blanks as regards the lack of further clarity from the Court.

3.1 CONSTRAINING THE RELEVANCE OF HIGHER INSTANCE NATIONAL COURTS AND TRIBUNALS

Much time past until the Court was faced with the conundrum in *Cartesio*, which marked a new departure for what became the 'new case law'. Here, the *Szegedi Ítélőtábla* (Regional Court of Appeal in Szeged) asked the Court, like in *Rheinmühlen-Düsseldorf I*, a rather pointed question. It asked, inter alia,

> Does a national measure which, in accordance with national law, confers a right to bring an appeal against an order for a preliminary reference, limit the power of the [lower instance national] courts to refer questions for a preliminary ruling or could it limit that power – derived directly from Article [267 TFEU] – if, in appeal proceedings the [higher instance national court] may amend the order, render the request for a preliminary ruling inoperative and order the court which issued the order for reference to resume the national proceedings which had been suspended?[37]

In essence, the question as to whether it was compatible with EU law for the national law of a Member State to allow a decision of a lower instance national court or tribunal, to make an order for reference, to be appealed to a higher instance national court or tribunal, which could either: amend the reference; render the reference inoperative; or force the lower instance national court or tribunal to resume proceedings, notwithstanding the reference to the Court.

Faced with such questions in a straightforward manner, the Court in *Cartesio* was bolder than it had ever been. Instead of being deferent to potential appeals that may lie within national legal orders, as it had in the 'old case law', against decisions of lower instance national courts and tribunals to make to make orders references, the Court qualified the scope of national procedural rules that could exist in the area. Whilst restating its position from the 'old case law', the Court then added,

> Nevertheless, the outcome of such an appeal *cannot limit the jurisdiction conferred by Article [267 TFEU] on that [referring] court to make a reference to the Court* if it considers that a case pending before it raises questions on the interpretation of provisions of [Union] law necessitating a ruling by the Court.[38]

---

[35] Francis G Jacobs and Andrew Durand, *References to the European Court: Practice and Procedure* (Butterworths 1975) 171.

[36] Finbarr Murphy, 'Campus Oil Ltd., Estuary Fuel Ltd., McMullan Bros. Ltd, Ola Teoranta, P.M.P.A. Oil Company Ltd., Tedcastle McCormick and Company Ltd. v. The Minister for Industry and Energy, Ireland, The Attorney General and The Irish National Petroleum Corporation Ltd. (1982–1983) J.I.S.E.L. 43; (1984) 1 C.M.L.R. 479.' (1984) 21 Common Market Law Review 741, 749.

[37] Case C-210/06 *CARTESIO Oktató és Szolgáltató bt (Cartesio)* ECLI:EU:C:2008:723, para 40.

[38] *CARTESIO* (n 37) para 93 (emphasis added).

It continued that 'the assessment of the relevance and necessity of the question referred for a preliminary ruling is, in principle, the responsibility of the referring court alone'.[39]

Therefore, the Court's position in *Cartesio* was that decisions of lower instance national courts and tribunals to make orders for reference under Article 267 TFEU could not be called into questions by national law, or the practice of higher instance national courts and tribunals to vary the reference, stop the reference, or to order resumption of the proceedings of the lower instance national court.

The Court's judgment in *Cartesio* was quite far-reaching,[40] in that Article 267 TFEU was to be interpreted in a manner that *any* national court or tribunal could make an order for reference, which could not be called into question by the application of national procedural rules. On the extreme end of *Cartesio*, it can be read as an attempt to level the hierarchy of the national courts and tribunals in EU Member States in their judicial dialogue with the Court. Though the Court, like its historic case law, did not actually rule out the possibility of appeals, notwithstanding the effects that Cartesio would have on such appeals.

This said, the Court did not go as far as AG Poiares Maduro in *Cartesio*, who had a bolder, more daring proposition to eliminate the very *potential* for higher instance national courts and tribunals to still have an upper hand, and interfere with the judicial dialogue of lower instance national courts and tribunals and the Court. Instead, for him, the power to make an order for reference derived from the EU Treaties themselves through Article 267 TFEU. As he put it,

> The Treaty did not intend that such a dialogue [between lower instance national courts and tribunal and the Court] should be filtered by any other national courts, no matter what the judicial hierarchy in a State may be.[41]

In line with ordinary consequential line of reasoning, and clearly of the same spirit as that of the Opinion of AG Warner in the *Rheinmühlen Düsseldorf* cases, AG Poiares Maduro feared that the preliminary reference procedure would end up only in the hands of higher instance national courts and tribunals, if appeals in national legal orders were possible. As he stated in *Cartesio*,

> [I]t could happen that, by virtue of a national rule or practice, orders for reference by lower courts would systematically become subject to appeal, giving rise to a situation in which – at least *de facto* – national law allowed only courts of last instance to refer questions for a preliminary ruling. The risk of treating such question as a question of national procedural law and not Community law is highlighted by the present case [*Cartesio*] in which the national law permits a separate appeal against a decision to make a reference for a preliminary ruling. It would be tantamount to allowing national procedural law to alter the conditions set out in Article [267 TFEU] for a reference to the Court of Justice.

---

[39] ibid para 96.
[40] For a reassertion of *Cartesio*, see, Case C-470/12 *Pohotovost' s. r. o. v Miroslav Vašuta* ECLI:EU:C:2014:101, paras 25-35.
[41] Opinion of Advocate General Poiares Maduro, Case C-210/06 *CARTESIO* ECLI:EU:C:2008:294, para 19.

In other words, he favoured a more absolutist approach, whereby appeals brought against decisions of lower instance national courts and tribunals to make orders for reference would not be appealable at all.

Notwithstanding the fact that the Court's judgment in Cartesio did not rule out appeals, the judgment was nonetheless reasonable, and a clear development of the law of Article 267 TFEU. It came closest the Court had to date in establishing an affirmative right of lower instance national courts and tribunals to have judicial dialogue with the Court. And it did gut, to some extent, the effectiveness of the appeal procedure at national level, given it would have little effect on the judicial dialogue between the referring lower instance national court or tribunal and the Court. The leading authority on the preliminary reference procedure goes further, however, reading that the *Cartesio* judgment effectively meant that decision of the higher instance national courts and tribunals, on appeal, 'can merely be an advisory opinion for the lower court'.[42]

Outstanding problems have remained, given the Court has not ruled out appeals themselves. Given the case law did not forbid appeals, there would be the continued *potential* for an appeal procedure, against decisions of lower instance national courts and tribunals to make orders for reference to delay, frustrate, and assert pressure on lower instance national courts and tribunals in their judicial dialogue with the Court. Moreover, the case law to date did not preclude higher instance national courts and tribunals from taking control of the main proceedings for itself on appeal, thereby obviating the need for any order for reference made by a lower instance national court or tribunal. Furthermore, what would happen if a higher instance national court or tribunal stated that the premise upon which the lower instance national court and tribunal had made a preliminary reference on the basis of making an error regarding findings of fact in which the reference was made.[43] *Cartesio* was far from being the end of the story.

3.2 THE INVOCATION OF PRIMACY, BUT CONTINUED REFUSAL TO ELIMINATE THE POSSIBILITY OF APPEALS

The relevance of appeals brought decisions of lower instance national courts and tribunals to refer to the Court raised its head again post-*Cartesio*, in the *IS* case. This time, the referring lower instance national court or tribunal brought explicit concerns to the Court, through the preliminary reference procedure, that if appeals were allowed against such decisions to make orders for reference by lower instance referring courts and tribunals, it would have a deterrent effect from even contemplating making referrals under Article 267 TFEU.[44] This was, in essence, the concerns of AGs Warner and Poiares Maduro, which were never fully met by the Court, notwithstanding its narrowing of the relevance of appeals brought.

In its *IS* judgment in 2021, the Court maintained that appeals of decisions of lower instance national courts and tribunals to make orders for reference were possible, or in the language of the Court, 'Article 267 TFEU does not preclude an order for reference from

[42] Broberg and Fenger (n 5) 296.
[43] As seen in Butler and Cotter (n 6).
[44] Case C-564/19 *IS (Illégalité de l'ordonnance de renvoi)* ECLI:EU:C:2021:949, para 42.

being subject to a judicial remedy under national court',[45] and applied the three elements of the *Cartesio* case.

However, the rather than just state – as it did – that appeals against such decisions were allowed, the Court nonetheless seized the opportunity to clarify further matters, and sought to build on *Cartesio* by putting lower instance national courts and tribunals. The Court, for the first time, engaged with the wider effects of the possibility of such appeals, similar to the concerns of its AGs in prior cases. The Court stated such that appeals being pursued in higher instance national courts and tribunals, against decisions of lower instance national courts and tribunals in making orders for reference,

> is likely to prompt the [national] courts to refrain from referring questions for a preliminary ruling to the Court, in order to preclude their requests for a preliminary ruling from being challenged by one of the parties on the basis of the [higher instance national court or tribunal] decision or from being the subject of an appeal in the interests of the law.[46]

From there, the Court recalled its exertions from *Van Gend en Loos*, and further noted, in a similar vein to AG Poiares Maduro in *Cartesio*, of the effects of such appeals, in that,

> Limitations on the exercise by national courts of the jurisdiction conferred on them by Article 267 TFEU would have the effect of restricting the effective judicial protection of the rights which individuals derive from EU law.[47]

Therefore, rather, that stating that appeals against referrals were not possible, the Court went for a different route, which was to *empower* lower instance national courts and tribunals vis-à-vis their senior Brethren in the national legal orders, through the invocation of primacy of EU law over national law, and decisions of higher instance national courts and tribunals. For the Court,

> the principle of the primacy of EU law requires a lower court to disregard a decision of the supreme court of the Member State concerned if it considers that the latter is prejudicial to the prerogatives granted to that lower court by Article 267 TFEU.[48]

This was the key distinction of *IS* from its prior *Cartesio* judgment, notwithstanding they both belonged to the 'new case law'. In *IS*, it would thus appear that the Court finally came to the view that the caveats to its existing case law were beginning to be exploited. Furthermore, the Court concerned itself with the wider effects of such appeals against decisions to make orders for reference, beyond the case at hand, and more willing to look at the wider factors that lead a lower instance national court or tribunal to make an order for reference.

The Court's *IS* judgment in effect, over and above prior case law, demands that lower instance national courts and tribunals disregard any practice in a national judicial system that prejudices their rights to make a preliminary reference under Article 267 TFEU, and demands that lower instance national courts and tribunals disregard decisions of higher

[45] *IS* (n 44) para 72.
[46] ibid para 75.
[47] ibid para 76.
[48] ibid para 81.

instance national courts and tribunals that interfere in their judicial dialogue with the Court. This was a deeper cut into national procedures, and certainly envisages the Court taking a more assertive approach towards appeals brought against decisions of lower instance national courts and tribunal to make orders for reference into the future.

4 APPEALS AGAINST DECISIONS TO REFER, AND THE NEED FOR CLARITY

Appeal against decisions of lower instance national courts or tribunals to make orders for reference has a number of consequences. For example, it disincentivises referrals made under Article 267 TFEU, it affects the possibility of ensuring effective judicial remedies making use of EU law, it has the potential affect the uniformity and consistency in EU law, it slows litigation, and it ultimately hampers the mode of dialogue and communication between national courts and tribunals and the Court.

Appeals are still allowed, notwithstanding the increasing uselessness of such appeals being brought, given *Cartesio* eliminated some of the effects, and *IS* empower lower instance national courts and tribunals to invoke the primacy of EU law against national rules, and decisions of higher instance national courts and tribunal. Post-*Cartesio* and *IS*, however, how lower instance national courts and tribunals are to fully respond to appeals of orders for preliminary references is unclear, given they remain possible. The fact remains that the very climate of still allowing the appeals potentially lessens to effect that the preliminary reference procedure. In other words, there remain lingering questions about how far national law, national actors, and national courts, have a role in limiting the effects of orders for reference made under Article 267 TFEU.

In anything, the Court appears to be at pains to avoid a situation where it would rule that appeals against orders for reference are prohibited. This is demonstrated by its extremely incremental approach the Court has taken across both its 'old' and 'new' case law, whereby the Court has only come about these positions, as judges in lower instance national courts and tribunals, have, in essence, begged for judicial protection themselves. Admittedly, *Cartesio* pre-dated the emergence of subsequent rule of law and judicial independence issues in some of these Member States. *IS*, however, was in the midst of the litany of cases that Court has been dealing with for some years on the undermining of certain national judiciaries by certain Member States. Whilst the Court is creating a protected space for lower instance national courts and tribunals, more will continue to be asked of it generally, and specifically with regard the continued ability of lower instance national courts and tribunals to make orders for reference.

The Advocates General in two prior cases, in particular, were concerned about the wider chilling effects of appeals against decisions making preliminary references. AG Warner in *Rheinmühlen Düsseldorf* was of the view that failing to prohibit higher instance national courts and tribunals from interfering in dialogue between the Court and lower instance national courts and tribunals would be tantamount to enabling and seeing free qualification of the preliminary reference procedure, without having due regard to Article 267 TFEU.[49] Given that in *IS*, the Court explicitly placed emphasis on the primacy of EU law – Article

[49] Opinion of AG Warner in *Rheinmühlen-Düsseldorf II* and *Rheinmühlen-Düsseldorf I* (n 28).

267 TFEU – over any national procedural measure, *IS* can be seen as a de facto endorsement of AG Warner's position, nearly half a century later. Secondly, AG Poiares Maduro in *Cartesio* feared that having appeals against orders for reference from lower instance national courts and tribunals would whittle down the procedure to only having courts of final instance referring.[50] This fear did not come to pass, but with *Cartesio*, and now *IS*, it is likely that AG Poiares Maduro's worst fears will not now come to pass.

The EU legal order has moved on significantly since *Cartesio*, as demonstrated by the underlying facts of *IS*, in which a national judge was subject to disciplinary proceedings by making use of the preliminary reference procedure. Rightly, the Court took the opportunity to also state that such disciplinary proceedings. Beginning in the *Association of Portuguese Judges* case,[51] the Court, in the face of persistent rule of law issues and the independence of national courts and tribunals in some Member States, commenced invoking stronger constitutional arguments on the nature of the EU legal order as basis for drawing the parameters of whom constitutes the European judiciary, and what the demands of it are. This rule of law case law has strengthened the demands of national judiciaries as a matter of EU law.[52]

Article 267 TFEU imposes, without question, the possibility for *all* national courts and tribunals to make orders for reference at their own motion, without any hindrance from higher instance national courts and tribunals. Yet, appeals are still conceivably possible. This requires clarity, and it can be pondered, if *Cartesio* and *IS* affirmatively eliminates the usefulness of bringing appeals against decision of lower instance national courts and tribunal to make orders for reference to higher instance national courts and tribunals, shouldn't the Court just state that appeals are not allowed?

The reasoning for this position in quite straightforward. National law, and higher instance national courts and tribunals, cannot reinterpret or amend Article 267 TFEU. The preliminary reference procedure therein is freestanding. Given Article 267 TFEU was not to be a reserve of higher instance national courts and tribunals, there ought to be next-to-no room for maneuver for higher instance national courts and tribunals to interfere with judicial dialogue taking place below them in lower instance national courts and tribunals. *All* national courts and tribunal, *of whatever instance*, have to have an unfettered and unfiltered possibility to interact with the Court through the preliminary reference procedure, given that Article 267 TFEU. At the next opportunity, the Court will be presented with a possibility to go further than it did in *Cartesio* and *IS*, and there should be no reason for the Court to be shy in prohibiting appeals of decisions of lower instance national courts and tribunals in their making of orders for references.

5 CONCLUSION

Lower instance national courts and tribunals must be aware that irrespective of the jurisprudence of higher instance national courts and tribunals, they have the right to engage

[50] Opinion of AG Poiares Maduro in *CARTESIO* (n 41).
[51] Case C-64/16 *Associação Sindical dos Juízes Portugueses v Tribunal de Contas (Association of Portuguese Judges)* ECLI:EU:C:2018:117.
[52] For comprehensive treatment of the post-*Association of Portuguese Judges* case law, see, Laurent Pech and Dimitry Kochenov, 'Respect for the Rule of Law in the Case Law of the European Court of Justice: A Casebook Overview of Key Judgments since the Portuguese Judges Case' (Swedish Institute for European Policy Studies 2021) 2021:3.

in judicial dialogue with the Court through the preliminary reference procedure in Article 267 TFEU. The rights of all or all national courts and tribunals in EU Member States to make orders for reference to the Court is a matter governed by EU law, and not national law. It has long been the case, through the ages, that national measures which impede the functioning of the preliminary reference procedure 'must be set aside'.[53] Impeding judicial dialogue through the preliminary reference procedure – be it by national law, or by higher instance national courts and tribunals – only stands to interrupt formal means of judicial dialogue, and do damage to the very purpose of the procedure, which is to ensure uniform interpretation of EU law, and ensuring its consistent application throughout the Union.

There are ways of analysing the preliminary reference procedure through different theoretical lenses.[54] It is a special procedure, given that it remains vastly different from other procedures before the Court, such as the numerous forms of direct actions.[55] Yet it remains the predominant type of case which arrives on the Court's docket. Rightly, the Court has grown to more staunchly defend the preliminary reference procedure and the role of national courts in making such requests.[56] But it will be forced to go further if lower instance national courts and tribunals decrease the number of cases referred when they ought to, or experience cold chilling effects in national legal orders if they are dissuaded from making orders for reference, owing to structural factors in Member States.

The case law, in this author's view, has to veer in the direction of not just being a mere tool in the hands of lower instance national courts and tribunals, but rather, one that is in their right under Article 267 TFEU, regardless of whatever higher instance national courts and tribunals think of such matters. *Cartesio* and *IS* will not be the end of the dilemma. Respectfully, the Union is at a more advanced stage of constitutional integration, and the Court ought to be more affirmative than it has previously been to date.

There are numerous limitations imposed by EU law on national laws, rules, and practices, or any national measures interfering in the preliminary reference procedure.[57] This now needs to go further. The permissive approach by the Court on the issue of appeals brought, whilst qualified in *Cartesio* and *IS*, has been a large demonstration of deference to national procedural rules. The Court may continue to underestimate the potential effects of such appeals against orders being permissible, deterring the willingness of lower instance national courts and tribunals to refer under Article 267 TFEU, and the dampening the enthusiasm of litigants to push for preliminary references to ensure the effectiveness of

[53] Eg, Case C-312/93 *Peterbroeck, Van Campenhout & Cie SCS v Belgian State* ECLI:EU:C:1995:437, para 13. This, however, was established in *Rheinmühlen Düsseldorf I* (n 25).

[54] See, eg, John Cotter, *Legal Certainty in the Preliminary Reference Procedure: The Role of Extra-Legal Steadying Factors* (Edward Elgar Publishing 2022).

[55] The most common direct action is the action for annulment, or nullity action, contained in Article 263 TFEU. See, on the distinction between the two, Angela Ward and Graham Butler, 'The Relationship between the Action for Annulment and Preliminary Reference Procedures: Opinion of Advocate General Jacobs in TWD' in Graham Butler and Adam Łazowski (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).

[56] For a recent reassertion, see Joined Cases C-558/18 and C-563/18 *Miasto Łowicz and Prokurator Generalny zastępowany przez Prokuraturę Krajową, formerly Prokuratura Okręgowa w Płocku v Skarb Państwa – Wojewoda Łódzki and Others* ECLI:EU:C:2020:234, paras 55-59 and cited case law therein.

[57] See, eg, Rosario Silva de Lapuerta, 'The Right of Any Court or Tribunal of a Member State to Request a Preliminary Ruling from the Court of Justice of the European Union' in Koen Lenaerts and others (eds), *Building the European Union: The Jurist's View of the Union's Evolution: Liber Amicorum in Honour of José Luís da Cruz Vilaça* (Hart Publishing 2021).

Union law. There are undoubtedly blind spots in the preliminary reference procedure.[58] But with more assertive lower instance national courts and tribunals highlighting issues, the Court cannot be naïve about what is taking place in EU Member States.

[58] On prior musings, when the preliminary reference procedure is gainfully used in a fraudulent manner, see Graham Butler and Urška Šadl, 'The Preliminaries of a Reference' (2018) 43 European Law Review 120.

LIST OF REFERENCES

Arnull A, 'The Past and Future of the Preliminary Rulings Procedure' in Mads Andenas and John A Usher (eds), *The Treaty of Nice and Beyond: Enlargement and Constitutional Reform* (Hart Publishing 2003).
DOI: https://doi.org/10.5040/9781472562852.ch-013

Bobek M, 'Cartesio: Appeals against an Order to Refer under Article 234(2) EC Treaty Revisited' (2010) 29 Civil Justice Quarterly 307.

Broberg M and Fenger N, 'Preliminary References as a Right – but for Whom? The Extent to Which Preliminary Reference Decisions Can Be Subject to Appeal' (2011) 36 European Law Review 276.

——, *Broberg and Fenger on Preliminary References to the European Court of Justice* (Third Edition, Oxford University Press 2021).
DOI: https://doi.org/10.1093/oso/9780198843580.001.0001

Butler G and Cotter J, 'Just Say No! Appeals Against Orders for a Preliminary Reference' (2020) 26 European Public Law 615.

Butler G and Łazowski A (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).

Butler G and Šadl U, 'The Preliminaries of a Reference' (2018) 43 European Law Review 120.

Cotter J, *Legal Certainty in the Preliminary Reference Procedure: The Role of Extra-Legal Steadying Factors* (Edward Elgar Publishing 2022).

Groussot X, 'Spirit Are You There? – Reinforced Judicial Dialogue and the Preliminary Ruling Procedure' (2008) Europarättslig tidskrift 934.
DOI: https://doi.org/10.2139/ssrn.1279367

Jacobs FG and Durand A, *References to the European Court: Practice and Procedure* (Butterworths 1975).

Keeling DT, 'The Rehabilitation of Trade Marks, the Demise of the Doctrine of Common Origin, and the Overruling of Prior Case Law: Opinion of Advocate General Jacobs' in HAG II' in Graham Butler and Adam Łazowski (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).

Kuisma M, 'Confronting Realities with the Legal Rule: On Why and How the European Court of Justice Changes Its Mind' (University of Turku 2021).

Lacchi C, 'Multilevel Judicial Protection in the EU and Preliminary References' (2016) 53 Common Market Law Review 679.

Lenaerts K, 'Form and Substance of the Preliminary Rulings Procedure' in Deirdre Curtin and Tom Heukels (eds), *Institutional Dynamics of European Integration: Essays in Honour of Henry G. Schermers, Volume II* (Martinus Nijhoff Publishers 1994).

Murphy F, 'Campus Oil Ltd., Estuary Fuel Ltd., McMullan Bros. Ltd, Ola Teoranta, P.M.P.A. Oil Company Ltd., Tedcastle McCormick and Company Ltd. v. The Minister for Industry and Energy, Ireland, The Attorney General and The Irish National Petroleum Corporation Ltd. (1982–1983) J.I.S.E.L. 43; (1984) 1 C.M.L.R. 479.' (1984) 21 Common Market Law Review 741.

O'Keeffe D, 'Appeals Against an Order to Refer under Article 177 of the EEC Treaty' (1984) 9 European Law Review 87.

Pech L and Kochenov D, 'Respect for the Rule of Law in the Case Law of the European Court of Justice A Casebook Overview of Key Judgments since the Portuguese Judges Case' (Swedish Institute for European Policy Studies (SIEPS) 2021) 2021:3.

Rosas A, 'The Preliminary Rulings Procedure' in Dennis Patterson and Anna Södersten (eds), *A Companion to European Union Law and International Law* (John Wiley & Sons, Inc 2016).

Silva de Lapuerta R, 'The Right of Any Court or Tribunal of a Member State to Request a Preliminary Ruling from the Court of Justice of the European Union' in Koen Lenaerts and others (eds), *Building the European Union: The Jurist's View of the Union's Evolution: Liber Amicorum in Honour of José Luís da Cruz Vilaça* (Hart Publishing 2021).

Ward A and Butler G, 'The Relationship between the Action for Annulment and Preliminary Reference Procedures: Opinion of Advocate General Jacobs in TWD' in Graham Butler and Adam Łazowski (eds), *Shaping EU Law the British Way: UK Advocates General at the Court of Justice of the European Union* (Hart Publishing 2022).

CROSS-BORDER TRANSFERS OF PERSONAL DATA AFTER *SCHREMS II*: SUPPLEMENTARY MEASURES AND NEW STANDARD CONTRACTUAL CLAUSES (SCCs)

MARCELO CORRALES COMPAGNUCCI,* MATEO ABOY,† TIMO MINSSEN‡

This article analyses the legal challenges of international data transfers resulting from the recent Court of Justice of the European Union (CJEU) decision in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II). This judgement invalidated the EU-US Privacy Shield Framework but upheld the use of standard contractual clauses (SCCs). However, one caveat is that organisations would have to perform a case-by-case assessment on the application of the SCCs and implement 'supplementary measures' to compensate for the lack of data protection in the third country, where necessary. Regrettably, the CJEU missed the opportunity to specify what exactly these 'supplementary measures' could be. To fill this gap, the European Data Protection Board (EDPB) adopted guidelines on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In addition, on June 4th, 2021 the European Commission issued new SCCs which replaced the previous SCCs that were adopted under the previous Data Protection Directive 95/46. These new developments have raised the bar for data protection in international data transfers. In this article, we analyse the current regulatory framework for cross-border transfers of EU personal data and examine the practical considerations of the emerging post-Schrems II legal landscape.

1 INTRODUCTION

One explicit goal of the General Data Protection Regulation (GDPR)[1] is to guarantee the free flow of personal data between EU Member States. Additionally, the GDPR contemplates the possibility of transferring personal data to a third country – a country outside of the European

* Associate Professor at the Centre for Advanced Studies of Biomedical Innovation Law (CeBIL), Faculty of Law (UCPH). Acknowledgments: The research of all three co-authors for this contribution was supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Programme in Biomedical Innovation Law (Grant agreement number NNF17SA0027784). Timo Minssen's Research has also been supported by the Wallenberg Foundations' 'Initiative for Humanistic and Social Scientific Research in AI and Autonomous Systems' (WASP-HS), see: https://portal.research.lu.se/portal/sv/projects/the-quantum-law-project(4d675bed-6738-4f81-9b28-48746ada562b).html.
† Principal Research Scholar in Biomedical Innovation, Precision Medicine, AI & Law at the Centre for Law, Medicine and Life Sciences (LML), Faculty of Law, University of Cambridge & Affiliated Professor & Fellow at CeBIL, Faculty of Law, University of Copenhagen (UCPH).
‡ Law Professor and the Founding Director for the Centre for Advanced Studies of Biomedical Innovation Law (CeBIL), Faculty of Law (UCPH). He is also affiliated as a guest researcher with Lund University.
[1] 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 L 119/1.

Economic Area (EEA) – or an international organisation, provided that importers and exporters can guarantee that data will be protected under the same European standards. GDPR provisions for international data transfers also include onward transfers. For instance, from a processor to a sub-processor in a third country outside the EEA.[2]

The current legal landscape to transfer personal data outside of the EEA as set out in the GDPR includes the following mechanisms:

i. *Adequacy decisions (Art. 45 GDPR).* Adequacy decisions are based on assessments that third country laws and practices guarantee the same level of European standard protection. The effect of such decisions is that personal data can flow without restrictions and any further additional safeguards. In other words, transfers to the countries in this list will be assimilated to intra-EU transmissions of data.[3]
ii. *Appropriate safeguards (Art. 46 GDPR).* In the absence of adequacy decisions, organisations involved in the cross-border transfers must implement 'appropriate safeguards' (ie, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), codes of conducts, certification mechanisms and ad hoc contractual clauses) to ensure that the level of protection is not undermined.[4]
iii. *Derogations (Art. 49 GDPR).* In the absence of an adequacy decision or appropriate safeguards, there are specific situations (eg, the transfer is necessary for important reasons of public interest) where derogations may be used but these have an exceptional nature and are subject to strict conditions such as occasional and non-repetitive processing activities.[5]

Recent developments, including the *Schrems II* decision, the follow-on European Data Protection Board (EDPB) Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,[6] and the new SCCs for the transfer of personal data to third countries[7] issued by the European Commission (EC) on June 4th, 2021, have raised a wave of debates and concerns among data protection professionals.

---

[2] Eduardo Unstaran, 'International Data Transfers' in Eduardo Ustaran (ed), *European Data Protection: Law and Practice* (2nd edn, IAPP Publication, 2019), 527.
[3] See GDPR (n 1) art 45. See also Commission, 'Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 9 October 2021.
[4] See GDPR (n 1) art 46. The transfer tools may require additional 'supplementary measures' to ensure essentially equivalent level of protection. See Case C-311/18 *Facebook Ireland and Schrems (Schrems II)* ECLI:EU:C:2020:559, paras 130 and 133.
[5] See GDPR (n 1) art 49.
[6] European Data Protection Board (EDPB), 'Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' ('EDPB Recommendations 01/2020') adopted on 10 November 2020, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en> accessed 9 October 2021.
[7] European Commission implementing decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3972 final.

While the *Schrems II* ruling ultimately found that the SCCs were valid, the Court also noted that the receiving country's laws could potentially undermine the protections in the SCCs, exacerbating the uncertainties and risks for organisations relying on this transfer tool.[8] The new SCCs provide more flexibility and ameliorates some of the shortcomings of the previous SCCs. They raise the standard of data protection and include stricter rules for data importers and exporters, in particular extensive obligations for data importers acting as controllers.[9]

In light of these new challenges, this article aims to analyse the emerging legal framework for international transfers of personal data. The paper is structured as follows. Section 2 elucidates the background and main issues raised in the *Schrems* cases. Section 3 then provides a synopsis of the current legal framework and data protection guidance for cross-border transfers after the *Schrems II* judgment. This provides the basis for Section 4, which delivers a discussion of the practical implications of these developments including a discussion of how to best navigate the new legal environment for international data transfer. This will allow us to draw conclusions in Section 5.

2 THE INVALIDATION OF THE SAFE HARBOUR AGREEMENT AND THE EU-US PRIVACY SHIELD IN *SCHREMS I & II*

In 2013, Austrian citizen and privacy activist Maximilian Schrems filed a legal suit with the Irish Data Protection Commission (DPC) against Facebook (*Schrems I*)[10] and requested to prohibit or suspend the transfer of his personal data from Facebook Ireland to the United States. He considered that the law and practice of the United States did not warrant adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities such as the US National Security Agency (NSA).[11]

The DPC, however, rejected the complaint on the grounds of, in particular, Decision 2000/520 (Safe Harbour Agreement) which ensured an adequate level of protection of personal data transferred between the EU and the US. Mr. Schrems contested the decision of the DPC and the Irish High Court referred the case to the CJEU for a preliminary ruling on the interpretation and validity of the Safe Harbour Framework.[12]

In addition to the lack of informed consent and the failure to provide legal remedies for individuals, Mr. Schrems argued that US surveillance laws (such as section 702 of the Foreign

[8] Aloke Chakravarty and Mary Colleen Fowler, 'What Schrems are Made Of: The European Commission Adopts New Standard Contractual Clauses for International Data Transfers Covered by GDPR' (*JDSUPRA,* 30 June 2021) <https://www.jdsupra.com/legalnews/what-schrems-are-made-of-the-european-3977830/> accessed 9 October 2021.

[9] Carol Umhoefer and Andrew Serwin, 'European Commission's standard contractual clauses: extensive new requirements coming for US businesses receiving EU personal data subject to GDPR' (*DLA Piper*, 8 June 2021) <https://www.dlapiper.com/en/us/insights/publications/2021/06/european-commissions-standard-contractual-clauses-extensive-new-requirements/> accessed 9 October 2021.

[10] Case C-362/14 *Maximillian Schrems vs Data Protection Commissioner (Schrems I)* ECLI:EU:C:2015:650.

[11] 'EU-US Data Transfers' (*NOYB*) <https://noyb.eu/en/project/eu-us-transfers> accessed 9 October 2021.

[12] Timo Minssen and others, 'The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the Legal Challenges and How Might These Affect Cloud-based Technologies, Big Data, and AI in the Medical Sector?' (2020) 4(1) European Pharmaceutical Law Review 34, 3941.

Intelligence Surveillance Act and Executive Order 12333) and US programs disclosed by the Snowden revelations[13] such as PRISM,[14] allowed US authorities to access personal data from US Big Tech companies. The CJEU agreed with the plaintiff and decided to overturn the Safe Harbour Agreement in 2015, thereby making illegal to transfer personal data under this framework. The CJEU held that this was a violation to European privacy laws and the fundamental principles enshrined in Articles 7, 8 and 47 of the Charter of Fundamentals Rights of the European Union (CFR).[15]

After the invalidation of the Safe Harbour Agreement, Facebook and other companies then changed to the SCCs to claim legal basis for the transfer of personal data outside of the EU.[16] The US and European authorities signed another agreement which would compensate the failings of Safe Harbour. This new agreement was the so-called EU-US Privacy Shield Framework,[17] whereby US-based companies could join by committing to the framework requirements and by submitting a self-certification to the US Department of Commerce. The EU-US Privacy Shield Framework included a list of requirements such as the submission of a privacy policy with specific details. In general, the framework required greater transparency, oversight and redress mechanisms, including the creation of an ombudsman to investigate complaints as well as arbitration and alternative dispute resolution (ADR) mechanisms.[18] In effect, the Privacy Shield enabled EU to US cross-border transfers under Art. 45 GDPR (as a *limited* adequacy decision).[19]

By an amended complaint in December 2015, Mr. Schrems challenged the validity of Facebook's use of SCCs and requested the DPC to prohibit or suspend the transfer of his personal data to Facebook Inc. Finally, in July 2020, the CJEU in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (*Schrems II*)[20] rendered the EU – US Privacy Shield invalid and upheld the validity of the SCCs.

Nevertheless, the Court required a 'case-by-case' analysis on the application of the SCCs. Controllers and processors exporting data need to verify if the law and practice of the third country impinges on the effectiveness of the appropriate safeguards established in Art. 46 GDPR. It follows from the *Schrems II* judgement that data exporters need to implement

---

[13] Barton Gellman, *Dark Mirror: Edward Snowden and the American Surveillance State* (Penguin Press 2020).
[14] Nicholas Watt, 'Prism Scandal: European Commission to Seek Privacy Guarantees from the US' (*The Guardian,* 10 June 2013) <https://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees≥ accessed 9 October 2021.
[15] Marcelo Corrales Compagnucci and others, 'Lost on the High Seas Without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After *Schrems II* Invalidation of the EU-US Privacy Shield' (2020) 4(3) European Pharmaceutical Law Review 153, 154-155.
[16] Leslie Hamilton, 'The Legal Environment' in Leslie Hamilton and Philip Webster (eds), *The International Business Environment* (4th edn, OUP 2018), 341.
[17] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176).
[18] Timo Minssen and others (n 12) 38.
[19] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'International Transfers of Health Data between the EU and USA: A Sector-Specific Approach for the USA to Ensure an 'Adequate' Level of Protection' (2020) 7(1) Journal of Law and the Biosciences 1.
[20] *Schrems II* (n 4).

'supplementary measures' that fill the gaps and bring it up to the level required by EU law. Unfortunately, the CJEU did not define or specify what these 'supplementary measures' are. [21] This permeated in heated debates and a wave of guidelines and recommendations on those additional safeguards.

3 RECENT DEVELOPMENTS AFTER *SCHREMS II*

After the *Schrems II* decision, on November 10th, 2020, the EDPB issued a six-step-approach Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The EDPB Recommendations are intended to help organisations comply with the requirements established by the CJEU in *Schrems II*. Following the Recommendations, on June 4th, 2021, the European Commission issued the long-awaited new SCCs for the transfer of personal data to third countries.[22] These two new developments are further explained below:

3.1 EDPB RECOMMENDATIONS: A SIX-STEP APPROACH

The EDPB recommends organisations to follow six steps to transfer personal data to third countries outside of the EEA:

> Step 1 – *Know your data transfers:* Data exporters should be fully aware of their transfers of personal data to third countries, including onward transfers. Mapping and recording all data transfers can be a complex task, however, this is necessary to ensure an essentially equivalent level of protection wherever it is processed. Data exporters should record all processing activities, keep data subjects informed and make sure it is in line with the principle of data minimisation.[23]
>
> Step 2 – *Identify the transfers tools you are relying on:* A second step is to identify the transfer tools set out in Chapter V of the GDPR including: a) adequacy decisions;[24] b) transfers tools containing 'appropriate safeguards' of a contractual nature in the absence of adequacy decisions (such as SCCs, Binding Corporate Rules (BCRs), codes of conducts, certification mechanisms and ad hoc contractual clauses);[25] and, c) derogations.[26] If your

[21] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data After *Schrems II*' (2020) 8(1) Journal of Law and the Biosciences 1.
[22] European Commission implementing decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3972 final.
[23] EDPB Recommendations 01/2020 (n 6), 8-9.
[24] See GDPR (n 1) art 45. Adequacy decisions may cover a country as a whole or be limited to a part of it. If you transfer data to any of these countries, there is no need to take any further steps described in this section. The EU Commission has so far recognised only twelve countries which can offer adequate level of protection. These countries are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. As of March 2021, adequacy talks were concluded with South Korea. See Commission, Adequacy decisions (n 3).
[25] GDPR (n 1) art 46. The transfer tools may require additional 'supplementary measures' to ensure essentially equivalent level of protection. See *Schrems II* (n 4), paras 130 and 133.
[26] GDPR (n 1) art 49.

data transfer does not fall under either a) 'adequacy decisions' or c) 'derogations', you need to continue to step 3.[27]

Step 3 – *Assess whether Art. 46 of the GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer:* Utilising a transfer tool under Art. 46 of the GDPR may not be sufficient if your transfer tool is not 'effective' in practice. 'Effective' means that the level of protection is essentially equivalent to that afforded in the EEA.[28] Data exporters should carry out a Transfer Impact Assessment (TIA) to assess – in collaboration with the importer – if the law and practice of the third country where the data is being transferred may impinge on the effectiveness of the appropriate safeguards of the Art. 46 in the context of the specific transfer. In performing this assessment, different aspects of the third country legal system should be taken into account, in particular whether public authorities can access personal data and, in general, those elements enlisted in Art. 45(2) of the GDPR[29] such as the rule of law situation and respect for human rights in that third country.[30]

Step 4 – *Adopt supplementary measures:* If the TIA revealed that your Art. 46 tool is not 'effective', data exporters – in collaboration with the importers, where appropriate – need to consider if 'supplementary measures' exist. By definition, supplementary measures are 'supplementary' to the safeguards that the transfer tools already provide. In other words, if added to the safeguards contained in Art. 46, could ensure that the data transferred is afforded an adequate level of protection in the third country which is essentially equivalent to the European standard. Exporters need to identify on a case-by-case basis which supplementary measures could be effective taking into account the previous analysis in steps 1, 2 and 3.[31]

Step 5 – *Formal procedural steps:* Make sure to take any formal procedural steps in case you have identified effective supplementary measures, which may vary depending on the transfer tool used or expected to be used. For instance, if data exporters intend to put in place supplementary measures in addition to the SCCs, there is no need to request an approval from the supervisory authority as long as the supplementary measures do not contradict, directly or indirectly, the SCCs and are enough to ensure that the level of protection guaranteed by the GDPR is not compromised in any way.[32]

Step 6 – *Re-evaluate at appropriate intervals:* The last step put forward by the EDPB is to monitor and review, on an ongoing basis, if there are new developments in the third country where data was transferred which could affect the initial assessment of the level of protection of the third country and the supplementary measures taken based on the TIA and the specific transfer. This is also in line with the principle of accountability which is a continuous obligation as set out in Art. 5(2) GDPR. Data exporters, in

[27] EDPB Recommendations 01/2020 (n 6) 9-11.
[28] See Schrems II (n 4), para 105 and second finding.
[29] ibid para 104.
[30] EDPB Recommendations 01/2020 (n 6) 12.
[31] ibid 15-17.
[32] ibid 17-18.

collaboration with the importers, should put in place sufficiently sound mechanisms to ensure that any transfer relying on the SCCs are suspended or prohibited if the supplementary measures are no longer effective in that third country or where those clauses are breached or impossible to honour.[33]

3.2 NEW STANDARD CONTRACTUAL CLAUSES (SCCs)

SCCs have a dual nature as a private contract and public instrument granting enforceable GDPR rights to third parties and subject to the oversight of the EU data protection authorities. They are intended to provide 'appropriate safeguards' under Art. 46 GDPR by creating legal obligations on the exporters and importers to ensure an appropriate level of data protection and GDPR compliance with respect to personal data transferred to countries which do not have adequacy decision (Art. 45 GDPR).[34] On June 4th, 2021, the European Commission released updated versions of the SCCs which reflect the GDPR requirements and take into account the legal analysis in the *Schrems II* decision. The Commission adopted two sets of SCCs, one for use between controllers and processors in the EU/EEA[35] and one for the transfer of personal data to third countries.[36]

The main innovations and salient points of the new SCCs can be summarised as follows:

A modular approach: Contrary to the prior set of SCCs which offered restricted possibilities of data transfers and separate sets of clauses, the new SCCs provide more flexibility for complex processing chains through a 'modular approach'. This means that data exporters and data importers can now choose the module that best applies to their needs within the same agreement.[37] In addition to the previously existing options for data transfers scenarios from 'controller to controller' and 'controller to processor', there are now two more modules governing data transfers from 'processor to processor'[38] and 'processor to controller'.[39]

Geographic scope of application: The new SCCs have a broader scope of application in comparison to the older version which only allowed the data exporter be a party if it was established in the EEA. This created barriers for data export compliance where a data exporter was established outside of the EEA but still subject to the GDPR by virtue of the GDPR's extraterritorial scope in Art. 3(2). According to the new SCCs, the data

---

33 EDPB Recommendations 01/2020 (n 6) 18-19.
34 Ian Lloyd, *Information Technology Law* (7th edn, OUP 2014), 183.
35 European Commission, Standard Contractual Clauses for controllers and processors in the EU (4 June 2021), available at: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors accessed 9 October 2021.
36 ibid.
37 Module 1: controllers to controllers, Module 2: controllers to processors, Module 3: processors to processors and Module 4: processors to controllers.
38 This is, for example, when there is a processor such as a cloud service provider located in the EEA and transfers data to another processor such as an infrastructure provider in the US.
39 In this case, the data is transferred back to the controller (back to 'its origin'). This is also sometimes referred as 'reverse transfer'.

exporter can also be a non-EEA entity. This provision, along with the modular approach, allows to cater any kind of data transfer between parties, despite of their data processing role or place of establishment.[40]

Multiparty clauses and docking clause: The new SCCs allow for multiple data exporting parties to contract (eg, within corporate groups or party collaborations) and for new parties to be added to them over time through the so-called 'docking clause' (Clause 7).[41] This clause is optional and allows additional third parties which are not (yet) a part of the agreement to join and sign up with the agreement of the other parties without having to conclude separate contracts. Third parties may now join by completing the Appendix – with details of the transfer, technical and organisational measures implemented and a list of sub-processors where relevant – and sign Annex 1.A.[42] This new mechanism provides a more flexible approach for the existing data processing practices, in particular in the context of acquisitions, additional corporate entities, and sub-processors.[43]

Data Protection Impact Assessment (DPIA): In response to the *Schrems II* ruling, companies must perform and document a mandatory DPIA that should include a data transfer impact assessment (TIA) and make it available to the competent supervisory authority upon request. The TIA should assess, for instance: i) whether the laws of the third country into which the data is imported could conflict with the SCCs and the GDPR, ii) whether any additional safeguards are necessary to enhance data protections (eg, implement supplementary technical measures). For example, a TIA should determine whether the data importer is subject to the US Foreign Intelligence Surveillance Act Section 702 (FISA 702).[44] The TIA should be monitored on a continuous basis and updated in light of any changes in the laws of the third country.

Security measures: Annex II of the new SSCs provides a more detailed list of examples of the technical and organisational measures necessary to ensure an appropriate level of protection, including measures to ensure the security of the data. While the list is non-exhaustive, it includes measures to provide assistance to the parties. According to Annex II, the technical and organisational measures must be described in 'specific (and not generic) terms'. This includes, in particular, any relevant 'certifications' to ensure an appropriate level of security, taking into consideration 'the nature, scope, context and

---

[40] Phillip Lee, 'The Updated Standard Contractual Clauses: A New Hope?' (*IAPP*, 7 June 2021) <https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/> accessed 9 October 2021.

[41] ibid.

[42] Alexander Milner-Smith, 'New Standard Contractual Clauses – what do you need to know?' (*Lewis Silkin,* 14 June 2021) <https://www.lewissilkin.com/en/insights/new-standard-contractual-clauses-what-do-you-need-to-know> accessed 9 October 2021.

[43] Martin Braun and others., 'European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data' (*WilmerHale,* 7 June 2021) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data> accessed 9 October 2021.

[44] Caitlin Fennessy, 'Data transfers: questions and answers abound, yet solutions elude' (*IAPP*, 12 February 2021) <https://iapp.org/news/a/data-transfers-questions-and-answers-abound-yet-solutions-elude/> accessed 9 October 2021.

> purpose of the processing, and the risks for the rights and freedoms of natural persons.' The measures of pseudonymisation and encryption are at the top of the list.[45]

There are several other new practical features in the new SCCs toolbox which provide more flexibility and legal certainty to the parties involved, such as the possibility to choose the governing law and jurisdiction of any EU Member State. This is particularly useful when the SCCs cover multiple international data transfers and servers are located in different countries. The new SCCs contain significantly more requirements and obligations for data exporters and importers, particularly for importers acting as controllers. This is also more in line with the GDPR requirements. The new SCCs include, for instance, obligations to give notice to data subjects and to notify personal data breaches to EU authorities.[46]

4 PRACTICAL CONSIDERATIONS

The CJEU ruled in *Schrems II* that the SCCs remain as a valid cross-border transfer mechanism provided the parties involved in the transfer implement the necessary 'supplementary measures' whenever they are needed to ensure substantially equivalent data protection by providing 'appropriate safeguards' to rectify any data protection gaps that undermine equivalency in the third countries.[47] Regrettably, the Court failed to provide any meaningful guidance about what specific supplementary measures might be required in this regard. In an attempt to fill this gap, the EDPB Recommendations provide a non-exhaustive list of factors to identify – in collaboration with the importer – which supplementary measures would be most effective in protecting the data transferred. The new SCCs provide a useful instrument to support cross-border data transfers in many situations (eg, cross-border transfers of clinical trial data).

SCCs are currently the primary mechanism for cross-border transfers of personal data among commercial entities. Unlike the country-specific adequacy rulings under Art. 45 GDPR which are at the purview of the Commission, SCCs were not designed as a stand-alone mechanism for data transfer based on the adequacy of data protection law in the country receiving the data. SCCs, and other Article 46 'appropriate safeguards,' such as Binding Corporate Rules (BCRs), were intended to offer an *alternative and additive*, multi-layered standard for data protection that utilises 1) the data protection law of the third party and addresses any gaps with respect to GDPR by adding 2) a customisable combination of legal, technological (eg, security measures), and organisational commitments to establish a safe and secure environment for cross-border data transfer beyond the EEA for situations where the third country does not have adequacy decision under Art. 45 GDPR.[48]

---

[45] See Annex II Standard Contractual Clauses (n 35).

[46] Carol Umhoefer and Andrew Serwin, 'European Commission's standard contractual clauses: extensive new requirements coming for US businesses receiving EU personal data subject to GDPR' (*DLA Piper*, 8 June 2021), <https://www.dlapiper.com/en/us/insights/publications/2021/06/european-commissions-standard-contractual-clauses-extensive-new-requirements/> accessed 9 October 2021.

[47] *Schrems II* (n 4) paras 103, 134.

[48] Laura Bradford and others 'Standard Contractual Clauses for Cross-Border Transfers of Health Data After (n 21).

The new SCCs are aligned with the GDPR and provide examples of technical and organisational measures in Annex III. They fill a long-existing gap in data protection law (since the former SCCs were adopted pre-GDPR), provide additional flexibility with regards to the permitted cross-border data-flows and help improve legal certainty for some international data transfers to third countries. It is expected that these modernised SCCs will enable businesses to account for a greater variety of complex data transfers and at the same time offering a safe exchange of personal data, adding uniformity and legal predictability to business transactions.[49] That said, in situations where an importer is subject to FISA 702 or similar public surveillance questions still remain. Specifically, what supplementary measures would be considered sufficient in such situations by the supervisory authorities or CJEU? Arguably, in conjunction with the SCCs the controller should at least 1) implement robust data minimisation to ensure the absolute minimum data needed for processing is transferred to the third country, 2) completely de-identify and encrypt the data transferred to the third country (both in transit and at rest encryption), 3) keep the encryption and pseudonymisation keys in the EU/EEA under the legal, organisational, and technical control of an EU party not subject to FISA (or other surveillance regime), 4) consider implementing multi-party encryption and processing (eg, multi-party homomorphic encryption), 5) implement a full information security management system (ISMS) such as the ISO 27001, and 6) document all these measures as part of Annex III of the SCC.

The use of the term 'supplementary measures' by the CJEU is unfortunate, as all these measures are technically part of the SCC security annex and were already needed to comply with the Art. 32 GDPR security of processing in light of part of the risk-based assessment (eg, Art. 35 GDPR, which provides for the DPIA). Furthermore, pursuant to Art. 46 the SCC is the 'appropriate safeguard' and these so-called 'supplementary measures' are technically not 'supplementary'. Instead, they are the same security measures that have always been documented and incorporated by reference as part of the SCCs.

In addition, organisations will have to pay particular attention to the new ISO 27701, which is the latest international standard for data privacy information management in the ISO 27000 series. It is a certifiable extension to the ISO 27001 that attempts to help organisations in meeting the GDPR requirements when implementing a comprehensive privacy information management system (PIMS). Organisations that have already implemented the ISO 27001 ISMS are advised to add privacy and data protection controls in ISO 27701 to ensure appropriate levels of data protection, especially when involved in cross-border transfers of personal data.[50]

There is a limited number of technical measures that could help organisations using SCCs to provide the European level of protection when the data is flowing around the world and possibly subject to public surveillance. These include 1) the use of robust end-to-end encryption with one or more independent EU/EEA-based trustees securely holding the keys, and 2) multi-

[49] European Commission, European Commission adopts new tools for safe exchange of personal data (4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847> accessed 9 October 2021.
[50] Luke Irwin, 'An Introduction to ISO 27701: The International Standard for Data Privacy,' (*IT Governance European Blog*, 20 April 2021) <https://www.itgovernance.eu/blog/en/iso-27701-the-new-international-standard-for-data-privacy> accessed 9 October 2021.

party homomorphic encryption.[51] Both of these security measures are technical controls and should be implemented within an overall ISMS[52] and PIMS[53] that is properly scoped and regulatory stress-tested (eg, subject to regular enhanced penetration testing). Additionally, it is important for the ISMS/PIMS to be independently audited (eg, subject to third-party ISO27001/27701 certification audits).

5 CONCLUSION

Arguably, the new SCCs raised the bar for data protection and security in international data transfers. Adopting and complying with this new legal framework may result in substantive legal, organisational and technical requirements for some parties. Businesses and organisations need to identify which transfer tools are already in place and be ready to migrate them to the new SCCs and working with data importers or exporters to ensure they are compliant. They should follow a risk-based approach and be ready to perform a DPIA and TIA taking into account the EDPB Recommendations and new SCCs requirements. Considering the increasing importance of data driven technologies and the global flow of data, as well as the ever-fiercer competition of emerging markets with less restrictive data protection regulations, it remains to be seen how these developments will affect the competitiveness of the European data innovation landscape and industry in a great variety of sectors.

[51] Marcelo Corrales Compagnucci and others, 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?', (2019) 3(4) European Pharmaceutical Law Review 144.
[52] Information Security Management System (ISO 27001).
[53] Privacy Information Management System (ISO 27701).

LIST OF REFERENCES

Bradford L, Aboy M and Liddell K, 'International Transfers of Health Data between the EU and USA: A Sector-Specific Approach for the USA to Ensure an 'Adequate' Level of Protection' (2020) 7(1) Journal of Law and the Biosciences 1.
DOI: https://doi.org/10.1093/jlb/lsaa055

— —, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data After *Schrems II*' (2021) 8(1) Journal of Law and the Biosciences 1.
DOI: https://doi.org/10.1093/jlb/lsab007

Braun M and others, European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data (7 June 2021), available at: https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data accessed 9 October 2021.

Chakravarty A and Colleen Fowler M, 'What Schrems are Made Of: The European Commission Adopts New Standard Contractual Clauses for International Data Transfers Covered by GDPR' (30 June 2021), available at: https://www.jdsupra.com/legalnews/what-schrems-are-made-of-the-european-3977830/ accessed 9 October 2021.

Corrales Compagnucci M, Minssen T, Seitz C, Aboy M, 'Lost on the High Seas Without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After *Schrems II* Invalidation of the EU-US Privacy Shield' (2020) 4(3) European Pharmaceutical Law Review 154.
DOI: https://doi.org/10.21552/eplr/2020/3/5

Corrales Compagnucci M, Meszaros J, Minssen T, Arasilango A, Ous T, Rajarajan M, 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?' (2019) 3(4) *European Pharmaceutical Law Review* 144.
DOI: https://doi.org/10.21552/eplr/2019/4/5

Fennessy C, Data transfers: questions and answers abound, yet solutions elude (12 February 2021), available at: https://iapp.org/news/a/data-transfers-questions-and-answers-abound-yet-solutions-elude/ accessed 9 October 2021.

Gellman B, 'Dark Mirror: Edward Snowden and the American Surveillance State' (Penguin Press 2020).

Hamilton L, 'The Legal Environment' in Hamilton L and Webster P (eds) *The International Business Environment* , (4th edn, OUP 2018).

Irwin L, 'An Introduction to ISO 27701: The International Standard for Data Privacy,' (20 April 2021), available at: https://www.itgovernance.eu/blog/en/iso-27701-the-new-international-standard-for-data-privacy accessed 9 October 2021.

Lee P, 'The Updated Standard Contractual Clauses: A New Hope?' (7 June 2021), available at: https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/ accessed 9 October 2021.

Lloyd I, *Information Technology Law* (7th edn, OUP 2014).
DOI: https://doi.org/10.1093/he/9780198702320.001.0001

Milner-Smith A, New Standard Contractual Clauses – what do you need to know? (14 June 2021), available at: https://www.lewissilkin.com/en/insights/new-standard-contractual-clauses-what-do-you-need-to-know accessed 9 October 2021.

Minssen T, Seitz C, Aboy M, Corrales Compagnucci M, 'The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the Legal Challenges and How Might These Affect Cloud-based Technologies, Big Data, and AI in the Medical Sector?' (2020) 4(1) European Pharmaceutical Law Review 39.
DOI: https://doi.org/10.21552/eplr/2020/1/6

Noyb, 'EU-US Data Transfers', available at: https://noyb.eu/en/project/eu-us-transfers accessed 9 October 2021.

Umhoefer C and Serwin A, 'European Commission's standard contractual clauses: extensive new requirements coming for US businesses receiving EU personal data subject to GDPR' (8 June 2021), available at: https://www.dlapiper.com/en/us/insights/publications/2021/06/european-commissions-standard-contractual-clauses-extensive-new-requirements/ accessed 9 October 2021.

Unstaran E, 'International Data Transfers' in *European Data Protection: Law and Practice,* 2nd Edition (IAPP Publication), 527.

Watt N, 'Prism Scandal: European Commission to Seek Privacy Guarantees from the US' (10 June 2013), available at: https://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees accessed 9 October 2021.

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).

EU DATA PROTECTION AND THE PRINCIPLE OF PROPORTIONALITY

ESTER HERLIN-KARNELL*

This paper explores the principle of proportionality in the context of EU data protection. The paper starts by setting out the basics of EU data protection at the EU level and explains why it is so interesting in the context of proportionality. The paper will briefly set out some of the main debate on proportionality before looking at some recent EU cases on data protection where the principle of proportionality has played a key role. The final part of the paper uses the Swedish derogations from the GDPR as a test case of a lack of proportionality.

1 INTRODUCTION

Why is data protection interesting from the perspective of proportionality? Or perhaps I should ask why proportionality is interesting from the perspective of data protection? The principle of proportionality has played a pivotal role in recent EU data protection cases.

This is not strange considering that in EU law, data protection is formulated as a right. Consequently, the right to data protection is codified in Article 16 TFEU and in Article 8 EU Charter. In addition, Article 7 EU Charter stipulates the right to privacy, communication and family life, and Article 8 ECHR also sets a general right to privacy, communication, home and family life.

It seems that the question of data protection is extremely important in the context of exactly proportionality, perhaps it is the most important principle for our understanding of the reach of data protection in the EU context. The notion of proportionality is of course a golden rule in EU law. Specifically, the principle of proportionality in EU law is taken to mean balancing the means and ends, in which the notion of appropriateness constitutes the golden thread for deciding on the desirability and need for EU action. Thus, proportionality is a classic in EU law and is one of the most crucial general principles, one which is used both as a sword and as a shield, usually in the context of to what degree the Member States could derogate from their EU law obligations. But it also constitutes one of the leading principles for deciding on whether EU legislative competence is warranted.[1]

The notion of proportionality is not an entirely straightforward principle, however. For example, Article 52 EU Charter makes it clear that any permissible derogations by Member States from EU law obligations as set out in the Charter, are contingent on proportionality. In other words, proportionality is a doubled edged sword: the same principle of proportionality is protecting individual rights in a positive sense can also be used to limits

* Professor of EU Law, University of Gothenburg. The paper was presented at the conference on 'The consequences of *Schrems II* from practical and theoretical perspectives', 16 September 2021, Faculty of Law, University of Lund.

[1] In the context of data protection and proportionality see the chapters in Ulf Bernitz and others (eds), *General Principles of EU Law and the EU Digital Order* (Wolters Kluwer 2020). On proportionality in general and EU law, see, eg, Takis Tridimas, *General Principles of EU Law* (OUP 2012), chs 3–5.

those rights. In other words, the Member States could invoke proportionality to derogate from the rights guaranteed in the Charter (Article 52). Proportionality appears to play a key role with regard to the Charter of Fundamental Rights more generally, both in its scope and in its application.

Many scholars have, of course, been interested in proportionality for a long time and there are very good reasons for such an extensive interest in the contours of proportionality. After all, the principle of proportionality has been viewed as intrinsic to the rule of law, and even as the ultimate rule of law.[2] Moreover, for example, Mattias Kumm has observed that '[o]ne important function of proportionality analysis is to function as a filter device that helps to determine whether illegitimate reasons might have tilted the democratic process against the case of the rights-claimant'.[3]

Recently there has also been an increased interest in the similarities between the doctrine of the principle of proportionality and that of a right to justification advocated by Rainer Forst.[4] The point of justification is that individuals have a right to reasoned decisions, and the function of courts is to assess whether the public authority taking the decision in question can be justified by public policy. Thus, the question of good reason is perhaps most clearly identified in the principle of proportionality, which functions as a justification tool.[5] In addition, Mattias Kumm has referred to proportionality reasoning as a form of 'Socratic contestation', which refers to the practice of critically engaging authorities in order to assess whether the claims that they make are based upon good reason.[6] Why is this so? In order to give the notion of justification concrete meaning in a legal context, it is often suggested we need to understand the principle of proportionality.[7] This is because the principle of proportionality is an expression of the right to justification and could be connected to the idea of justice (at least in the legal sense) and the bigger issue of good governance.

This paper will set out to examine the importance of the principle of proportionality and the role it plays in the area of EU data protection cases. The paper will briefly explain what the principle of proportionality entails and will turn to some recent EU cases on data protection where the principle of proportionality has played a key role. The final part of the paper uses the Swedish derogations from the GDPR as a test case of a lack of proportionality.

---

[2] David M Beatty, *The Ultimate Rule of Law* (OUP 2004) 56; Aharon Barak, *Proportionality: Constitutional Rights and their Limitations* (CUP 2012).

[3] Mattias Kumm, 'Alexy's Theory of Constitutional Rights and the Problem of Judicial Review' in Matthias Klatt (ed), *Institutionalized Reason: The Jurisprudence of Robert Alexy* (OUP 2012).

[4] Rainer Forst, *The Right to Justification: Elements of a Constructivist Theory of Justice* (Columbia University Press 2012).

[5] For recent studies of proportionality, see, eg, Eon Daly, 'Republicanizing Rights? Proportionality, Justification and Non-Domination' in Ester Herlin-Karnell and others (eds), *Constitutionalism Justified: Rainer Forst in Discourse* (OUP 2019).

[6] Mattias Kumm, 'The Idea of Socratic Contestation and the Right to Justification: The Point of Rights-based Proportionality Review' (2010) 4(2) Law & Ethics of Human Rights 141.

[7] See, for example, Barak (n 2); Jud Mathews and Alec Stone Sweet, 'All Things in Proportion? American Rights Doctrine and the Problem of Balancing' (2010) 60 Emory Law Journal 797; Kai Möller, *The Global Model of Constitutional Rights* (OUP 2012); Moshe Cohen-Eliya and Iddo Porrat, *Proportionality and Constitutional Culture* (CUP 2013); Jacob Weinrib, *Dimensions of Dignity: The Theory and Practice of Modern Constitutional Law* (CUP 2016) ch 7.

2 THE GRAND DEBATE ON PROPORTIONALITY IN A NUTSHELL[8]

The principle of proportionality has been key to the development of EU law and plays a central role in constitutional law in general. Proportionality reasoning is then connected not only to the question of the quality of arguments, but also to the question of reasonable disagreement.[9] In this regard the idea of proportionality is closely linked to justice-based reasoning. For example, applying a Rawlsian account to the theory of justice would, probably, imply using reasonableness as an adequate standard for measuring legitimacy at EU level.[10] As Malcolm Thorburn argues, courts assess justifications by asking whether the infringement was prescribed by law, and whether it was undertaken in furtherance of a legitimate state purpose. These considerations play an essential part in the justification process. Taken together, they mean that no one can use the powers of the state to infringe constitutional rights on his or her own private say-so (where the act was not prescribed by law) or for his or her own private purpose (rather than a legitimate public purpose). Furthermore, the requirement of a legitimate state purpose also excludes any purpose that is at odds with the regime of constitutional rights.[11] Yet for Robert Alexy, for example, the reasonableness test is not sufficient, in that there are cases which require a much closer review than an absurdity test in terms of what is to be counted as 'reasonable' can provide.[12] Therefore, for him, correctness as a regulatory idea means that it is open to future argumentation and strives towards the dimension of the absolute.

With regard to the EU, as noted, the Member States could invoke proportionality to derogate from the rights guaranteed in the Charter since Article 52 applies to all rights. Yet, the Charter refers to the ECHR in Article 52(3) in pointing out that the ECHR is always the minimum standard of protection, which means that also the EU Charter treats absolute rights as 'absolute'. The assumption is that interference with EU law rights should be kept to a minimum, in which the test is to ascertain whether it has been manifestly disproportionate to interfere with these rights. The CJEU will inquire as to whether the measure was suitable or appropriate to achieve the desired result or whether this could have been attained by a less onerous method. Proportionality is therefore a general review in EU law that is applicable to test the legality both of EU action, and of Member State action when the latter falls within the ambit of the Treaty.[13] While the principle of proportionality is part of the EU's arsenal for deciding on legislative authority for the EU legislator, it is also a principle that is addressed to individuals in the freedom of movement context. This is usually called the strict proportionality test of the otherwise rather state-centric proportionality test. Hence, the individual plays an increasingly important role in the EU context. For example, Article 3 TFEU makes it clear that not only is the Union to aim to promote the well-being of its

[8] This section builds on Ester Herlin-Karnell, *The Constitutional Structure of Europe's Area of Freedom, Security and Justice and the Right to Justification* (Hart Publishing 2019) ch 4.
[9] John Rawls, *Justice as Fairness: A Restatement* (Harvard University Press 2001).
[10] ibid.
[11] Malcolm Thorburn, 'Proportionality' in David Dyzenhaus and Malcolm Thorburn (eds), *Philosophical Foundations of Constitutional Law* (OUP 2016).
[12] Robert Alexy, 'The Absolute and the Relative Dimensions of Constitutional Rights' (2017) 37(1) Oxford Journal of Legal Studies 31.
[13] Paul Craig, 'Proportionality, Rationality and Review' [2010] New Zealand Law Review 265.

peoples, but it is also to offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to, among other things, the prevention and combating of crime. This implies a balance not only vis-à-vis the EU and its Member States, but also between the individual and the EU.[14]

The principle of proportionality is designed for looking at the question of the reason for any derogations and on the question of what counts as good reasons. Thus, the question of 'good reason' is very important as proportionality functions as a justification tool in this regard. But, who decides which reasons are good enough? For Forst, 'good reasons are not to be found in ethical principles alone, but in an evaluative space of communal values and self-understanding'.[15] In this way, discourse truly articulates what belongs to the character of the community. For him, this means that a good reason is a substantive one and is, as such, ethical, as a citizen needs to understand himself or herself as part of a community which is internally connected to the common good. Forst anchors this in the idea of legitimacy. The main commitment would not be to democracy itself, but to the values that a community holds dear, meaning that democracy is not autonomous, but is itself ruled by communal values.[16]

Notwithstanding the attractiveness of proportionality as a judicial principle, proportionality is often attacked on the grounds that it involves judicial weighing of incommensurables, and thereby erodes rights. Moreover, it is often accused of being far too pragmatic and thus simply too mechanical as a legal principle. The argument hinges on the concern that moral values cannot be adequately balanced, as the interests at stake cannot actually be weighed on any sort of scale.[17] In short, critics argue that there is too much ambiguity with the pathologies of the proportionality test, and that it fails to deliver what it promises, namely, that, contrary to what some scholars argue, it increases neither transparency nor rationality, and thus has no legitimacy. Another critique is that often not enough information is, empirically speaking, available in the proportionality cases, which makes it difficult to rule on the facts and strike a balance.[18] The principle of proportionality much like justice, is vulnerable to the critique that its political dimension means that it is not amenable to judicial review.

What then justifies giving so much power to courts? According to some scholars in order to determine more precisely when the competence of courts is supported by democratic legitimacy, we may employ the three key values of democracy: accountability; participation; and equality.[19] As Matthias Klatt has described it: 'The more serious a limitation of rights is, the more intense should be the review engaged in by the court'.[20] But, as David Beatty notes:

---

[14] Tridimas (n 1).
[15] Forst (n 4) 172, discussing Taylor's work - see, eg, Charles Taylor, *The Ethics of Authenticity* (Harvard University Press 1992).
[16] Forst (n 4) 173.
[17] Timothy Endicott, 'Proportionality and Incommensurability' (2012) No 40/2012 Oxford Legal Research Papers.
[18] Bernhard Schlink, 'Proportionality in Constitutional Law: Why Everywhere but Here?' (2012) 22 Duke Journal of Comparative and International Law 291.
[19] Matthias Klatt, 'Positive Rights: Who Decides? Judicial Review in Balance' (2015) 13(2) International Journal of Constitutional Law 354.
[20] ibid.

> Although it would seem to count in favour of the proportionality principle that it satisfies Dworkin's twin criteria of 'fit' and 'value' better than any rival theory, some may worry that its empirical and moral claims leave it open to a fundamental, potentially fatal objection.[21]

Clearly, the debate is connected to the classic debate in constitutional theory about the legitimacy of judicial review and to what extent rights can be limited. The idea of a 'justification-blocking function' of human rights is akin to Dworkin's view of human rights as trumps that can be deployed against policy arguments in legal discourse.[22] He points out that 'Rawls argues that: "Each person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override"'.[23] Also, Jürgen Habermas cautions against reducing the idea of human rights to policy arguments, observing that: 'if in cases of collision all reasons can assume the character of policy arguments, then the fire wall erected in legal discourse by a deontological understanding of legal norms and principles collapses'.[24]

Regardless of the answer to the big question of how much proportionality and how much judicial review and what it tells us about the legitimacy of the system, it is clear that the EU court acts as a constitutional court with regard to the data protection cases.

3 RECENT CASES ON PROPORTIONALITY AND DATA PROTECTION

Why then is proportionality so central in the context of EU data protection?

The principle of proportionality has played a key role for ensuring data protection. After all, the recent case of for example the *Digital Rights case*,[25] and the *Schrems* and *Tele 2 Sverige* cases are instructive as they stress the importance of data protection and proportionality. In *Digital Rights*, the Court annulled the 2006 Data Retention Directive, which was aimed at fighting crime and terrorism, and which allowed data to be stored for up to two years. It concluded that the measure breached proportionality on the grounds that the Directive had too sweeping a generality and therefore violated, inter alia, the basic right of data protection as set out in Article 8 of the Charter. The Court pointed out that access by the competent national authorities to the retained data was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data to what was strictly necessary for the purpose of attaining the objective pursued. Nor did it lay down a specific obligation on Member States designed to establish such limits. The EU legislator had provided insufficient justification – it was simply not good enough from the perspective of EU fundamental rights protection

The approach was confirmed in *Schrems I*[26] and subsequently in *Schrems* 2 and *Tele 2 Sverige*, where the Court held that:

---

[21] Beatty (n 2) 176; Ronald Dworkin, *Law's Empire* (Hart Publishing 1998).
[22] Yutaka Arai-Takahashi, 'Proportionality' in Dinah Shelton (ed), *The Oxford Handbook of International Human Rights Law* (OUP 2013) ch 19.
[23] ibid.
[24] Jürgen Habermas, *Between Facts and Norms* (Oxford: Polity Press 1996) 258–9, also discussed in Arai-Takahashi (n 22).
[25] Opinion of Advocate General Cruz Villalón, Case C-293/12 *Digital Rights Ireland and Seitlinger and Others (Digital Rights)* ECLI:EU:C:2013:845.
[26] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner (Schrems I)* ECLI:EU:C:2015:650.

> [L]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

In view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict. Both the AG and the Court in *Schrems II* stressed that according to Article 52(1) of the Charter, any limitation on the exercise of the rights recognised by the Charter must genuinely meet an objective of general interest recognised by the Union. Article 8(2) of the Charter also provides that any processing of personal data that is not based on the consent of the person concerned must have a 'legitimate basis laid down by law'. The AG pointed out Article 8(2) of the ECHR lists the aims capable of justifying interference with the exercise of the right to respect for private life.

So in *Schrems II,* the Court held that, it follows from the judgment in *Schrems I* that

> legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the [data] without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.[27]

These findings were also confirmed in Opinion 1/15 where the Court annulled a pending Agreement between Canada and the EU on the transfer and processing of Passenger Name Record (PNR) data.[28] Here the Court held that the Agreement granted too sweeping a purpose of fighting terrorism without concrete justification in the individual case just simply a general concern of public security and without respecting private life and data protection (Articles 7 and 8 of the Charter, Article 16 TFEU) and proportionality (Article 52 of the Charter).

Moreover, the important role of proportionality was once again confirmed in the recent case of *Privacy International* affirming that mass surveillance without any justification or concrete suspicion presented, much in line with the *Digital Rights* case, mentioned above, is contrary to EU data protection as it does not stand the proportionality test.[29] Similarly, in *La Quadrature du Net*, an obligation requiring the general and indiscriminate retention of traffic

---

[27] Summary of Case C-311/18 Facebook Ireland and Schrems (*Schrems II*) ECLI:EU:C:2020:559, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=182494&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=97149> accessed on 11 December 2021, para 8 (with reference to paras 91-95 of *Schrems II* judgment).

[28] Opinion 1/15 *On the draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (Opinion 1/15)* ECLI:EU:C:2017:592.

[29] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (Privacy International)* ECLI:EU:C:2020:790.

and location data is incompatible with the Charter.[30] The Court emphasized that legislation which permits the general and indiscriminate transmission of data to public authorities entail general access and that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society.[31]

The crucial point here is that the proper application of proportionality functions as a rebuttal to the EU legislator or the Member States, if the reasons provided are not deemed good enough. When constitutional rights are at stake, there needs to be a good justification for relying on trust. Therefore, as noted it could be argued that the scope of data protection under the Charter turns on the width of the proportionality principle. Although the Member States could invoke proportionality to derogate from the rights guaranteed in the Charter, since Article 52 applies to all rights, there are limits in the light of dignity and the rule of law (EU law principles). Nonetheless, the explanatory memorandum on the Charter confirms that these exceptions are based upon the Court's well-established case law that restrictions may be imposed on the exercise of fundamental rights.[32]

While the principle of proportionality is part of the EU's arsenal for deciding on the legislative authority for the EU legislator, it is also a principle that is addressed to individuals in the free movement context. This is usually called the strict proportionality aspect of the otherwise rather state-centric proportionality test.

In Opinion 1/15 where the Court annulled a pending Agreement between Canada and the EU on the transfer and processing of Passenger Name Record (PNR) data.[33] The Court held that the Agreement granted too sweeping a purpose of fighting terrorism without concrete justification in the individual case just simply a general concern of public security and without respecting private life and data protection (Articles 7 and 8 of the Charter, Article 16 TFEU) and proportionality (Article 52 of the Charter). The PNR Agreement would have permitted data retention for up to five years.[34] The Court specifically stated that the Agreement needs to limit the retention of passenger name record after departure to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism.[35]

Much of EU law is contingent on the proportionality principle, as it is concerned with constitutional rights: it could be argued that the scope of EU human-rights protection under the Charter seems to turn on the width of the proportionality principle. After all, the Member States could invoke proportionality to derogate from the rights guaranteed in the Charter and this applies to all rights. The explanatory memorandum on the Charter confirms that these exceptions are based upon the Court's well-established case law that restrictions may

[30]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

[31] The Court refers to Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter.

[32] Explanations relating to the Charter of Fundamental Rights (Explanations to the EU Charter) [2007] OJ C303/17.

[33] *Opinion 1/15* (n 28).

[34] ibid paras 154–78.

[35] ibid para 232.

be imposed on the exercise of fundamental rights.[36] The explanatory notes also make it clear that the reference to the general interests recognised by the Union covers both the objectives mentioned in Article 3 TEU and other interests protected by specific provisions of the Treaties provided that those restrictions do, in fact, correspond to the objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference which undermines the very substance of those rights.[37] Indeed, the Charter refers to the ECHR in Article 52(3) in pointing out that the ECHR is always the minimum standard of protection.

4 SWEDEN AS A TEST CASE OF (MISSING) PROPORTIONALITY

As I have previously argued in this journal, the Swedish system is an interesting case of (what I would call) a flagrant breach of the GDPR and primary EU law when it comes to data protection.[38] More specifically, Sweden has a very peculiar system with regard to EU data protection and one which is very interesting in the context of proportionality. Anyone who buys a publishing license from the state is exempted from the GDPR, the argument goes, because it gives them the freedom of expression and the right to publish.[39] Largely absent from this claimed derogation from the GDPR, however, is the question as to whether the Swedish exception breaches primary EU law on data protection (Article 16 TFEU and Article 8 EU Charter), as well whether the exception from the GDPR is proportionate. Buying a license without much scrutiny gives a carte blanche to share information about individuals.[40] This seems not only wrong but also a disproportionate weight between different rights (ie, the right to publish if you buy a license and the right to data protection of individuals). The problem here is not about journalistic freedom because traditional media is bound by press ethics, while companies that buy a license get access to bulk data of all Swedish residents. The companies in turn can sell the data and make it available on the internet, thereby infringing EU data protection. In addition, these private actors who buy those licenses can earn a profit from advertisement when publishing information about individuals and in certain cases they even sell the information.[41] This seems not to be about freedom of expression and of the right to publish (as important rights in a democratic society), but rather about conducting business. Likewise, if the argument is one of general concern for freedom of expression and rights in the Swedish constitution (grundlagen) there is something important missing here, namely a proportionality assessment as there needs to be a balance between competing rights. Any derogations from EU law must be justified. In addition, it seems strange to favour business over individual data protection (and of course if people agree to have their personal data published on the internet, it is no problem). Therefore, if there is no consent at least there has to be a proportionality assessment, and a balance between a Swedish 'right' to buy information and publish it and that of an individual's right

[36] Explanations to the EU Charter (n 32).
[37] ibid.
[38] Ester Herlin-Karnell, 'EU Data protection Rules and the Lack of Compliance in Sweden' (2020) 3(2) NordicJournal of European Law 95.
[39] Myndigheten för press, radio och tv, 'Utgivningsbevis' <http://www.mprt.se/sv/att-sanda/internetpublicering/utgivningsbevis/> accessed 11 December 2021.
[40] ibid, it costs SEK 2,000 for a licence obtaining.
[41] See, eg, MrKoll.se website (*Bättre koll på privatpersoner*) <https://mrkoll.se> accessed 11 December 2021.

to private life, dignity and data protection according to EU law. And of course, EU law is primary to national law.

There is also an external dimension. As explained above, in several recent cases such as *Digital Rights* and *Schrems 1 & 2*, the CJEU has stressed the EU's data protection rules cannot be derogated from without any justification. The proportionality review and the need to secure equivalent protection of data protection in cooperation with third states is interesting in the Swedish case. When data is published online it also become a global question as the data is available to third countries also. From this perspective it could be argued that, actually, EU data protection rules are not complied with when it comes to the importance of upholding EU standards with regard to third states. Therefore, it could be questioned whether data protection in the EU is not lived up to vis-à-vis third countries.[42]

5 CONCLUSION

The principle of proportionality continues to play a central role in EU integration. It appears to be a key principle in the area of data protection. This is neither strange or new: EU data protection is treated as a constitutional right and the principle of proportionality is used as a balancing principle balancing different rights at the constitutional level – and boils down to what we make of the proportionality test.

The idea that Member States can derogate from constitutional duties, if it can be justified, is a common feature of human rights law including EU law. Article 16 TFEU and Article 8 the Charter are formulated as rights. It should also be stressed that in the *Schrems 1 & 2* the Court held that:

> [L]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[43]

The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities (Article 2 TEU). But how this is achieved at EU level is trickier. And this is where the role of courts and the application of proportionality is both interesting and important.

Clearly, the debate is connected to the classic debate in constitutional theory about the legitimacy of judicial review. The balancing test is surely the most important aspect of the principle of proportionality when applied in the context of EU data protection. As the case of Sweden demonstrates with regard to the peculiar system of publishing license and where national practice is considered to stand above EU law on data protection, what is largely missing to the Swedish debate is exactly the principle of proportionality and the supremacy of EU law.

---

[42] Herlin-Karnell (n 38).
[43] *Schrems II* (n 27) para 187, with reference to *Schrems I* (n 26) para 95.

LIST OF REFERENCES

Alexy R, 'The Absolute and the Relative Dimensions of Constitutional Rights' (2017) 37(1) Oxford Journal of Legal Studies 31.
DOI: https://doi.org/10.1093/ojls/gqw013

Arai-Takahashi Y 'Proportionality' in Shelton D (ed), *The Oxford Handbook of International Human Rights Law* (OUP 2013).

Barak A, *Proportionality: Constitutional Rights and their Limitations* (CUP 2012).

Beatty D M, *The Ultimate Rule of Law* (OUP 2004).
DOI: https://doi.org/10.1093/acprof:oso/9780199269808.001.0001

Bernitz X, Groussot X, Paju J, de Vries S (eds.), *General Principles of EU Law and the EU Digital Order* (Wolters Kluwer 2020).

Cohen-Eliya M and Porrat I, *Proportionality and Constitutional Culture* (CUP 2013).
DOI: https://doi.org/10.1017/cbo9781139134996

Craig P, 'Proportionality, Rationality and Review' (2010) New Zealand Law Review 265.

Daly E, 'Republicanizing Rights? Proportionality, Justification and Non-Domination' in Herlin-Karnell E, Klatt M, Morales Zúñiga H A (eds), *Constitutionalism Justified: Rainer Forst in Discourse* (OUP 2019).
DOI: https://doi.org/10.1093/oso/9780190889050.003.0009

Dworkin R, *Law's Empire* (Hart Publishing 1998).

Endicott T, 'Proportionality and Incommensurability' (2012) No 40/2012 Oxford Legal Research Papers.

Forst R, *The Right to Justification* (Columbia University Press 2012).

Habermas J, Between Facts and Norms (Oxford: Polity Press 1996).
DOI: https://doi.org/10.7551/mitpress/1564.001.0001

Herlin-Karnell E, 'EU Data protection Rules and the Lack of Compliance in Sweden' (2020) 3(2) Nordic Journal of European Law 95.
DOI: https://doi.org/10.36969/njel.v3i2.22395

— —, *The Constitutional Structure of Europe's Area of Freedom, Security and Justice and the Right to Justification* (Hart Publishing 2019).
DOI: https://doi.org/10.5040/9781509912520

Klatt M, 'Positive Rights: Who Decides? Judicial Review in Balance' (2015) 13(2) International Journal of Constitutional Law 354.
DOI: https://doi.org/10.1093/icon/mov019

Kumm M, 'Alexy's Theory of Constitutional Rights and the Problem of Judicial Review' in Klatt M (ed), *Institutionalized Reason: The Jurisprudence of Robert Alexy* (OUP 2012).
DOI: https://doi.org/10.1093/acprof:oso/9780199582068.003.0009

— —, 'The Idea of Socratic Contestation and the Right to Justification: The Point of Rights-based Proportionality Review' (2010) 4(2) Law & Ethics of Human Rights 141.
DOI: https://doi.org/10.2202/1938-2545.1047

Stone Sweet M, 'All Things in Proportion? American Rights Doctrine and the Problem of Balancing' (2010) 60 Emory Law Journal 797.

Möller K, *The Global Model of Constitutional Rights* (OUP 2012).
DOI: https://doi.org/10.1093/acprof:oso/9780199664603.001.0001

Rawls J, *Justice as Fairness: A Restatement* (Harvard University Press 2001).

Schlink B, 'Proportionality in Constitutional Law: Why Everywhere but Here?' (2012) 22 Duke Journal of Comparative and International Law 291.

Taylor C, *The Ethics of Authenticity* (Harvard University Press 1992).
DOI: https://doi.org/10.2307/j.ctvv41887

Thorburn M, 'Proportionality' in Dyzenhaus D and Thorburn M (eds), *Philosophical Foundations of Constitutional Law* (OUP 2016).
DOI: https://doi.org/10.1093/acprof:oso/9780198754527.003.0016

Tridimas T, *General principles of EU Law* (OUP 2012).

Weinrib D, *Dimensions of Dignity: The Theory and Practice of Modern Constitutional Law* (CUP 2016).

TOLERATING AMBIGUITY: REFLECTIONS ON THE *SCHREMS II* RULING

SUSANNA LINDROOS-HOVINHEIMO*

This paper considers the European Court of Justice's Schrems II ruling from a variety of angles. From a strictly legal point of view, considering the GDPR, the CJEU came to a logical conclusion. In this paper, I nevertheless try to think about other ways of understanding the dispute and the ruling. In addition to data protection law, the case is about surveillance, platform power, resistance, global politics, data territoriality and the Court's competence. These sensitive issues come forth when the strict data protection issues are set aside and a slightly more open analysis undertaken. In the end, however, the ruling does bring about real-life problems that pertain to data protection law. Transfers of data to third countries are a pressing problem that no one seems to know how to solve.

1 INTRODUCTION

On 16 July 2020, the Court of Justice at the European Union (CJEU) gave a preliminary ruling in the so-called *Schrems II* case.[1] The request had been made by the High Court in Ireland and concerned the legality of data transfers by Facebook Ireland to Facebook Inc., that is, transfers from the EU to the US.

The ruling is rather complex, and here my focus is only on certain key aspects. Firstly, the EU Court decided that the matter falls under EU law and the GDPR[2] because it does not concern Member States' national security. Secondly, the Court found that the Commission's decision on guidelines for Standard Contractual Clauses (SCCs)[3] is valid. These clauses are one means by which personal data can lawfully be transferred to third countries. The third conclusion by the Court – and the one that has received the most attention – concerns the Commission's Privacy Shield decision on the adequacy of data

* Professor, Faculty of Law, University of Helsinki (Finland). This article is based on a presentation delivered at the seminar *Schrems II and its Practical and Theoretical Consequences* held in Lund 16 September 2021, which was organised by Xavier Groussot. I thank Professor Groussot and Lund University for the kind invitation to participate.

[1] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559.

[2] 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 L 119/1.

[3] 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 Council [2010] OJ L39/5, as amended by Commission Implementing Decision 2016/2297 (SCC Decision) [2016] OJ L344/100 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.

protection rights provided by the US.[4] The Court found that the decision is invalid because the US does not provide adequate protection.

From a data protection point of view, there is little to criticise in the judgment – if one belongs to the majority of academic data protection lawyers, who see the right to personal data as a good thing. In this ruling, the Court takes a logical step in the direction in which data protection law has been developing for a long time. The argumentation picks up where the first *Schrems* ruling[5] left off. There are no real surprises. The Court's reasoning respects the law – the GDPR – and provides no innovative or radical interpretations. The legislators' wishes were heard.

The legislators have been active indeed. Data protection is one area of fundamental rights protection areas – perhaps even *the* area – in which the Union has really made a difference. Our right to privacy would look very different if it were not for the active steps that the EU has taken. The individual's right to personal data is almost a trump card now; when it is in danger, the law does not hesitate. Many political and ideological obstacles have been overcome to achieve this level of protection and it stays strong under the Court's watchful eye. The *Schrems* rulings are one indicator of this general trend.

However, on closer inspection, the case proves puzzling. In this paper, I offer impressions of what the case is about, as well as what it brings about.

So, what happens in the case? There are several alternatives for interpreting it. The dispute touches on surveillance, data transfers, platform power, data protection authorities' duties, resistance, global politics, data territoriality, individualism, as well as the Court's competence. And it brings about a situation wrought with ideological, political and practical problems. In my view, the ruling of the EU Court seems to be riddled with ambiguities and it leaves quite a few questions unanswered.[6]

2 SURVEILLANCE OR SURVEILLANCE CAPITALISM?

I situate this analysis within the conceptual landscape of surveillance capitalism. In Shosanna Zuboff's critique,[7] massive data gathering causes privacy intrusions that produce new forms of capitalist exploitation. She calls this surveillance capitalism. A new kind of economic gain is derived from data, especially personal data. Tech giants, but also other kinds of commercial operator, are the ones to blame. They exploit us and turn our private information into data that has commercial value. Ever more efficient marketing of goods and services is their primary target, and they do not even shun brainwashing for consumerist purposes.

---

[4] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection [2016] OJ L 207/1 provided by the EU-US Privacy Shield is invalid.

[5] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650.

[6] For interesting analyses, see also, eg, Maria Helen Murphy, 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) International and Comparative Law Quarterly 2021 1; Jockum Hildén, 'Mitigating the risk of US surveillance for public sector services in the cloud' (2021) 10(3) Internet Policy Review 2; Roisin Aine Costello, '*Schrems II*: Everything Is Illuminated?' (2020) 5 European Papers 1045; Andraya Flor, 'The Impact of *Schrems II*: Next Steps for U.S. Data Privacy Law' (2020-2021) 96 Notre Dame Law Review 2035; Jan Xavier Dhont, 'Editorial, *Schrems II*. The EU adequacy regime in existential crisis?' (2019) 26(5) Maastricht Journal of European and Comparative Law 597.

[7] Shoshana Zuboff, *The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power* (London: Profile Books 2019).

However, what Mr. Schrems is after in the *Schrems* cases at the CJEU is to combat something else. His ultimate critique is directed towards the surveillance authorities of third countries, most specifically the US. He is concerned with the widespread privacy breaches that are perpetrated by spying agencies. It is noteworthy that the *Schrems* rulings are not aimed at hindering surveillance capitalism, but surveillance as such, the kind of surveillance that government institutions do mainly for national security purposes. Neither Mr. Schrems nor the Court have a problem with the massive data gathering that Facebook does in Europe. Transferring data overseas is the problem.

Hence, in a surveillance capitalist framework we see that capitalism comes away unscathed. The traditional version of surveillance is the target here, not the surveillance capitalism for economic profit that Zuboff describes. Mr. Schrems has nothing against that. Hence, the set-up of the *Schrems* cases amounts to the conclusion that it is fine if Facebook does the surveillance in Europe, but it is not fine if public authorities in the US have unlimited and unchecked powers to access the data for their surveillance purposes.

The scenario can be compared with the German Facebook competition law case,[8] and the Commission investigation[9] into Facebook's actions on the European market. In these proceedings, it is assessed whether Facebook violates EU competition rules. According to the German authorities, Facebook collects user and device-related data from sources outside of Facebook and merges it with data collected on Facebook, which constitutes an abuse of a dominant position on the social network market in the form of exploitative business terms.[10] This legal perspective on Facebook's operations has emerged recently and is more closely tied to the critique of new forms of capitalism than the *Schrems* cases. In this sense, the *Schrems* rulings may be slightly disappointing. They provide no real objection to the capitalist operations of large platform companies.

3 LEGAL BASIS

It is interesting to note that a large part of the disagreement between Mr. Schrems and Facebook concerns the legal basis for the data transfers. Let us remind ourselves of how the story started. First, in 2013, Mr. Schrems made a formal complaint to the Data Protection Commissioner in Ireland that Facebook Ireland unlawfully outsources data processing operations to Facebook Inc. (Facebook Ireland's parent company). In 2013 the Data Protection Commissioner refused to investigate the complaint, arguing that it was bound by the Safe Harbour Decision made by the Commission. This decision allowed for data transfers to the US. Mr. Schrems initiated proceedings against the Data Protection Commissioner, and the High Court made the first reference to the CJEU.

In the *Schrems I* ruling from 2015, the EU Court invalidated the Safe Harbour Decision. Following the judgement, the High Court remitted the matter back to the Data Protection Commissioner who should investigate 'promptly with all due diligence and speed'.

---

[8] Case C-252/21 *Facebook Inc. and Others v Bundeskartellamt* (pending).

[9] See, eg, European Commission, 'Antitrust: Commission opens investigation into possible anticompetitive conduct of Facebook' (4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2848> accessed 30 September 2021.

[10] Compare with the recent ruling in Case T-612/17 *Google LLC, formerly Google Inc. and Alphabet, Inc. v European Commission (Google Shopping)* ECLI:EU:T:2021:763.

In November 2015, the Data Protection Commissioner informed Mr. Schrems that Facebook Ireland has in fact never relied exclusively on Safe Harbour as the legal basis for the data transfers. Months before the first case against the Data Protection Commissioner was filed in 2013, Facebook Ireland had in fact informed the Data Protection Commissioner that Facebook Ireland uses a number of means to legitimise the transfer, including consent and the use of SCCs. However, Mr. Schrems was not informed of this, nor apparently were the High Court or the EU Court. In fact, Mr. Schrems argues in the second case that the legal basis under which Facebook Ireland relies when transferring data remains unclear. Facebook Ireland had informed Mr. Schrems in 2015 that it now relies on SCCs, but also on several other legal means. Thus, Facebook Ireland seems to have changed its mind on which legal bases it relied on and was also hesitant to disclose them to Mr. Schrems.[11]

The discussion about legal bases is significant for various reasons. Firstly, the GDPR is quite explicit that there should always be a legal basis for processing. Of course, there can, be many. The controller, Facebook Ireland in this case, needs to be very clear in its decision on the basis on which in it relies. Secondly, the data subjects (that is, the people whose data is being processed) generally have a right to know the legal basis.

We see that the legal basis for transfers is a crucial issue in the dispute. However, the legal basis for Facebook's operations inside the EU is not. What is the legal basis? Contract or consent are possible options. However, they can both be contested because the GDPR puts specific weight on the control of the informed data subject. It may be unclear to most Facebook users what they are giving their consent to when agreeing to Facebook's terms.

Nevertheless, this dispute is not about the fact that Facebook gathers data, even though it could be about that. It is about the surveillance apparatus of the US. Mr. Schrems' complaint concerns only the fact that Facebook Ireland outsources personal data to the US, although there is no need to do so, when it is subject to electronic surveillance law such as FISA 702.

Note, though, that Mr. Schrems is not unhappy with all transfers to the US. He clarifies in his observations to the CJEU that his complaint does not raise the matter of the data protection level in the US as a whole. The electronic surveillance law (FISA 702) only applies to 'electronic communication service providers'. It does not apply to all other US industries, such as banks, trade, or airlines. Hence, Mr. Schrems argues that there are many situations in which EU data controllers can rely on instruments like the SCCDs to transfer data to the US, when no conflict between EU and US law arises. In addition, his complaint does not concern personal data that Facebook Ireland must send to the USA, such as messages that a European Facebook user sends to a friend over there. The complaint is limited to outsourcing of data processing operations that could just as well be processed within the EU.[12]

Facebook, on the other hand, argued that the US does indeed provide adequate access to judicial remedies:

> The US is a constitutional democracy with a centuries-old history of adherence to the rule of law, robust judicial review, and multi-layered protections to guard against

[11] See written observations of Maximilian Schrems in Case C-311/18 *Schrems II* (lodged on 31 August 2018), 1-2.
[12] ibid 2-3.

> governmental abuses of power. A decision that the US legal system does not ensure sufficient protection would not only affect data transfers to the US, but would likely imperil data transfers to the vast majority of other States, potentially including some benefitting from adequacy findings under Article 25 of the Directive.[13]

The US argued similarly.[14] Understandably, they did not admit that there would be problems with legal safeguards. They saw the US system as comparable to the ones used within the EU.[15] According to the US, the protection of personal data relating to national security data access adopt a holistic approach and afford protections for privacy. After personal data is transferred to a business in the US, any US government national security demand to disclose the data must be based on statutory authority, require adequate justification, and be targeted at a specific person. When data is acquired, it is subject to detailed data-handling procedures. There is a multi-layered system of checks, including independent oversight by the executive branch, the legislature, and the judiciary. The US also referred to the judicial remedies provided for individuals to access information about themselves, as well as possibilities for redress for unlawful intelligence activities by the government.[16]

We see in the observations by Facebook and the US that they argue in strong terms that the US system provides just as much protection for personal data as EU law does. They also point out that the legal system as a whole allows individuals access to various judicial remedies. However, the CJEU was not convinced.

4 RESISTANCE

The *Schrems* cases took a long time. They attest to the fact that legal proceedings are time-consuming, burdensome and of course expensive. The burden is especially large for private individuals and other small actors. The amount of work that Mr. Schrems and his lawyers had to put in is quite remarkable. Even after the first *Schrems* ruling from the CJEU, the Data Protection Commissioner refused to stop the transfers, which was Mr. Schrems' main objective. Instead, it started a quite baffling procedure. In 2016, it decided to file a lawsuit against Facebook Ireland and Mr. Schrems before the High Court, arguing that it has doubts about the validity of the Commissions SCC decisions.[17] With this, the investigation of any other matters raised by the complaint was again paused by the Data Protection Commissioner.

---

[13] Written observations of Facebook Ireland Ltd. in Case C-311/18 *Schrems II* (lodged on 3 September 2018), 4.

[14] The High Court admitted the US as *amicus curiae* in the main proceedings. The aim was to provide the High Court an accurate and up-to-date account of US privacy protections relating to national security access to EU individuals' data after transfer to the US. Also the CJEU gave the US this opportunity.

[15] On this, see also Marc Rotenberg, '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26(1-2) European Law Journal 141.

[16] See written observations of the United States of America in Case C-311/18 *Schrems II* (lodged on 31 August 2018), 5.

[17] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19; Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74; Commission Decision of 5 February 2010 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 Council [2010] OJ L 39/5; (collectively - the 'SCCDs').

The Data Protection Commissioner maintained that any other matter or legal basis that Facebook Ireland may rely on can be dealt with at a later stage. Understandably, this was not what Mr. Schrems had hoped for. After five years without even a first decision by the Data Protection Commissioner, this approach opens the opportunity for never-ending attempts to shift the responsibility to the CJEU by requesting a preliminary ruling for each legal basis contained in Chapter 5 of the GDPR. In effect, Mr. Schrems argued that the DPC ignored its obligation to act on its findings following the investigations into Mr. Schrems' complaint.[18]

Mr. Schrems did not give up, and eventually his side of the story became the one that the CJEU mostly agreed with. Therefore, another theoretical lens through which to analyse the *Schrems* saga is resistance. In political philosophy, it is sometimes seen that law, and legal practices, facilitate little resistance. Instead, law is understood as the instrument to uphold the *status quo* of society and to legitimise possible power imbalances. Above all, this kind of thinking stems from the Marxist traditions of critical legal scholarship.[19]

This case may prove an exception, though. It presents an opportunity to see the emancipatory potential of law. The legal arena can be the scene for political battles. To me, this is one illustrative example of law becoming the space and the means for resistance.

What is so marvellous about this case is the role that Mr. Schrems is allowed to play. He becomes the champion of quite a large battle, in which he is not fighting for his own rights but trying nothing less than to make the world a better digital place. In its own way, the CJEU facilitates this battle.

Mr. Schrems is an activist. A statement by him a year after the *Schrems II* ruling shows that he continues the work because the decision has not had the desired effect:

> Over the last year, it seems that the relevant stakeholders have mainly engaged in deflection and finger pointing, each passing on responsibility to the next. Only a fraction of European businesses have realised that the underlying conflict between EU data protection and US surveillance law will not be solved in the short-term, and have moved towards hosting personal data in Europe, or other safe regions, instead of engaging in an endless compliance nightmare over US law. Other European companies regularly complain about a lack of 'guidance' despite two clear judgments. When guidance is given, such as the recent EDPB guidelines, many argue that it is 'unrealistic' to follow the requirements of the law […].[20]

5 IS DATA LOCALISATION THE INTENDED OUTCOME?

What we are left with after both *Schrems* decisions are insecurities. The SCCs are still one option for data transfers, even though not a viable option for many US companies because the CJEU has now ruled that the US legal system does not include the necessary protection. Nevertheless, the GDPR recognises that there may be situations in which non-EU countries provide an equivalent level of data protection. There are countries, where national law is

[18] See written observations of M Schrems in *Schrems II* (n 11) 3, 35-36.
[19] See on this discussion for example the ways in which Jacques Rancière's thinking has been applied in law. Monica Lopez Lerma, Julen Etxabe (eds), *Rancière and Law* (Oxon: Routledge 2019).
[20] Statement by Max Schrems on the "*Schrems II"* Anniversary' (*NOYB*, 16 July 2019) <https://noyb.eu/en/statement-max-schrems-schrems-ii-anniversary> accessed 18.10.2021.

similar to EU law (for instance Switzerland, Israel, and Canada) and companies can voluntarily commit to EU principles by signing SCCs. US companies, on the other hand, should rely on one of the contractual options in Articles 46 to 48 of the GDPR for outsourcing. However, for companies that fall under US surveillance laws, most options are practically impossible, as US law was not deemed adequate by the CJEU.

In sum, there are not many viable legal options for certain companies to transfer data to the US. This pushes the interpretation of the judgement towards a view where data should be held in Europe and not transferred at all. However, it can be asked whether data localisation can be a solution in today's digitalised world. As Chander puts it,

> First, keeping the information in the EU does not insulate the data from the surveillance of the European Member States' own intelligence services. Second, keeping data in the EU does not insulate it from data sharing by European intelligence services with the USA. Third, if the goal of the GDPR is to assure that the foreign protection is 'essentially equivalent' to that available under EU law, it seems fair to ask whether the Member State surveillance law is markedly more protective, if the shoe were on the other foot.[21]

Fourth, the US intelligence services seem quite able to do their surveillance in Europe even if the data remained here.

So, what is the fight really about? It is probably about power. But it may just be that the surveillance organisations have so much of it anyway that no court case can really change that. To stop data transfers to the US may just be one small detail in a very large picture, one in which data is being processed by surveillance agencies in all countries anyway.

If data localisation is the outcome of the *Schrems* cases, then it does not seem like a practical solution, nor is it perhaps the solution anyone was looking for to combat privacy intrusions by surveillance authorities. It certainly makes life difficult for many companies.

6 DATA TERRITORIALITY – AN OUTDATED NOTION?

In the GDPR context, the logic is that data always reside somewhere. This may be an outdated notion, yet it informs these cases, too. It seems odd in today's digital landscape that data would exist in a place, or that it needs to be physically moved.

Rather, one wonders whether the internet could be understood as a limitless space, where data moves freely in all directions all the time. After all, Facebook Ireland does permit my friends in the US to access my data. My American friends can usually see everything I post, and that way the data are also accessible to the surveillance agencies. Likewise, a hotel in New York will need to collect my data if I make a booking. A book shop in the UK will do the same. If a family member of mine has lived in a third country and then dies, the authorities of both countries will have to exchange various data. The relatives will need some from the third country as well, in order to manage the deceased's estate. Is it a realistic legal solution that all such access across borders constitutes a data transfer subject to the GDPR

[21] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23(3) Journal of International Economic Law 771, 781.

Chapter 5?[22] How all the different legal bases are really supposed to work and which of them is suitable for the various global communications taking place in different situations is all but clear. It may be that the whole notion of data transfers and the set-up for their legal bases is too impractical for real-life use. One reason surely is the territoriality notion. To think that my data on Facebook would exist only inside the EU is simply misleading. It exists everywhere I share it.

Where is the space in which the internet is? And what kind of space is it? In trying to tackle these issues, current legal thinking easily stumbles on its own boundaries. Law, even transnational law, simply does not have the tools to grapple with the non-territoriality of the internet. One is reminded of Foucault's idea of *heterotopia*:

> There are also, probably in every culture, in every civilization, real places – places that do exist and that are formed in the very founding of society – which are something like counter-sites, a kind of effectively enacted utopia in which the real sites, all the other real sites that can be found within the culture, are simultaneously represented, contested, and inverted. Places of this kind are outside of all places, even though it may be possible to indicate their location in reality. Because these places are absolutely different from all the sites that they reflect and speak about, I shall call them, by way of contrast to utopias, heterotopias.[23]

The internet is a site of its own, a place like no other, yet a real place in the sense that it does exist. It is not an imaginary space or a metaphor, rather, it is an existing site where many things happen with real, tangible effects. But it does not exist anywhere and is therefore outside all places. It is absolutely different from the places which it reflects.

Moving data around the internet could be seen as moving it within one place, a place of its own, even though the data simultaneously may move across the borders of traditionally-conceived legal places, states. However, there is a clear discrepancy between the spatiality of the internet and the territoriality of states' jurisdiction, and it brings this case a certain uncanny flavour. The fight is about data being moved but only about certain data being moved in certain specific situations in which it might end up in the wrong hands. At the same time, data moves all the time by other means and other actors into all kinds of hands on both sides of the Atlantic and beyond.

7 PERSONAL DATA IS PURELY INDIVIDUAL – DEFINITELY AN OUTDATED NOTION

Every conversation on Facebook, every comment and every press on the 'like' button includes personal data of at least two people: mine and my friend's, with whom I interact. Communication takes two.

[22] One option for Facebook Ireland and Facebook Inc. would perhaps be to argue that they are one and the same controller (or, perhaps, joint controllers), whose operations revolve around the same data sets (and happen in Europe). There would be no need for data localisation, nor any transfers; the data would just be in the hands of them both from the beginning. This scenario was not discussed in the *Schrems II* judgment.
[23] Michel Foucault, 'Of Other Spaces' (1986) 16(1) Diacritics 1986 22, 24.

The individualist ideology that data protection law builds upon is problematic for many reasons, but this is one of them.[24] It is extremely hard to delineate where my data begins and another person's ends when we are dealing with communication and interaction. Communication is simply not compatible with the notion of separate individuals' personal data staying separate, even though the GDPR often seems to require this.

According to the GDPR, personal data is any data that relates to identified or identifiable individuals. This is the key feature of the Regulation and it defines the scope of data protection law in the Union. Only data that can be linked to an individual is protected.[25] On the other hand, any kind of data that can be linked to an individual is protected. The data does not have to be sensitive nor personal in any way. Also, publicly available data fall within the scope of the Regulation.

The individualist starting point of data protection law is prominent, whereas protection of private life is a much broader – and older – legal concept. The protection of privacy, private life and correspondence, which are found in most European constitutions, can conceptually include protection of groups – such as families – from unwanted intrusion. The more traditional forms of privacy protection were about the home and the private sphere of the household. These do not aim solely at protecting an individual. Much has changed. Today, when the legal focus on privacy protection lies on personal data, the emphasis of privacy rights is very much centred on individuals.

There are continuous problems when data protection rules are applied to something for which they do not really fit. A non-technological example is the *Nowak* case also from the CJEU, which includes difficulties in applying data protection rules to data that constituted the personal data of two people.[26] In this sense, the *Schrems II* judgement takes no steps towards clarification, but leaves us with ambiguities that no-one knows how to solve.

How does the Court, then, decide on the case? By focusing on Mr. Schrems, the individual. It is the protection of him that drives the Court's reasoning. The protection of his rights opens up the case procedurally and also as regards competence. His rights are the aim that override all else. Transfers cannot be allowed. Here the Court seems to argue that it has no leeway because otherwise there would be a loophole in the protection of rights.[27] The teleology of the GDPR dictates the outcome of the case: the individual must be protected.

It may be that the Court's conclusions are the best ones possible, and it may be that they are the only ones to satisfy the wishes of the legislators who drafted the GDPR. Nevertheless, they do leave us with the question of whether data protection legislation is ideal in its current, individualised form. To protect the fundamental right to personal data is naturally the right thing to do, but to construct both the data and the people in strictly individualised ways may prove problematic in future case law.

---

[24] For critique of individualism in privacy protection, see Susanna Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021).

[25] See, eg, Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779.

[26] Case C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994.

[27] See *Schrems II* (n 1), especially para 105. For similar teleological reasoning, see Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388.

8 COMPETENCE AND JURISDICTION

The Court clearly has jurisdiction, as the whole data protection regime rests solidly on the TFEU and the Charter. Hence, there should be no problem with formal legitimacy of the Court's ruling.

Nevertheless, the Court has to deal with questions about competence because some of the parties, especially Facebook, argue that the Court does not have the required amount of it:

> The application of EU law to the transfer of data from the EU to third countries is not disputed by Facebook. However, the implicit assumption underlying the High Court's findings is that the Directive's provisions apply in respect of processing operations relating to State security activities within the EU, notwithstanding (i) the lack of Union competence by virtue of Article 4(2) TEU and (ii) Article 3(2) of the Directive excluding operations concerning State security from the Directive's scope.[28]

The argument is that because national security matters fall outside the reach of EU competence in accordance with Article 4(2) TEU, the EU Court cannot in fact engage in a proper comparison of US regulation and European security regulation. This way, the claim is that the Court does not have the jurisdiction to assess the national security regulation of third countries.

This is an interesting argument, but it does not succeed. The Court reasons in a teleological manner pointing out that it has full competence because without it, data protection in the EU could not be considered in full. Therefore, even though the Court may not have jurisdiction to assess the legality of European national service regimes, it does have jurisdiction to assess the remedies afforded by US law in this area.

For the outcome of the case, it becomes decisive that the Court is not convinced that the US legal system provides enough protection for individuals. In this assessment, the Court also indirectly considers the protection afforded in European security regimes. However, this does not diminish the competence of the Court, according to the Court, because that rests on EU data protection law.

The CJEU considers several statements about the US legal system and its various options for remedies. From a procedural point of view, it is quite interesting that even though this is a preliminary reference ruling, much of the reasoning does indeed concern facts. The CJEU has a lot to say about the actual practicalities of data transfers. It is understandable within the context of the case, but does go against the traditional view of EU law, according to which the CJEU does not rule on facts in preliminary rulings. In addition, many parts of the judgment concern evaluation of another legal system, and they get similar significance as the facts of the dispute. This is one illustration of how other matters than strictly data protection law come to be intertwined in the case.

[28] Written observations of Facebook Ireland Ltd in *Schrems II* (n 13) 3.

9 CONCLUSIONS: AMBIGUITIES

There are two aspects that I would like to highlight by way of concluding this discussion. The ruling caused a lot of debate and has been criticised in many fora. The attention it got is striking, considering that: (a) the ruling only concerns certain data transfers in certain contexts, and (b) the ruling is faithful to data protection rules as they are defined in the law. Hence, it may be that much ado has been caused by some other factors, most likely political ones. It is certainly understandable that a European Court deciding that US law is not good enough could be considered to be rude.

When analysing this decision – any decision – in a critical manner, it is nevertheless prudent to consider alternatives. Could the Court have decided the case in another way? What way could that have been?

I argue that the Court came to the only logical conclusion. The data protection rules are what they are and when applying them in this context, the Court reached a legally sound decision. The legislators' wishes were respected and the fundamental purposes of data protection law, as they are defined in case law today, were upheld. The Court really did not have any choice.

In the end, this is quite a technical data protection case. The commotion it has caused has most likely been about things other than just data protection law. In this paper, I have offered suggestions on what those things could be. The case is about surveillance, platform power, resistance, global politics, data territoriality and the Court's competence, among other things. These are sensitive issues.

The results of the choices that the Court makes cannot be ignored. The consequences are significant. There is still no clarity on data transfers to the US and the diplomatic endeavours to create a mutual framework have not progressed. The Court's ruling has left us with a real-life dilemma that is hard to solve because of political pressure and national self-interests – not an unusual situation in EU law, I suppose. The Court may not be a legislator as such, but its decisions prompt legislative solutions that are needed urgently. At present, we are left with ambiguities.

LIST OF REFERENCES

Chander A, 'Is Data Localization a Solution for Schrems II?' (2020) 23(3) Journal of International Economic Law 771
DOI: https://doi.org/10.1093/jiel/jgaa024

Costello R A, '*Schrems II*: Everything Is Illuminated?' (2020) 5 European Papers 1045

Dhont J X, 'Editorial, *Schrems II*. The EU adequacy regime in existential crisis?' (2019) 26(5) Maastricht Journal of European and Comparative Law 597
DOI: https://doi.org/10.1177/1023263x19873618

Flor A, 'The Impact of *Schrems II*: Next Steps for U.S. Data Privacy Law' (2020-2021) 96 Notre Dame Law Review 2035

Foucault M, 'Of Other Spaces' (1986) 16 Diacritics 22
DOI: https://doi.org/10.2307/464648

Hildén J,'Mitigating the risk of US surveillance for public sector services in the cloud' (2021) 10(3) Internet Policy Review 2
DOI: https://doi.org/10.14763/2021.3.1578

Lindroos-Hovinheimo S, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021)
DOI: https://doi.org/10.1017/9781108781381

Lopez Lerma M and Etxabe J (eds), *Rancière and Law* (Oxon: Routledge 2019)
DOI: https://doi.org/10.4324/9781315666563

Murphy M H, 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) International and Comparative Law Quarterly 1
DOI: https://doi.org/10.1017/s0020589321000348

Rotenberg M, '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26(1-2) European Law Journal 141
DOI: https://doi.org/10.1111/eulj.12370

Zuboff, Shoshana, *The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power* (London: Profile Books 2019).

NATIONAL SECURITY CONCERNS AS AN EXCEPTION TO EU STANDARDS ON DATA PROTECTION

ARACELI TURMO*

Discussions on the appropriate fundamental rights standards in the EU and the need to take into account conflicting interests are increasingly being reframed as debates on the conflict between the primacy of EU law and the constitutional standards of the Member States. One example of this reframing is the French administrative supreme court's decision following the ECJ judgment in La Quadrature du Net. The Conseil ruled that the EU standards set in that judgment must be reviewed, at the national level, with regard to a national understanding of security concerns and the requirements of the fight against terrorism. Thus, constitutional requirements related to public security may be relied upon to argue for a lower standard of protection of personal data than those which the ECJ requires. As this decision shows, the ability of corporations and Governments to rely on litigation before national courts to challenge the standard of protection set at the EU level creates a significant risk, not only for the uniformity of EU law, but also for the protection of the rights of individuals.

1 INTRODUCTION

In his contribution titled 'Lower Instance National Courts and Tribunals in Member States, and Their Judicial Dialogue With the Court of Justice of the European Union',[1] Graham Butler examines the pertinence of greater hierarchical authority from the European Court of Justice over national implementations of EU law. He examines the risks involved in litigants forming strategies to use national courts and judicial systems as an indirect means to avoid, or even fight against, EU standards related to the protection of personal data. This paper highlights the importance of the participation of national courts if the EU is to uphold the standards set out in judgments such as *Schrems I*[2] and *Schrems II*.[3] If national courts can be used as a means for corporations or national governments to avoid EU standards which are seen as too restrictive to trade, innovation or surveillance, the effectiveness of the ECJ's efforts will be greatly diminished.

* Assistant Professor, University of Nantes. This paper partly draws on the analysis presented in a more detailed case note forthcoming in the Common Market Law Review: Araceli Turmo, 'National security as an exception to EU data protection standards: The judgment of the Conseil d'État in French Data Network and others' (2022) CMLRev. 59 (forthcoming).

[1] Graham Butler, 'Lower Instance National Courts and Tribunals in Member States, and Their Judicial Dialogue With the Court of Justice of the European Union' (2021) 4(2) Nordic Journal of European Law 19.

[2] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650.

[3] C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559.

The judgment of the French Conseil d'État, published on 21 April 2021,[4] in the case which jointly gave rise to the *La Quadrature du Net* judgment[5] once again proves the existence of these risks. Although this case had to do with the protection of personal data from state interventions concerning the collection and access to metadata in the EU, rather than on the standards applicable to international transfers of personal data, its treatment by the French administrative supreme court raises concerns related to those presented in G. Butler's contribution. In this case, the French judicial system was successfully used by the Government as a shield from the full reach of EU fundamental rights standards. Moreover, the reasoning followed to justify this decision may prove to be a tempting alternative for national supreme courts and governments which are uneasy with aspects of ECJ case law. This is particularly worrying at a time when the ability of EU institutions to ensure compliance with core tenets of primary law is called into question. The 'cross-pollination' of Eurosceptic lines of reasoning across national courts could become a significant hurdle in the fight to protect the integrity of European Union law, as evidenced by the reference to the BVfG case law[6] in the Polish Trybunal Konstytucyjny's infamous 7 October 2021 ruling.[7] In these judgments, the national court have resorted to ruling the case law of their EU counterpart to be *ultra vires*, a rather blunt but efficient instrument in removing the efficacy of parts of EU law in a given Member State. The French Government had in fact encouraged the French supreme court to go down the same path in reaction to *La Quadrature du Net*, in order to preserve French regulatory provisions allowing the indiscriminate gathering and retention as well as relatively unrestricted access to this metadata by security and intelligence services.

The approach followed by the Conseil d'État is less obviously confrontational, but ultimately more insidious[8] and it could prove to be more efficient in challenging the implementation of EU fundamental rights standards within the Member States. The French court has established a new exception to the primacy of EU law, justified by national security concerns: whenever the French judges are not satisfied that EU standards are compatible with these concerns, as defined by French authorities, they reserve the right not to implement them and thus to set aside the balance established by the ECJ between fundamental rights and the need to fight against crime and ensure security and public order. Like the *ultra vires* accusations, this decision is based on a challenge to the EU's competences. At the core of the Conseil d'État's decision is the idea that the EU is not capable of setting the balance between the protection of personal data and security, because the EU has very limited competences in the fight against crime, and the preservation of public order and security is a policy field that mostly remains in the hands of the Member States. National courts are the

---

[4] CE Ass., 21 April 2021, Req. no. 393099. For a more complete analysis of this judgment, see *inter alia*: Loïc Azoulai and Dominique Ritleng, "'L'État, c'est moi". Le Conseil d'État, la sécurité et la conservation des données' [2021] Revue trimestrielle de droit européen 349, 354.

[5] 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. Significantly, one of the cases was initiated by a preliminary reference on very similar provisions in Belgium, but the Belgian Constitutional Court had had a very different reaction to the ECJ judgment.

[6] Bundesverfassungsgericht, Judgment of the Second Senate of 5 May 2020, 2 BvR 859/15, 2 BvR 1651/15, 2 BvR 2006/15, 2 BvR980/16.

[7] Trybunal Konstytucyjny, Judgment of 7 October 2021, K 3/21.

[8] Shahin Vallée and Gerard Genevoix, 'A Securitarian Solange' (*Verfassungsblog*, 25 April 2021) <https://verfassungsblog.de/a-securitarian-solange/> accessed 11 December 2021.

more appropriate *locus* for the debate (1), and national concerns such as those related to security are acceptable justifications for exceptions to EU law on personal data protection (2).

2 NATIONAL COURTS AS THE LOCI OF CHALLENGES TO THE SCOPE OF EU COMPETENCES ON PERSONAL DATA PROTECTION

Like other national supreme courts and constitutional courts, the Conseil d'État relies on its own understanding of the distribution of competences between the EU and its Member States in order to challenge the European Court of Justice's case law and its legitimacy under the principle of conferral. However, the French court avoids the direct confrontation of an *ultra vires* finding and chooses instead to ignore the ECJ's exercise of EU competences in the area which it deems to be outside their scope. In practice, in the *La Quadrature du Net* judgment and the rest of the case law concerning EU standards for the protection of personal data from national authorities, this means ignoring the balance chosen by the ECJ between privacy and the protection of public security and holding that, by nature, the ECJ was unable to determine the contents of the latter. Instead of complying with a balance established at the European level, according to the Conseil d'État, national authorities must be capable of establishing their own balance between the (fundamental rights) standards set at the EU level and the security concerns defined within the Member State.

The reasoning presented by the Conseil d'État is a reply to the arguments presented by the French Government, which clearly sought to rely on this national court in order to prevent the EU standards from being implemented fully. By asking the judges to hold that the ECJ had ruled *ultra vires*, and encouraging them to determine whether or not they must follow the rules established in EU law, the Government was relying on the Conseil's willingness to challenge the ECJ's own understanding of EU competences in this area. The fact that a Government which otherwise likes to present itself as very pro-European was willing to challenge EU standards on personal data to the extent that it would ask its highest court to set them aside is a very worrying sign. It signals that Member States are far from ready to accept EU standards on data protection which restrict the powers of police and national security forces. It also weakens that the ability of EU institutions to establish common standards for the protection of privacy and even to carry out international negotiations in this area: to what extent is the EU credible in requiring partners such as the United States to adapt to a higher degree of protection of personal data, when it is unable to convince its own Member States that it has struck an appropriate balance with security interests?

The Conseil d'État's choice to avoid direct conflict, in the form of an *ultra vires* decision which could easily have justified infringement proceedings against France, does show an attempt at reaching a compromise position between the Government and the ECJ.[9] However, this debate should not be taking place before national courts, after Governments

[9] Jacques Ziller, 'Le Conseil d'État se refuse d'emboiter le pas au joueur de flûte de Karlsruhe' (*Blog Droit Européen*, 23 April 2021) <https://blogdroiteuropeen.com/2021/04/23/le-conseil-detat-se-refuse-demboiter-le-pas-au-joueur-de-flute-de-karlsruhe-par-jacques-ziller/> accessed 11 December 2021.

have failed to make their case convincingly before the ECJ (or, at any rate, to succeed in convincing the judges that they should strike a different balance between privacy and security). EU standards should be debated and determined at the EU level and, if they are to have tangible effects, must be followed across the Member States. Allowing Governments to renegotiate such standards before national courts, which are institutionally more likely to be sensitive to State-specific concerns and, in the case of the Conseil d'État, inherently closer to the national executive, would be antithetical to the duty of sincere cooperation set out in Article 4(3) TEU. It also poses a major threat to the EU's law-making abilities and its ability to establish fundamental rights standards within the scope of its own competences.

3 NATIONAL SECURITY CONCERNS AS EXCEPTIONS TO EU FUNDAMENTAL RIGHTS

The strategy which focuses on bringing the debate on the appropriate balance between the protection of personal data and security before national courts relies on the belief that Member States' courts will be more receptive to national security concerns than the ECJ. Moreover, the very nature of the legal grounds raised before the Conseil d'État and the judges' reasoning tilts the balance in favour of security concerns. In the framework introduced by the Conseil d'État, the only focus of the additional test carried out by the national court is national security.

The aim of the challenge and the Conseil's response is not really to propose a French perspective on the appropriate balance between privacy and security in EU law. Rather, the Conseil d'État was invited to centre security concerns, as defined by the French Government, on the understanding that the ECJ had given too much weight to fundamental rights. The EU standard is not presented as a legitimate attempt to strike a balance between the conflicting goals at issue, but as excessively focused on personal data protection. All this is justified by a presumption that the EU and, more specifically, the ECJ, is inherently incapable of taking into account the security concerns raised by Governments because it is biased towards fundamental rights protection and does not have sufficient competences in the fields of public order and security in order to develop a clear understanding of that side of the debate. In effect, the approach chosen by the Conseil d'État is based on the idea that the standard set at the EU level is inherently flawed and cannot be unquestioningly accepted by national authorities, which must be able to add a layer of judicial review based on their own understanding of security concerns in order to construct an appropriate balance applicable within each Member State.

By relying on an exception to the implementation and thus to the primacy of EU law, the Conseil d'État affirms the superior legitimacy of national standards regarding public security over the equivalents established at the level of the EU. This is particularly apparent in the justification given for this exception, which draws from the *Arcelor* case law.[10] Under that case law, similarly to what has been established by other supreme and constitutional courts, an exception to the primacy of EU law was permitted where it was necessary to

[10] CE, ass., 8 févr. 2007, *Arcelor*, Req. n°287110. On this judgment, see *inter alia* Paul Cassia, 'Le droit communautaire dans et sous la constitution française' [2007] Revue trimestrielle de droit européen 378; Anne Levade, 'Le Palais-Royal aux prises avec la constitutionnalité des actes de transposition des directives communautaires' [2007] Revue française de droit administratif 564.

ensure the protection of national constitutional standards, ie, where a provision based on EU law is compatible with EU fundamental rights standards but incompatible with more stringent national standards. In this ruling, this exception is reversed, in order to allow provisions of national law which are *incompatible* with EU fundamental rights standards to stand, if they are deemed necessary to protect different national constitutional standards: in this case, ill-defined goals related to security concerns and the fight against organised crime and terrorism. Setting aside the issue of the justification for this ruling from the perspective of French constitutional law,[11] this approach raises serious concerns. It enshrines into French public law the idea that any type of (broadly defined) constitutional norm or objective can justify an exception to EU fundamental rights standards, not only when national authorities believe their understanding of a specific right provides better protection, but also when they choose a lower level of protection than the one which EU institutions are trying to enforce.[12]

The approach chosen by the Conseil d'État relies on the national judges carrying out their own verification of the extent to which EU standards on personal data protection affect the State's ability ensure public security and fight against crime. In practice, this means national courts will, when reviewing national provisions, first apply the EU standard as they understand it, second check whether the results of this review make it excessively difficult to reach the constitutional objective at issue. In this case, the Conseil d'État ruled that only a very limited number of the provisions it was reviewing were incompatible with the standard set by the CJEU. But the broader implications of such two-pronged reviews could be significant as they seek to give national judges significant leeway with regard to EU standards. The attempts to establish a high level of protection of personal data in EU law could easily be thwarted if all national courts give precedence to national security objectives and allow themselves to decide, on a case-by-case basis, whether or not to implement the standards set by the ECJ. The scope of the exception is also unclear: with regard to the justification put forward by the French court, which simply refers to the existence of a conflicting constitutional objective, it seems entirely possible to imagine raising similar exceptions based on different values and principles, such as a national understanding of a different fundamental right, or concepts such as legal certainty or proportionality.

A more recent decision by the French Conseil constitutionnel, on the duty of air carriers to reroute third country nationals who are refused entry into the French territory, illustrates the risks associated with such broad exceptions to primacy being established by national courts. In this case, the Conseil constitutionnel followed its earlier case law indicating that it would abstain from reviewing EU law instruments with regard to national norms, except when they conflict with a principle which is 'inherent to the constitutional identity' of France. It then went on to hold that the prohibition of any delegation of general administrative police powers inherent to the exercise of 'public force' to private entities is such a principle, derived from Article 12 of the 1789 Declaration of the Rights of Man.[13]

---

[11] In particular, the reference to the concept of 'objectives of a constitutional value' and to Article 12 of the Declaration of the Rights of Man of 1789 is not fully convincing: Édouard Dubout, 'Le Conseil d'État, gardien de la sécurité' (2021) chron. 18 Revue des droits et libertés fondamentaux <http://www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/> accessed 11 December 2021.

[12] Anastasia Iliopoulou-Penot, 'La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué' (2021) 24 JCP 659.

[13] CC Decision 15 October 2021, n°2021-940 QPC, *Société Air France,* para. 15.

According to the Conseil constitutionnel's own commentary of this decision, the principle is part of France's constitutional identity because there is no equivalent norm in EU law:[14] the concept does not indicate that the principle is particularly central or historically important in French constitutional law, but simply that it is absent from, or insufficiently protected in, the EU legal order. In this instance, the Conseil ruled that this principle was not violated by the legislative provisions implementing EU law. However, this decision denotes the flexibility of exceptions based on 'constitutional identity' which, combined with the ability of constitutional and supreme courts to establish or elaborate on constitutional principles, could lead to a multiplication of opportunities for the national review of EU law. Under this reading of Article 4(2) TEU and of French public law, any of the multiple principles established in the case law of the Conseil constitutionnel is capable of justifying an exception to primacy if national institutions believe that it is not recognised, or even not sufficiently well protected, under EU law.

Should this type of reasoning become common in national courts, it would allow a variety of political and legal considerations stemming from more or less specific national contexts to impede the appropriate implementation of EU standards for the collection, retention and access to personal data by governments and corporations. The temptation for governmental and corporate actors could become great to rely on such national layers of judicial review to prevent the full implementation of EU law and thus to prevent the ECJ and other EU institutions from constructing and promoting a coherent and ambitious framework for the protection of this data. If these challenges to EU law are successful, they could become a significant cause for variation between the Member States, which would constitute a particularly challenging development at a time when the EU is trying to defend its standards on an international stage.

[14] Conseil constitutionnel, Commentaire de la Décision n°2021-940 QPC du 15 octobre 2021 <https://www.conseil-constitutionnel.fr/decision/2021/2021940QPC.htm.> accessed 11 December 2021.

LIST OF REFERENCES

Azoulai L and Ritleng D, '"L'État, c'est moi". Le Conseil d'État, la sécurité et la conservation des données' [2021] Revue trimestrielle de droit européen 349.

Cassia P, 'Le droit communautaire dans et sous la constitution française' [2007] Revue trimestrielle de droit européen 378.

Dubout É, 'Le Conseil d'État, gardien de la sécurité' (2021) chron. 18 Revue des droits et libertés fondamentaux <http://www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/> accessed 11 December 2021

Iliopoulou-Penot A, 'La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué' (2021) 24 JCP 1152.

Levade A, 'Le Palais-Royal aux prises avec la constitutionnalité des actes de transposition des directives communautaires' [2007] Revue française de droit administratif 56.

Vallée S and Genevoix G, 'A Securitarian Solange' (*Verfassungsblog,* 25 April 2021) <https://verfassungsblog.de/a-securitarian-solange/>accessed 11 December 2021.

Ziller J, 'Le Conseil d'État se refuse d'emboiter le pas au joueur de flûte de Karlsruhe', (*Blog Droit Européen*, 23 April 2021) <https://blogdroiteuropeen.com/2021/04/23/le-conseil-detat-se-refuse-demboiter-le-pas-au-joueur-de-flute-de-karlsruhe-par-jacques-ziller/> accessed 11 December 2021.

BOOK REVIEW

Ester Herlin-Karnell, Gerard Conway and Aravind Ganesh, *European Union Law in Context*, Hart Publishing 2021, 288 pages, ISBN: 9781849467018

Annegret Engel*

Throughout the decades of its existence, the EU has created an abundance of laws in the form of primary and secondary legislation, case law and legal doctrines, the entirety of it also known as EU *acquis*. What is more, the entanglement between constantly changing national and European laws in multi-layered governance presents an additional complexity which is difficult to grasp at first go. A student studying EU law for the first time will thus experience their personal Sisyphean moment at some point during their studies. Leading textbooks in this area, most notably Craig and de Búrca's 'EU Law'[1] covering all constitutional matters and Barnard's 'The Substantive Law of the EU'[2] on the four freedoms of the internal market, provide the dogmatic essentials in extensive format of what a law student ought to know before attempting an exam. For some, this can be a rather challenging endeavour.

This is precisely what 'European Union Law in Context' aims to address. A much lighter fare – both thematically and literally in terms of the number of pages – this book provides a very promising contextual understanding of the societal and political influences which have shaped EU law as it is now. In particular, it includes discussion of the most recent crises the EU had to face, such as the financial crisis 2008, the migration crisis 2015, the COVID-19 crisis 2020, and Brexit. Each one of these has affected various policy areas of EU law and is said to have a lasting impact on EU legislation and case law beyond the mere situation of crisis itself. This contextualisation of different aspects of EU law makes it easier for the reader to connect the dots and enhance a broader understanding of this area, which will be appreciated by students as supplementary reading in addition to their standard textbooks.

The book itself is divided into seven chapters. After an introductory Chapter One on EU Law in Context, Chapter Two discusses the Constitutional Framework of EU Law. By far the most extensive chapter is Chapter Three on Economic Challenges of Integration with sections on the four freedoms of the internal market, competition law, and the economic and monetary Union. Chapter Four then deals with the specific issues of the UK's withdrawal, Brexit. Chapter Five discusses selected themes under the Area of Freedom, Security and Justice. Chapter Six analyses the EU's role as an International Actor, before some conclusions are drawn in the final chapter, Chapter Seven.

---

* Senior Lecturer in EU Law, Lund University.

1 Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (7th edn, OUP 2020).

2 Catherine Barnard, *The Substantive Law of the EU: The Four Freedoms* (6th edn, OUP 2019).

Chapters One and Two nicely set the scene and above all manage to make accessible in such brevity and clarity some of the more complex principles of EU constitutional law, such as the principles of conferral, subsidiarity, and proportionality, as well as issues on enforcement and judicial review, with reference to the current rule of law crisis in Poland and Hungary. For those who have not yet come in contact with EU law before, it will be a great starting point. For anyone who already studied the basics, this will be an easy read to refresh one's memory of the key facts as well as to understand the bigger picture, before getting into the more specific topics on EU law.

Chapter Three covers a range of specific topics which each present their own challenge in the European process of integration. It is unfortunate that these are all covered under the same chapter which not only makes this chapter the longest in the entire book, but also could result in a reader getting lost between the various headings and subheadings. While it is true that all four freedoms of the internal market as well as competition law and other economic policy areas covered in this chapter are all related, a separation into two or potentially three chapters would have perhaps been more beneficial in this case.

Another surprising feature of Chapter Three is that it includes a discussion of the relevant provisions under the EU-UK Trade and Cooperation Agreement (TCA) for each individual topic. Indeed, the withdrawal of the UK has posed enormous challenges on the EU's remaining Member States and the process of European integration. However, the rules regulating the internal market or competition law remain unaffected by Brexit and the negotiated international agreement with a now third country. Considering the fact that the subsequent Chapter Four is dedicated entirely to Brexit, the relevant TCA provisions shaping the new relationship between the EU and the UK would have perhaps been better placed there.

Chapter Four itself provides a lengthy overview of the various stages of the UK's inner political struggles with EU membership and their eventual withdrawal. Undoubtedly, Brexit lends itself as an excellent case study and is relevant to students on both sides of the Channel. In particular, the Miller litigation is relevant for understanding the initial delays in the withdrawal process as well as the subsequently concluded Withdrawal Agreement and the controversies surrounding the Northern Ireland Protocol. However, the great detail of the initial accession process, the UK's position during the different treaty amendments, or the (rejected) models of a future relationship, seem slightly out of place here. A more concise appraisal of the relevant facets of the UK's withdrawal process and its impact on EU law would have perhaps better suited the overall format of the book.

Chapters Five and Six discuss the policy areas under the former intergovernmental pillars pre-Lisbon, which are explained concisely and in a contextual manner with reference to some carefully selected and recent developments in EU criminal law cooperation and foreign policy. These make for some very interesting and highly topical case studies on security matters and artificial intelligence, the establishment of the European Public Prosecutor's Office, data protection (Chapter Five) as well as the extraterritoriality of European values and standards by means of international relations with third countries and the EU's role in international organisations (Chapter Six). Both chapters revert back to the original style found in the earlier Chapters One and Two.

The general impression thus given by the book is that there is a divide between Chapters One, Two, Five, and Six on the one hand and Chapters Three and Four on the

other hand. While the former seem to be written from an EU perspective and aimed at students studying in the EU, the latter's perspective is clearly that of the UK with UK students in mind. It is not evident from the outset; neither the book title nor the aims of the book outlined in the introduction suggest a British perspective or justify the divide. Rather, one would think that the book should have taken an overall European perspective. By no means would this have excluded UK law students reading EU law which is now separate to their own national legal framework.

All in all, the book deserves to be applauded for the very effective contextual approach taken, which is novel to the area of EU law. Regrettably, however, it fails to take a homogeneous perspective across its chapters, thus affecting its overall coherence.

BOOK REVIEW

Mirka Kuisma, *Confronting Legal Realities with the Legal Rule, On Why and How the European Court of Justice Changes Its Mind,* University of Turku 2021, 343 pages

Alezini Loxa*

The work under review is a doctoral dissertation, successfully defended at the University of Turku on 7 May 2021. The doctoral thesis under the title 'Confronting Legal Realities with the Legal Rule, On Why and How the European Court of Justice Changes Its Mind' examines the phenomenon of doctrinal change in the case law of the Court of Justice of the EU (hereinafter the Court).

On its face, the title of Mirka Kuisma's work can provoke different feelings to lawyers, and will perhaps leave many of them wondering how a legal study can answer the question of how and -most importantly- why the Court proceeds in change of doctrine. A quick look through the book is enough for one to realize that Mirka Kuisma is doing a lot more than answering her research question. She is proceeding in a truly comprehensive and novel study of doctrinal change in the case law of the CJEU,[1] and she is providing the readership with a concise overview not only of the phenomenon of doctrinal change, but also of how the Court should structure its future work on the matter.

Kuisma begins the thesis with an introductory Part (Part I) that sets out the theoretical and methodological considerations of her work. Essentially her work is 'loosely' grounded in Scandinavian Legal Realism,[2] MacCormick's second-order justification,[3] and on social constructivism.[4] The work examines two key questions: how and why the Court changes its mind. The first question relates to the factors that affect doctrinal change. The second question focuses on how the Court signals such change in a ruling. In order to answer these questions, the material is examined through doctrinal analysis and qualitative textual analysis. In this first part, Kuisma further acknowledges the limitations of her study, ie, the lack of

* PhD Researcher, Lund University.

[1] The issue of doctrinal change was the subject of examination in Vassilis Christianos, *Reversals of ECJ case law* (Ant. N. Sakkoulas 1998). The theoretical output was of great significance, but the scope was limited in the examination of *Keck* and *Mithouard* and the publication exists in Greek only. The author is not expected to be aware of this, but I note it in order to point out that this matter has been of timeless interest in different EU law academic communities, but very few have attempted to tackle it conclusively.

[2] As she states in her summary Mirka Kuisma, *Confronting Legal Realities with the Legal Rule, On Why and How the European Court of Justice Changes Its Mind* (PhD dissertation, University of Turku 2021). She mentions on this, among others, Alf Ross, *On Law and Justice* (University of California Press 1959) and Ruth Nielsen, 'Legal Realism and EU Law' in Henning Koch and others (eds), *Europe: The New Legal Realism* (Djøf 2010).

[3] Neil MacCormick and Ota Weinbeger, *An Institutional Theory of Law: New Approaches to Legal Positivism* (D Reidel Publishing 2010).

[4] Peter Berger and Thomas Luckmann, *The Social Construction of Reality. A Treatise in the Sociology of Knowledge* (Doubleday 1967).

falsifiability of her claims; the impossibility of ever knowing the full reasons behind change when all the Court produces is a final ruling. Nevertheless, she does proceed in the endeavour and she limits her lenses by focusing 'on the account of the law that the Court gives' as a reason for change.[5]

In Part II, Kuisma explores the issue of judicial discretion and sets her study against the broader framework of the Court's role in the Union legal system. After explaining her choice of treating Court as one collective institutional actor, due to the unitary image cultivated by the Court itself and reflected in the practice of the Court, she goes on to focus on the concept of judicial policy. Judicial policy is a concept, which Kuisma introduces in order to capture the element of choice inherent in judicial interpretation. As she notes, judicial policy is used in order to 'connote judicial constructions about what legal interests the law is seen to promote as well as the best ways of achieving them'.[6] The concept builds on the theoretical premises of her study regarding judicial worldview and MacCormick's second-order justification.[7] More specifically, while MacCormick's second-order justification exists in the context of a particular case, Kuisma's judicial policy is used to refer to the same considerations, but 'as an overarching theme visible in the body of case law on a given issue'.[8] In this Part, Kuisma states her hypothesis that doctrinal change takes places when the Court's perception of what is the best judicial policy changes.[9] She argues that judicial discretion, as linked to judicial policy, is a way for the Court to be in touch with social reality and maintain its legitimacy as a constitutional actor. For this, Kuisma suggests that the legitimacy of the Court's judicial governance should be evaluated by how open the Court is when developing judicial policy.

In Part III, Kuisma discusses doctrinal change on a general level and analyses the elements of the doctrine of change of the Court. Before zooming in the case studies, Kuisma analyses the phenomenon through the examination of different lines of case law in order to extract its more concrete characteristics. In this Part, she also engages with accounts of Members of the Court in order to guide her analysis.[10] Kuisma shows that there is a general – albeit undertheorized - agreement on the ability of the Court to change its mind. However, there appears to be no concrete threshold for when change should happen. Moreover, Kuisma classifies three categories of grounds deemed legitimate for change: technical grounds, system-maintenance grounds, and policy- driven grounds.[11] She further notes that there is a support by Members of the Court for openness, with regard to the communication of change. However, she also notes that there might be other reasons that point to implicit action. Finally, she observes that the way in which the Court proceeds in doctrinal change

[5] Kuisma (n 2) 21.

[6] ibid 35.

[7] On judicial worldview, she bases the study on Aarnio Aulis, *The Rational as Reasonable. A Treatise on Legal Justification* (D Reidel Publishing 1987), who elaborated on legal worldview, and Richard Posner, *How Judges Think* (Harvard University Press 2008) on judge's worldviews as priors.

[8] Kuisma (n 2) 38.

[9] ibid.

[10] She refers to either AG Opinions or extra-judicial writings of the Members of the Court serving at the period when doctrinal change happened and/or who were involved in the cases where doctrinal change happened.

[11] Kuisma (n 2) 87-102. These categories go back to the Opinion of Advocate General Lagrange, Case 28/62 *Da Costa en Schaake NV and others v Administratie der Belastingen* ECLI:EU:C:1963:2.

has repercussions for the application of EU law at national level, which can be expected to affect the Court's grounds for change as well as the methods of communication.

In Part IV, Kuisma abandons the abstract examination and dives deeper in four specific case studies.[12] These are 1) *Keck* and *Mithouard* as a 'paradigmatic' example of a change of doctrine;[13] 2) the *Mangold* saga, where the court openly refused a change of doctrine;[14] 3) the *Dano* quintet, which, according to Kuisma, represents a misread doctrinal change;[15] and 4) the *ERTA* doctrine where she focuses on the failed attempts by different interlocutors to force doctrinal change. This pointillistic, as she states, examination does not have the aim of providing general conclusions, but rather of illustrating what she developed on the previous parts through concrete examples. To do this, Kuisma employs the components of the doctrine of change that she identified in her examination under Part III and she examines how they appear in each case study. In this examination, she looks both at the factors that affected the Court's approach towards doctrinal change, but also on the communicative practices of the Court as to how the change (or rejection of change) was announced in the rulings.

Finally, in Part V, Kuisma proceeds in answering her research questions and she critically evaluates her work. On the why and how the Court changes its mind, Kuisma responds that the Court does so 'if forced thereto by reasons of doctrinal inconsistency or social demand, rarely and opaquely'. Further, she suggests that there is a disconnect between the role and communication of doctrinal change in the Court's praxis. That is in the sense that the ability of the Court to change its mind seems connected to its discursiveness with surrounding social developments. Nevertheless, the Court's communicative practices seem to prevent transparent discussion between the Court and the different stakeholders.[16] That is in the sense that the Court may at times attempt to hide or understate the doctrinal development that is taking place. According to Kuisma, such communicative practices can harm the Court's credibility. For this reason, she concludes with the suggestion that the Court should ensure more openness in doctrinal changes. For Kuisma, this would ensure that the stakeholders are able to hear and to gain the experience of being heard.

Overall, Mirka Kuisma examines a substantial amount of very diverse material, in order to tackle a very tough question, and she proceeds in a truly novel scientific contribution. She is to be commended not only for the novelty and consistency of her work, but also for her ability to navigate through an immense amount of case-law from different areas of EU law with due respect to the specificities of each area and full awareness of the strengths and limitations of her endeavour. This is apparent in Part II, where she reviews different instances of doctrinal change and masterfully induces the general characteristics of the doctrine of

---

[12] The reasons for the choice not to proceed in an exhaustive examination are substantiated in Kuisma (n 2) 23-28.

[13] ibid 27.

[14] Here she focuses on Case C-144/04 *Mangold* ECLI:EU:C:2005:709; Case C-555/07 *Kücükdeveci* ECLI:EU:C:2010:21; Case C-441/14 *Dansk Industri* ECLI:EU:C:2016:278.

[15] Here she includes Case C-333/13 *Dano* ECLI:EU:C:2014:2358; Case C-67/14 *Alimanovic* ECLI:EU:C:2015:597; Case C-299/14 *García-Nieto and others* ECLI:EU:C:2016:114; Case C-233/14 *Commission v Netherlands* ECLI:EU:C:2016:396; Case C-308/14 *Commission v United Kingdom* ECLI:EU:C:2016:436.

[16] By stakeholders Kuisma seems to broadly mean other EU institutions, Member States, national courts and the parties to the proceedings.

change. It is even more so, in Part IV, where she examines in the same detail and with the same diligence all four case studies from different EU fields, and she even goes as far as to suggest readings that are not widely shared by the established scholarship in each field. For example, in the *Dano* case-study, Kuisma challenges the mainstream account of doctrinal change as noted in academic scholarship and suggests that a change in the abstract interpretation of the law took place at an earlier stage in the Court's case-law.

This work further attests a rare pedagogic ability, which Kuisma clearly possesses. In between the sections and the chapters, she is constantly moving between very abstract theoretical ideas and their concrete deep applications in diverse areas of EU law. While doing this, she does not lose the attention of the readership or the coherence of her argumentation for a second. Everything is masterfully tied together for her broader examination and is well communicated to her audience.

Her work, as any, is not without critique. For example, some sections, while informative, did not add much to the main point. Similarly, in her reflection in Part V, there is an overlap between addressing the why and the how questions as regards the communicative discrepancy. This, however, does not take away from the importance of her work or the meticulous way in which she executed it.

Mirka Kuisma's dissertation definitely deserves publication with a major publisher to reach a wider audience, as it is a great contribution to the literature engaging with the CJEU as a constitutional actor. Different authors who have examined specific instances of doctrinal change wryly mention that the Luxembourg Judges must be reading the morning papers. One can never be certain about that or about what are the exact reasons why the Court changes its mind. What is certain is that if the Luxembourg Judges were to read Kuisma's work, they would be impressed by the meticulous nature of her work and they would find – very much needed – suggestions on how to better-perform doctrinal change in the future.