Schrems I and *Schrems II*: Assessing the Case for the Extraterritoriality of EU Fundamental Rights

MARIA TZANOU

I. INTRODUCTION

The issue of the territorial and extraterritorial application of European Union (EU) data privacy rights has attracted significant attention in recent years. Questions of digital sovereignty and extraterritoriality have preoccupied regulators, the Court of Justice of the EU (CJEU) and commentators alike. The EU's centrepiece of data protection legislation, the GDPR,[1] has strengthened the extraterritorial scope of application of EU data protection law. However, the main focus of the EU data protection beyond borders debate has been on the CJEU's jurisprudence. In particular, the Court has generated significant attention in a first line of cases, such as *Google Spain*[2] and *Schrems I*,[3] that established the extraterritorial application of EU privacy rights worldwide. Conversely, more recent decisions, such as *CNIL v Google*,[4] have provoked further discussions as to whether the Court is exercising some kind of self-restraint with regard to the extraterritorial scope of EU data protection rights.

While the CJEU's seemingly confusing approach regarding the territorial application of EU data privacy rights continues to dominate the debate, scant attention has been paid to the *factors* which form the basis of the extraterritoriality of EU data protection rights. This refers to two fundamental problems: one *internal* and one *external*. The *internal* problem concerns the *interpretation* of EU fundamental rights

[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), OJ, L 119/1, 4 May 2016.
[2] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos ('AEPD') and Costeja González*, ECLI:EU:C:2014:317.
[3] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650.
[4] Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:772.

and the *standards* of their extraterritorial *application*. The *external* problem refers to the *examination* of foreign law.

A clear articulation of the *internal* and *external* factors of extraterritoriality is important if the Court wishes to protect fundamental rights online without being accused of engaging in data protection imperialism. The present chapter examines this particular aspect of the extraterritoriality by focusing on the application of EU fundamental privacy rights to trans-border data flows in the *Schrems I* and the recently decided *Schrems II*[5] cases. The chapter raises two criticisms regarding the Court's structuring of the premises of extraterritoriality in *Schrems I*. It argues that the CJEU's analysis failed to meaningfully engage with issues relating both to the *interpretation* of EU fundamental rights in the context of their extraterritorial *application* and to the *examination* of foreign law. More particularly, regarding the *internal* dimension of the problem, I question the invocation of the 'essence of fundamental rights' for the determination of matters of extraterritorial significance undertaken without appropriate theoretical and doctrinal considerations. *Schrems I* is also problematic with regard to the *external* aspect of extraterritoriality, ie the examination of foreign law. The final part of the chapter focuses on the construction of the dimensions of extraterritoriality in *Schrems II*. It concludes that this ruling clarifies both the rules of *applicability* of EU data protection law beyond borders and its *substantive* requirements and, therefore, establishes EU digital rights protection on more solid grounds.

II. *SCHREMS I*: DIMENSIONS OF EXTRATERRITORIALITY

A. Safe Harbour and Transatlantic Data Transfers

The *Schrems I* case arose from Edward Snowden's revelations that the National Security Agency (NSA) had been operating secret surveillance programmes that allowed it to pursue mass surveillance of EU citizens through direct access to the central servers of leading US tech giants, such as Facebook, Skype, Microsoft and Yahoo.[6]

[5] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Judgment of the Court (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559.
[6] Glenn Greenwald and Ewen MacAskill 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June 2013.

Max Schrems, an Austrian lawyer had been a subscriber to the social network Facebook since 2008. He lodged a complaint with the Irish Data Protection Commissioner (DPC) in June 2013, asking it to prohibit Facebook Ireland from transferring his personal data to the US, where it could be subject to NSA surveillance. The Commissioner rejected Schrems' complaint as 'frivolous or vexatious' on the basis that it was unsustainable in law. Mr Schrems challenged the DPC's decision before the Irish High Court, which decided to stay the proceedings and refer the issue to the CJEU following the preliminary reference procedure. The CJEU issued its decision in 2015, concluding that the US authorities were able to access the personal data transferred from EU Member States and process it beyond what was strictly necessary and proportionate to the protection of national security.[7]

Before turning to the decision, it is worth taking a closer look at the legal background of *Schrems I* by placing this in the broader context of the EU's complex regulatory framework for trans-border data flows. Under EU data protection law there are broadly three mechanisms that allow for personal data to be transferred from the EU to a third state. First, transfers can be based on a Commission decision finding that the third state ensures an 'adequate level of protection'.[8] In the absence of such a decision, the transfer can take place when it is accompanied by 'appropriate safeguards'[9] (for example 'Standard Contractual Clauses' (SCCs) or Binding Corporate Rules (BCRs));[10] and in the absence of such safeguards, on the basis of certain derogations for specific situations.[11]

Among the systems adopted worldwide to regulate trans-border data flows, the EU's adequacy requirement has been characterised as 'gunboat diplomacy'[12] that has prompted many countries to change their data protection rules – or indeed introduce new ones – in order to be able to receive data transfers from the EU.[13] The Commission

[7] For a discussion, see Maria Tzanou, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' (2017) 17(3) *Human Rights Law Review* 545.
[8] Article 45 GDPR.
[9] Article 46 GDPR.
[10] Article 47 GDPR.
[11] Article 49 GDPR.
[12] Vagelis Papakonstantinou and Paul de Hert, 'The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic' (2009) 46 *Common Market Law Review* 885, 901.
[13] See Michael Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24(6) *Computer Law & Security Report* 508.

has recognised a number of countries or jurisdictions as providing adequate protection.[14]

There has been no formal adequacy finding regarding the US data privacy regime, but the general approach is that the US lacks adequate protection.[15] This is mainly because the US privacy regime is piecemeal and included in different sources: the US Constitution, the Supreme Court case law, federal legislation, State legislation and the theory of torts.[16] The Constitutional protection of privacy is mainly based on the First Amendment (protection of free speech and freedom of assembly), the Fourth Amendment (protection from unreasonable searches and seizures), and the Fifth Amendment (privilege against self-incrimination).[17] The Fourth Amendment, which protects personal privacy 'against unwarranted intrusion by the State',[18] is limited in its scope by the so-called third-party doctrine that stipulates that the US Constitution does not protect 'what a person knowingly exposes to the public, even in his own home or office'[19] or any 'information in the hands of third parties'.[20] Moreover, the Fourth Amendment does not protect persons overseas, such as EU citizens.[21] At the federal level, there is no omnibus legislation; privacy protection is included in various sector-specific[22] legislative measures that are different for the public and the private sector.[23]

---

[14] The following countries have been recognised to provide adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

[15] See Maria Tzanou, 'The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?' in E Fahey (ed), *Institutionalisation of EU-US Relations: Multi-disciplinary Perspectives on Transatlantic Trade and Data Privacy* (Springer, 2018), 55; Paul Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966; Article 29 Working Party, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, 26 January 1999.

[16] Gregory Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' (2000) 25 *Yale Journal of International Law* 1, 22.

[17] Susan Brenner, 'Constitutional Rights and New Technologies in the United States' in R Leenes, BJ Koops and P De Hert (eds), *Constitutional Rights and new technologies: A comparative Study* (TMC Asser Press, Distributed by Cambridge University Press, 2008) 225, 230.

[18] *Schmerber v California*, 384 US 757 (1966). It should be noted, however, that the Fourth Amendment has not been interpreted to afford a 'comprehensive right to personal data protection'. See Francesca Bignami, 'The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens', Study for the LIBE Committee, PE 519.215, (European Union, Brussels, 2015), p 8, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf; Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017).

[19] *Katz v United States*, 389 US 347 (1967).

[20] Ibid.

[21] *United States v Verdugo-Urquidez*, 494 US 1092 (1990).

[22] Shaffer (n 16 above).

[23] Schwartz (n 15 above), 1974.

Regarding the oversight of the US privacy legislation, 'the closest that the United States comes to a national data protection agency is the Federal Trade Commission (FTC)',[24] which faces significant limits in its enforcement powers.[25]

In order to allow for international trade, transatlantic data flows between the EU and the US were made possible[26] (between 2000 and 2015) through the Safe Harbour scheme.[27] Safe Harbour was based on a system of voluntary self-certification and self-assessment of US-based companies that they abide with certain data protection principles (the 'Safe Harbour principles'), combined with some intervention by the public authorities. In particular, under the scheme, US companies were required to register their compliance with the Safe Harbour principles with the US Department of Commerce, while the FTC was responsible for enforcing the agreement. On the basis of this, the Commission issued the Safe Harbour Decision recognising the adequacy of protection provided by the Safe Harbour principles. Safe Harbour proved to be an important tool of transatlantic commercial relations, with over 3200 companies signing up to the scheme. It has also been argued that Safe Harbour has levelled up US privacy protection standards.[28] Nevertheless, it was found to suffer from major weaknesses in terms of compliance by the self-certified companies and enforcement and oversight by the US authorities,[29] and the Snowden revelations raised additional concerns about the systematic access of US law enforcement authorities to data held by the private companies certified under the scheme.[30]

As mentioned above, the Commission's Safe Harbour adequacy decision was eventually invalidated by the CJEU in its *Schrems I* judgment delivered on 6 October 2015. In that case, the Court took the opportunity to clarify the adequacy criterion. While noting that there was no definition provided in law of the concept of an adequate

[24] Ibid, 1977.
[25] Ibid.
[26] Transatlantic data flows also take place through SCC and BCR.
[27] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ 2000 L 215/7.
[28] Shaffer (n 16 above), 22.
[29] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, Brussels, 27 November 2013, COM(2013) 847 final.
[30] Communication from the Commission to the European Parliament and the Council, 'Rebuilding Trust in EU-US Data Flows', 27 November 2013, COM(2013) 846 final, 13.

level of protection,[31] the CJEU observed that adequacy does not require a level of protection 'identical to that guaranteed in the EU legal order', but nevertheless protection of fundamental rights and freedoms that is 'essentially equivalent' to that of the EU.[32] This requires an assessment of the content of the applicable domestic and international law rules in the third country as well as the practice designed to ensure compliance with those rules. The 'essentially equivalent' criterion shows that the Court is trying to bring external legal systems as close as possible to the EU's internal data protection legal framework[33] in order to ensure that domestic data protection rules are not circumvented by transfers of personal data from the EU to third countries.[34]

This approach is closely linked to the elevation of data protection to the level of a fundamental right that makes the EU's exercise of jurisdiction 'not just … permissive (discretionary), but also *mandatory*'.[35] This necessarily means that trans-border data flows should be regarded as part of the EU institutions' fundamental rights protective duty.[36] Indeed, the Court stated that individuals cannot be deprived of their fundamental rights by the transfer of their data to third countries.[37] A valid argument can be made, therefore, in favour of the extraterritorial application of EU data protection standards.[38] In *Schrems I*, the Court applied EU fundamental rights law to data processing in the US by identifying the problems of the Commission's adequacy decision, rather than directly challenging the US legislation.

B. Establishing the *Internal* Dimension of Extraterritoriality

[31] *Schrems I* (n 3 above), para 70.
[32] Ibid, para 73.
[33] Steve Peers, 'The party's over: EU data protection law after the Schrems Safe Harbour judgment', 7 October 2015, www.eulawanalysis.blogspot.co.uk/2015/10/the-partys-over-eu-data-protection-law.html.
[34] *Schrems I* (n 3 above), para 73.
[35] Cedric Ryngaert and Mistale Taylor, 'Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?' (2019) *AJIL Unbound* 5, 6.
[36] See Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013), 129–33. It should be noted that unlike international human rights treaties such as the European Convention on Human Rights (ECHR), the European Union Charter of Fundamental Rights (EUCFR) does not have a limiting jurisdictional clause.
[37] *Schrems I* (n 3 above), para 58.
[38] Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) *International Data Privacy Law* 235; Mistale Taylor, 'The EU's human right obligations in relation to its data protection laws with extraterritorial effect' (2015) 5(4) *International Data Privacy Law* 246; Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23(5) *Maastricht Journal of European and Comparative Law* 812.

There are a number of problems regarding the CJEU's interpretation of the law that determined the extraterritorial application of EU data privacy rights in *Schrems I*. I focus here on one that is particularly problematic: the Court's discussion of the 'essence' of fundamental rights.

It should be recalled that the CJEU found in *Schrems I* that the essence of both the fundamental rights to privacy in the European Union Charter of Fundamental Rights (Article 7 EUCFR) and to effective judicial protection (Article 47 EUCFR) had been breached. According to the CJEU, the essence of the fundamental right to privacy was breached because the US mass online surveillance programmes grant access on a generalised basis not only to communications metadata but to the actual content of electronic communications.[39] The essence of the right to effective judicial protection was compromised because the US legislation does not provide EU persons with sufficient guarantees and effective legal remedies to exercise their data access, rectification and erasure rights.[40] The CJEU applied, in the *Schrems I* case, Article 52(1) EUCFR which is one of the horizontal provisions of the Charter detailing its interpretation and application and which states: 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must … respect the essence of those rights and freedoms'.

The CJEU analysis in *Schrems I* regarding the essence of the right to privacy raises both theoretical and practical questions. Starting from the theoretical questions, what exactly is the 'essence of fundamental rights', and how is this essence to be determined? Does the concept of the essence signify a maximum or a minimum[41] level of protection?[42] Is the essence of fundamental rights to be considered 'absolute', meaning that it 'can claim validity in all legal systems'[43] or is this a relative concept that can have a different meaning in each particular case? Besides the theoretical

[39] *Schrems I* (n 3 above), para 94.
[40] Ibid, para 95.
[41] Understood as preventing the complete diminishing or negation of a right. See for instance the ECtHR cases *Baka v Hungary*, Application No 20261/12, para 121 and *Christine Goodwin v United Kingdom*, Application No 28957/95, paras 99–101.
[42] See Maja Brkan, 'The concept of essence of fundamental rights in the EU legal order: peeling the onion to its core' (2018) *European Constitutional Law Review* 332; Katharine G. Young, 'The Minimum Core of Economic and Social Rights: A Concept in Search of Content' (2008) 33 *Yale Journal of International Law* 113.
[43] Robert Alexy, 'The Absolute and the Relative Dimensions of Constitutional Rights' (2017) 37(1) *Oxford Journal of Legal Studies* 31. See also Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press, 2004).

problems, there are also practical questions regarding the essence of fundamental rights: Who is to determine this and how? Are the courts the ones to determine the essence of rights? If so, which courts exactly? Specialised human rights courts, like the ECtHR and constitutional courts or every court? How are courts to determine the essence of a fundamental right? Do they do this following their own intuition or is there another way? What happens if the courts get the essence of a fundamental right wrong? How can a legal system (local or global) deal with conflicting judgments regarding the essence of fundamental rights?

These theoretical and practical questions are valid in general; however, they are compelling in the context of trans-border data flows that might entail the extraterritorial application of fundamental rights. Until now, both these sets of questions seemed quite philosophical, but in *Schrems I*, by finding a violation of the essence of two rights, the CJEU made this discussion very real. Admittedly, in *Digital Rights Ireland*[44] the CJEU had already indicated what constitutes the essence of the right to privacy: the access to the content of the data. Nevertheless, *Schrems I* constitutes a landmark, because while in the past the CJEU had indeed spoken in a number of cases about the essence of fundamental rights and more specifically in what I am more interested here – the essence of the rights to privacy and data protection – it had never found an actual breach of these.

Going back to the questions raised earlier, the issue becomes particularly problematic when these are examined in the context of trans-border data flows and the extraterritorial application of fundamental rights.

First, one might wonder why the Court did not follow the path it had taken in its previous *Digital Rights Ireland* judgment that was decided on the basis of a proportionality assessment, but it went straight to find a breach of the essence of the right to privacy, without discussing proportionality at all. Different authors have given different answers to this. Some have argued that the triggering of the essence of fundamental rights at issue really determined the outcome of the case, without there being 'any need to examine the content of the safe harbour principles', 'address any other legal arguments made' or having to balance between privacy and security. This

[44] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Karntner Landesregierung and Others* (C-594/12), ECLI:EU:C:2014:238.

explanation appears tautological: the CJEU is assumed to recognise an infringement of the essence of a right when it sees it and, therefore, a discussion of proportionality is simply not needed.[45] However, I argue that there might be other reasons underpinning the Court's essence of fundamental rights analysis.[46] In my view, these may be related with the extraterritorial application of EU fundamental rights.[47] The Court, indeed, confirmed in *Schrems I* the application of the fundamental rights to privacy and effective judicial protection outside the EU territorial boundaries, but it is possible that it opted to limit this extraterritorial reach to serious circumstances in which the 'essence' of EU fundamental rights was affected.[48]

In this respect, the use of the 'essence' of EU fundamental rights as a *factor* to establish the extraterritoriality of these rights and invalidate a trans-border data transfer that violates these appears somewhat paradoxical: on the one hand, the essence of fundamental rights is the most serious infringement of fundamental rights that can be established (signifying a *maximum* level of protection). On the other hand, this can be seen as an exercise of self-restraint by the Court when it deals with extraterritorial questions: foreign laws would be considered problematic and invalidated only when they impinge on the very essence of EU fundamental rights (signifying a *minimum* level of protection within the context of trans-border data flows).

Secondly, the lack of depth of the CJEU's analysis of the essence of the fundamental to privacy is particularly troubling. The Court did not come up with a clear methodological approach or a comprehensive doctrinal justification why the essence of this right was breached in that case. It just drew a supposed red line – first laid down in *Digital Rights Ireland* – between generalised access to the content of communications and access to metadata, and concluded that the former constitutes the essence of the fundamental right to privacy. This conclusion can be criticised as erroneous, as it clearly disregards the fact that in the context of the Internet and modern digital technologies such a distinction between accessing the *content* of communications and the *metadata*

[45] Martin Scheinin, 'Towards Evidence-based Discussion on Surveillance: A Rejoinder to Richard A. Epstein' (2016) 12(2) *European Constitutional Law Review* 341 at 343.
[46] See Loïc Azoulai and Marijn van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust: *Schrems.* Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*, joined by *Digital Rights Ireland*, judgment of the Court of Justice (Grand Chamber) of 6 October 2015, EU:C:2015:650' (2016) 53 *Common Market Law Review* 1343, 1365; David Cole et al (eds), *Surveillance, Privacy and Trans-Atlantic Relations* (Hart Publishing, 2017).
[47] See also Brkan (n 42 above), 354.
[48] See Kuner (n 36 above), 242–43.

is often artificial and very problematic. It is artificial because in the online, digital world, many Internet metadata, such as a simple Google search or the subject of an email, already reveals the content of the communication as well.[49] It is extremely problematic because metadata using modern data mining and algorithmic techniques can often reveal more precise and sensitive information than the data subjects are aware of themselves.[50]

I submit that the essence of fundamental rights should not be a mere symbolic, abstract idea of human rights protection, but it should be something that can come into play in real cases. That being said, the CJEU should resist the temptation of reformulating simply any fundamental rights issues – admittedly very serious ones – as an infringement of the essence of fundamental rights, even if these issues *do* cause a public outrage. The essence of fundamental rights is necessarily a vague notion and should to an extent remain so. Here, I agree with Robert Alexy about the abstractness of human rights in general. As Alexy has noted, 'human rights refer to abstract subject matter, like liberty and equality, life and property, freedom of speech and protection of personality.'[51] In contrast, the CJEU in *Schrems I* pinpointed in a dangerously accurate manner not just the content, but the very essence of the right to privacy, to the access to content of communications as opposed to metadata. Such an approach is problematic because not only it is based on an artificial distinction but because it also ends up prescribing in definitive – and possible incorrect – terms the essence of privacy, that will probably do more harm than good to digital privacy protection and the claim for informational sovereignty in the Internet context.

C. Establishing the *External* Dimension of Extraterritoriality

The CJEU's construction of extraterritoriality in *Schrems I* is problematic in its *external* dimension as well. This refers to the problem of the examination of the *foreign law*.

[49] See *Digital Rights Ireland* (n 44 above), para 27; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others*, ECLI:EU:C:2016:970; and Opinion of AG Saugmandsgaard Øe in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, delivered on 19 December 2019, ECLI:EU:C:2019:1145, para 257.
[50] See also *Malone v United Kingdom*, Application No 8691/79, 2 August 1984, [1984] ECHR 10, para 84; *Ben Faiza v France*, Application No 31446/12, 8 February 2018, para 66.
[51] Alexy (n 43 above), 34.

Scholars, particularly, on the other side of the Atlantic, have been very critical of the CJEU's assessment of US law in *Schrems I*.[52] In particular, it seems that the finding of a breach of the essence of rights spared the Court from dealing with the issue of how complete information concerning the third country's surveillance can be obtained and used in a judgment. The Court has been accused by mainly American scholars of relying 'on sources that took at face value news articles containing substantial falsehoods regarding US surveillance'; of engaging 'in a series of errors'; and, of being driven 'by EU perceptions that ignore reality'.[53]

These accusations should be taken seriously when considering the extraterritorial impact of the Court's decision. To put it differently, the essence of fundamental rights cannot be used as a quick, easy-fix solution that bars the Court from seriously considering foreign law,[54] just because the case concerns a particularly sensitive issue involving a third country that provoked public outrage. A careful and thorough examination of foreign law is necessary if a valid argument is to be made that EU fundamental rights override this. The temptation of finding that politically sensitive cases trigger the essence of fundamental rights opens up the risk of producing inaccurate or incorrect conclusions that go beyond a particular case: they undermine the very foundations of the claim for digital sovereignty and expose this as a disguised case of data privacy imperialism.

III. *SCHREMS II*: A MORE ROBUST CASE FOR THE EXTRATERRITORIALITY OF EU DATA PRIVACY RIGHTS

A. Privacy Shield

[52] Richard A Epstein, 'The ECJ's Fatal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices' (2016) 12(2) *European Constitional Law Review* 330; Russell A Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press, 2017).
[53] David Bender, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective' (2016) 6(2) *International Data Protection Law* 117, 118.
[54] It should be noted that the CJEU dealt with the validity of the Commission's Safe Harbour adequacy decision, on which it has jurisdiction to rule, rather than directly challenging the US legislation. See Tzanou (n 7 above), 553.

Privacy Shield[55] was adopted in July 2016 to replace Safe Harbour, invalidated by the CJEU in *Schrems I*. It comprised a 'byzantine compilation of documents'[56] that included the European Commission's adequacy decision, the US Department of Commerce Privacy Shield Principles (Annex II) and the US government's official representations and commitments on the enforcement of the arrangement (Annexes I and III to VII).

Similarly to its predecessor, Privacy Shield was based on a system of self-certification by which US organisations committed to a set of privacy principles. However, unlike Safe Harbour that contained only a general exception for the purposes of national security, the Privacy Shield decision included a section on the access and use of personal data transferred under the agreement by US public authorities for national security and law enforcement purposes.[57] In this, the Commission found that

> there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the EU to the US to what is strictly necessary to achieve the legitimate objective in question.[58]

This conclusion was based on the representations and assurances provided by the Office of the Director of National Surveillance (ODNI) (Annex VI), the US Department of Justice (Annex VII) and the US Secretary of State (Annex III), which describe the limitations, oversight and opportunities for judicial redress under the US surveillance programmes.

Serious concerns have been raised as to whether Privacy Shield complies with EU data protection and privacy standards.[59] As I have argued elsewhere,[60] the Commission based its Privacy Shield adequacy analysis merely on a detailed description of US law – found in the US assurances – without any substantive

[55] Commission Implementing Decision of 12.7.2016 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, Brussels, 12 July 2016, C(2016) 4176 final.
[56] Elaine Fahey, 'Introduction: Institutionalisation beyond the Nation State: New Paradigms? Transatlantic Relations: Data Privacy and Trade Law' in E Fahey (ed), *Institutionalisation beyond the Nation State: Transatlantic Relations: Data Privacy and Trade Law* (Springer, 2017) 1.
[57] See Tzanou (n 7 above); Tzanou (n 15 above).
[58] Privacy Shield (n 55 above), recital 88.
[59] See WP29, Opinion 1/2016 of 13 April 2016 on the EU–U.S. Privacy Shield draft adequacy decision WP 238; Resolution of the Parliament of 6 April 2017 on the adequacy of the protection afforded by the EU–US Privacy Shield, P8_TA(2017)0131, para 17; Report of the Parliament of 20 February 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement A8-0044/2017, paragraph 17; European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU–US Privacy Shield, P8_TA(2018)0315, para 22.
[60] Tzanou (n 7 above), 561–63.

commitments (with the exception of the Ombudsperson) being undertaken by the US authorities to comply with EU fundamental rights requirements as laid down by the CJEU in *Schrems I*. Privacy Shield has also been criticised for the lack of oversight of US surveillance programmes, the lack of judicial redress and the shortcomings of the Ombudsperson mechanism.[61]

A. The Judgment

The CJEU confirmed in *Schrems I* a new *procedural* safeguard regarding the extraterritoriality of EU data protection rights: DPAs were granted the power to investigate individuals' complaints alleging a third country's non-compliance with EU fundamental rights – despite the Commission's adequacy decision on the matter – and, if they consider them well-founded, to initiate proceedings before national courts, which must then make a preliminary reference to the CJEU on the validity of the Commission's decision.

Schrems II arises from this new *procedural* DPA power. The factual background of this case is very similar to the 2016 *Schrems I* case. Following the invalidation of Safe Harbour, Max Schrems asked the DPC to suspend the transfer of his personal data held by Facebook Ireland to Facebook, Inc, its parent company established in the USA, on the basis that these could be made available to US authorities, such as the NSA and the Federal Bureau of Investigation (FBI), in the context of surveillance programmes that impede the exercise of the rights guaranteed in Articles 7, 8 and 47 EUCFR. The legal background of the claim this time concerned data transfers in the US under SCCs on the basis of Decision 2010/87.[62] As the DPC took the view that the assessment of Mr Schrems' complaint was conditional on the validity of Decision 2010/87, it initiated proceedings before the Irish High Court and requested that this made a preliminary reference to the CJEU to seek clarification on that point.

---

[61] See, WP29, EU–U.S. Privacy Shield – First Annual Joint Review, 28 November 2017, WP 255; European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2018)0315 (paragraph 22); and EDPB, EU–U.S. Privacy Shield – Second Annual Joint Review, 22 January 2019.

[62] 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 (OJ 2010 L 39/5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344/100, 'Decision 2010/87').

Advocate General Saugmandsgaard Øe delivered a lengthy Opinion in the case in December 2019.[63] The AG focused primarily on the validity of Decision 2010/87. The AG concluded that the SCC decision was valid and invited the CJEU not to deal with the validity of Privacy Shield even though the High Court had submitted several preliminary questions in this regard.[64] Nevertheless, the AG went on to offer some 'alternative observations' relating to the effects and the validity of Privacy Shield, finding that this did not conform with Article 45(1) GDPR, read in the light of Articles 7, 8 and 47 EUCFR and Article 8 ECHR.

In a landmark judgment delivered on 16 July 2020, the CJEU agreed with the AG that the SCC decision remains valid,[65] but annulled the Privacy Shield adequacy decision despite the AG's call for restraint. The invalidation of Privacy Shield raises significant questions regarding the future of transatlantic data flows. Indeed, *Schrems II* has important theoretical and practical ramifications that go well beyond transatlantic relations. The judgment constructs new requirements for legal mechanisms for trans-border data transfers other than adequacy decisions, such as for instance SCCs. While the validity of SCCs was confirmed by the Court in the case, the conditions for their use in third states that require government access to personal data become significantly complicated and raise questions about the role of private companies, such as Facebook, in assessing that the legal regimes of third countries 'do not go beyond what is necessary … to safeguard … national security'[66] and in providing 'additional safeguards'[67] to those offered by the SCCs where necessary;[68] as well as the powers of the DPAs[69] and the EDPB. These issues fall outside the scope of this chapter, which focuses instead on the construction by the Court of the *internal* and *external* dimensions of the extraterritoriality of EU fundamental rights in the context of the examination of Privacy Shield.

[63] Opinion of AG Saugmandsgaard Øe (n 49 above).
[64] Ibid, paras 173, 178 and 180–183.
[65] *Schrems II* (n 5 above), para 149.
[66] Ibid, para 141.
[67] EDPD, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Adopted on 23 July 2020.
[68] *Schrems II* (n 5 above), para 134.
[69] Ibid, para 121.

C. Privacy Shield and the Construction of the Extraterritoriality of EU Data Privacy Rights

The CJEU's assessment of Privacy Shield is more carefully elaborated compared to the assessment of Safe Harbour in *Schrems I*. Overall, the Court's analysis in *Schrems II* pays closer attention to the *internal* and *external* dimensions of extraterritoriality and their respective interlinks. This is demonstrable for a number of reasons.

First, the Court clearly established the standard of protection under which the validity of the Privacy Shield decision should be ascertained: this should comply 'with the requirements stemming from the GDPR read in the light of the Charter'.[70] This pronouncement is significant because it provides legal certainty regarding the legal standard under which the Commission's adequacy decisions (and foreign law) are to be judged. It also clarifies that the GDPR

> applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.[71]

The possibility, therefore, that personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of national security by the authorities of a third country 'cannot remove that transfer from the scope of the GDPR'.[72]

Second, the substantive examination of the *internal* dimension of extraterritoriality steers clear of the analysis on the 'essence' of the rights to privacy and to effective judicial protection and the confusion that arose thereof in *Schrems I*. The Court made clear, however, that US national security requirements cannot be given primacy over data protection principles.[73] *Schrems II* thus aligns with established case law concerning internal cases of surveillance where individuals' data privacy rights are the point of departure to ascertain the constitutional legitimacy of any interference posed by public policy objectives such as national security.[74] This confirms that the

[70] Ibid, para 161.
[71] Ibid, para 89.
[72] Ibid, para 86.
[73] Ibid, para 164. See also *Schrems I* (n 3), para 86.
[74] See Maria Tzanou 'The Future of EU Data Privacy Law: Towards a More Egalitarian Data Privacy' (2020) 7(2) *Journal of International and Comparative Law (Symposium Special Issue)* (forthcoming December 2020).

normative starting point for the examination of external surveillance measures should be the same as that on the basis of which internal surveillance measures are examined.

Third, the examination of the *external* dimension of the extraterritoriality is more carefully crafted in this case than in *Schrems I*. In particular, the Court in *Schrems II* laid down with sufficient clarity the factors that should be considered when assessing *external* limitations to fundamental rights in light of Article 52(1) EUCFR. These factors are (i) such limitations must be provided for by law; (ii) the legal basis which permits the interference with fundamental rights must itself define the scope of the limitation on the exercise of the right concerned;[75] (iii) to satisfy the requirement of proportionality, the legislation in question must lay down 'clear and precise rules governing the scope and application' of the relevant measures and 'imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse';[76] and, (iv) the third country must provide 'effective and enforceable data subject rights' for persons whose personal data is transferred.[77] These requirements construct a four-prong fundamental rights test, applicable to the *merits* of the examination of foreign surveillance programmes, thus providing legal certainty in an area of law that has remained unpredictable since the invalidation of the Safe Harbour principles in *Schrems I*.

Having established a reasonably clear test on the substantive requirements that foreign surveillance measures should satisfy in order to comply with EU fundamental rights, the Court proceeded to apply this in the context of US surveillance programmes. First, the CJEU held that neither section 702 of the Foreign Intelligence Surveillance Act (FISA),[78] nor Executive Order 12333,[79] read in conjunction with Presidential Policy

[75] *Schrems II* (n 5 above), para 175.
[76] Ibid, para 176.
[77] Ibid, para 177.
[78] 50 U.S.C. § 1881. Section 702 FISA allows the targeting of persons reasonably believed to be located outside the United States to acquire 'foreign intelligence information' and provides the basis for the PRISM and UPSTREAM surveillance programmes. Under the PRISM programme, Internet service providers are required to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA). Under the UPSTREAM programme, telecommunications undertakings operating the 'backbone' of the Internet —the network of cables, switches and routers — are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a 'selector'.
[79] E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981). E.O. 12333 allows the NSA to access data 'in transit' to the United States, by accessing

Directive 28 (PPD-28) Signals Intelligence Activities, correlate to 'the minimum safeguards' required to satisfy the principle of proportionality.[80] This is because section 702 FISA 'does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes';[81] and, EO 12333 that allows for access to data in transit does not 'delimit in a sufficiently clear and precise manner the scope of … bulk collection of personal data'.[82] Second, the Court examined data subjects' rights in the US and found that these subjects 'have no right to an effective remedy'[83] because neither PPD-28 nor EO 12333 grant data subjects 'rights actionable in the courts against the US authorities',[84] the Ombudsperson does not have the power to adopt decisions that are binding on intelligence services[85] and the latter's independence can be undermined by the executive.[86]

Overall, the Court's analysis in *Schrems II* is 'unprecedented for the level of detail'[87] with which the CJEU interrogates the US surveillance programmes. This is explained by the fact that, unlike Safe Harbour, a detailed description of US national security and surveillance law was included in the Commission's Privacy Shield adequacy decision. It can, therefore, be argued that the *external* dimension of extraterritoriality, namely the examination of foreign law, was an easier task for the Court with respect to Privacy Shield than with Safe Harbour, as the former explicitly contained the legal bases regarding US authorities' access to personal data. The invalidation of Privacy Shield can be seen, therefore, less as a claim of data imperialism and more as 'punishing' the Commission for its failure to address the problems identified in Safe Harbour and reach a robust adequacy finding.

It has been pointed out that the extraterritorial application of data privacy rights must be based on 'rules that are reasonably clear and predictable, both with regard to

---

underwater cables on the floor of the Atlantic Ocean, and to collect and retain such data before arriving in the United States and being subject there to the FISA.

[80] *Schrems II* (n 5 above), para 184.

[81] Ibid, para 180.

[82] Ibid, para 183.

[83] Ibid, paras 181, 182 and 192.

[84] Ibid, para 192.

[85] Ibid, para 196.

[86] Ibid, para 195.

[87] Kristina Irion, 'Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law', *European Law Blog*, 24 July 2020, www.europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/#more-6410.

the threshold question of *applicability* and with regard to the *merits*' (emphasis added).[88] *Schrems II* achieves both these requirements. It first establishes the *applicability* of EU data protection law to adequacy decisions for trans-border data flows under 'the GDPR read in the light of the Charter'.

Regarding the examination on the *merits* of the extraterritorial application of EU fundamental rights, the CJEU could have proceeded in two ways: One approach would be to apply the analytical framework of Article 52(1) EUCFR, as developed internally, to external cases of interference with privacy and data protection rights (I call this the *inflexible* approach). A second way would be to flesh out an amended test on the *merits* for external surveillance – 'if the differences between the internal and external settings so warrant'[89] (I call this the *flexible* approach). In *Schrems I* the CJEU seemed to have followed the *inflexible* approach: it assessed the interference of US surveillance measures with the EUCFR on the basis of the 'essence' of EU fundamental rights. As seen above, this raised questions as to whether it implied a maximum or a minimum level of protection of rights in the extraterritorial context.

In *Schrems II* the CJEU adopted the *flexible* approach: it constructed a four-pronged test applicable to external interferences by interpreting Article 52(1) EUCFR in this context. The substance of the test illustrates that the Court is willing to recognise potential differences between the internal and the external settings: the test requires that foreign law imposes '*minimum* safeguards', so that the persons whose data has been transferred to third countries have some enforceable rights and sufficient protection 'against the risk of *abuse*' (emphasis added). Swire argues that '[f]or national security experts, it is puzzling in the extreme to think that citizens of one country have a right to review their intelligence files from other countries'.[90] This is not what the CJEU is requiring with its newly-devised merits test. The insistence on minimum guarantees and general requirements to prevent abuse demonstrates that the Court is well aware of the external constraints. It applies fundamental rights requirements more flexibly in the external context, while being cautious at the same time not to deprive them of their

[88] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard International Law Journal* 81, 132.
[89] Ibid, 138.
[90] Peter Swire, '"Schrems II" backs the European legal regime into a corner — How can it get out?', International Association of Privacy Professionals (IAPP), 16 July 2020, www.iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/ .

substance[91] by rendering their application so flexible 'that it ceases to have any impact or compromises the integrity of the whole regime'.[92]

IV. POTENTIAL CRITICISMS

Despite the Court's attempt to be flexible in the extraterritorial context, a crucial question remains: Does the CJEU's new test for external interference with data privacy rights show a 'reasonable degree of pragmatism in order to allow interaction with other parts of the world'?[93] Does it recognise adequately that while 'the protection of personal data … within the European Union meets a particularly high standard' 'the law of the third State of destination may reflect its own scale of values according to which the respective weight of the various interests involved may diverge from that attributed to them in the EU legal order'?[94]

Initial reactions by American commentators show that this is not the case. *Schrems II* is a decision that has not been received with enthusiasm on the other side of the Atlantic. Indeed, an American commentator declared that the ruling is 'gobsmacking in its mix of judicial imperialism and Eurocentric hypocrisy' and noted that 'it is astonishing that a European court would assume it has authority to kill or cripple critical American intelligence programs by raising the threat of massive sanctions on American companies'.[95] But even less angry voices consider that 'the CJEU provides very little room for effective protection against military action' that is premised on 'needed intelligence activities'.[96]

I argue that in order to answer the above questions one needs to take a step back and delve deeper into the claim for extraterritoriality of privacy rights. What is the rationale behind the claim for the extraterritoriality of privacy? Or, to put it more simply, why is the extraterritoriality of privacy rights needed? So far, this claim has been examined within the context where (the GDPR) and the CJEU has placed it in the *Schrems I* and *II* judgments. For the Court, the answer to 'Why extraterritoriality of EU

[91] Opinion of AG (n 49 above), para 249.
[92] Milanovic (n 88 above), 132.
[93] Opinion of AG Saugmandsgaard Øe (n 49 above), para 7.
[94] Ibid, para 249.
[95] Stewart Baker, 'How Can the U.S. Respond to Schrems II?', *Lawfare*, 21 July 2020, www.lawfareblog.com/how-can-us-respond-schrems-ii.
[96] Swire (n 90 above).

privacy rights?' is simple: personal data transferred to third countries should be followed by adequate data privacy protections. Extraterritoriality is therefore essentially linked to the *trans-border/ extraterritorial* personal data *flow* element; since data travels, data protection laws (the GDPR) are applicable as well. This centring of extraterritoriality on *trans-border data flows*, however, disregards another important aspect of the *Schrems* cases that justifies the need for the extraterritoriality of EU privacy rights: *extraterritorial surveillance*. US *extraterritorial surveillance* is designed to target non-US persons and is founded on the basis that US citizenship, residence or the presence of an individual on US soil, are 'criteria of categorical normative relevance with regard to the enjoyment of the right to privacy'.[97] Indeed, US surveillance programmes are 'inherently discriminatory on grounds of nationality'.[98] It is misplaced, therefore, to accuse the CJEU of impeding critical intelligence activities when it requires some minimum safeguards against abuse and enforceable rights for the protection of individuals that are subject to US extraterritorial surveillance without any guarantee of effective privacy protections.

V. CONCLUSION

The CJEU confirmed in *Schrems I* the effects of the extraterritorial application of EU fundamental rights by invalidating Safe Harbour. While this gave a clear message, the decision failed to establish the *conditions* for extraterritoriality, both *internally* and *externally*. *Internally*, the 'essence' of the fundamental right to privacy was used as the benchmark to assess the US surveillance measures, with the unfortunate consequence of confining this concept to a minimum level of protection that entailed incorrect assumptions about the way modern surveillance is undertaken. *Externally*, the infringement of the essence of EU fundamental rights barred any serious discussion of US law – as it was considered redundant – and left the Court open to criticisms from the other side of the Atlantic. As such, the claim for extraterritoriality of EU privacy rights remained weak.

Schrems II presents a more robust *internal* and *external* approach to extraterritoriality that brings legal certainty and clarity both with regard to the question

[97] Milanovic (n 88 above), 89.
[98] Tzanou (n 7 above), 556.

of *applicability* of EU law and with regard to the *merits* of assessing external interference with EU fundamental rights. The CJEU avoided an analysis based on the 'essence' of EU fundamental rights and undertook a more careful examination of US law. It showed willingness to follow a more flexible approach with respect to extraterritoriality by constructing a test of minimum safeguards against abuse that takes into account the specificities of external settings.

It remains to be seen how *Schrems II* fits in with the Commission's ambition to promote 'convergence of data protection standards at international level' and the goal to

> ensure that when companies active in the European market are called on the basis of a legitimate request to share data for law enforcement purposes, they can do so without facing conflicts of law and in full respect of EU fundamental rights.[99]

While conflicts of law seem unavoidable, *Schrems II* takes a first step towards a more reasonable, clear and principled way to addressing these.

[99] Communication From the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', Brussels, 24 June 2020, COM(2020) 264 final, p 13.