Data transfers to the U.S. since the *Schrems II* judgement: An analysis seeking to integrate GAFAM and major providers in the E.U. enforcement strategy

Tilburg Institute for Law, Technology and Society, Tilburg University
LL.M. Law and Technology
Janvier Parewyck
SNR 2065486
June 2021
Supervisor: Prof. Dr. Eleni Kosta
Second Reader: Dr. Irene Kamara

Table of Content

Chapter 1 – Introduction

1.1 Background

On the 16th of July 2020, a well-known pandora's box was once again opened in the data protection sphere, bringing the question of the legality of personal data transfers from the European Union (EU) to the United States (US) to the forefront. In the so-called *Schrems II* ruling,[1] the Court of Justice of the European Union (CJEU) declared the Privacy Shield invalid, instantly depriving of their legal basis a massive number of data transfers to no less than 5378 American companies, including Google LLC, Facebook INC and Amazon.com INC to name a few.[2] The Privacy Shield, adopted by the European Commission (the Commission), formerly declared that the level of data protection in the US was sufficient to automatically allow companies to transfer personal data to self-certified US companies.[3] It was not the first time that transferring personal data to the US was challenged: In 2015, the *Schrems I* judgement[4] already invalidated the ancestor of the Privacy Shield, i.e. the Safe Harbor, hinting that keeping such transfers going in a legal way might not be as easy as hoped due to deep-rooted issues with US surveillance laws and practices.

Nowadays, not only does the Internet itself, by its very nature, imply that electronic data flows from one continent to another, but companies rely on offshore IT services and Cloud infrastructures around the world, including in the US, to operate their businesses,[5] resulting in ever-increasing transfers of personal data in the meaning of the General Data Protection Regulation (GDPR).[6] It is therefore not surprising that European companies, and more broadly companies subject to the GDPR, have been and are still looking for ways to maintain data transfers to the US rather than shutting them down immediately. The *Schrems II* ruling indeed did not entirely prohibit transfers as it did not invalidate the other legal bases and safeguards on which it can be relied upon – in particular the Standard Contractual Clauses (SCCs). However, it has introduced stringent additional requirements for data exporters, which have been further developed through several guidelines of the European Data Protection Board (EDPB).

Stated simply, the problem at stake goes beyond the considerations related to data transfers as such and lies in the different vision of privacy in the US and the EU or, more precisely, between the levels of protection granted. In the EU, data protection is a fundamental

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

[2] Number of participating enterprises listed on the snapshot of 16 July 2020 of the official Privacy Shield official website; 'Privacy Shield List' (*Internet Archive*) <https://web.archive.org/web/20200716063154/https://www.privacyshield.gov/list>

[3] 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 (notified under document C(2016) 4176) [2016] OJ L 207

[4] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

[5] Netskope INC, 'EMEA Cloud Report' (September 2016) <https://resources.netskope.com/h/i/285920664-september-2016-emea-cloud-report>; See also Christopher J Millard, *Cloud Computing Law* (Oxford University Press 2014) 3ff

[6] 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) [2016] OJ L119/1

right under the Charter of Fundamental Rights of the European Union (the Charter).[7] The GDPR, and its ancestor the Data Protection Directive (DPD),[8] were conceived under the prism of a geographical approach to data flows[9], which implies that for data to be transferred to a third country, it must first be ensured that the degree of protection to which the data subject will be exposed is 'not undermined'.[10] It is worth noting that EU law has concurrently an organisational approach resulting in an extraterritorial application,[11] as companies outside EU jurisdiction can be subject to the GDPR under certain circumstances[12].

In the US, providers of IT services operating under the US jurisdiction can be compelled pursuant to the Stored Communications Act (SCA) to disclose user data to Law Enforcement Authorities (LEA).[13] While such possibility is also conceivable in the EU Member States, the Clarifying Lawful Oversea Use of Data Act (CLOUD Act) went further by amending the SCA in 2018 and extending the US providers' disclosure obligation to all information in their 'possession, custody or control'.[14] This enacted the extraterritorial application of the US law (after first having been challenged in Court[15]), meaning that LEAs can even require US providers to disclose data stored by their subsidiaries in third countries[16]. Moreover, the PATRIOT Act enables disclosure injunctions to be combined with a 'gag order' forcing the company to conceal the LEA's data acquisition request.[17] This ability is furthermore coupled with several bulk interception and mass surveillance programs (including, but not limited to, the PRISM system providing the NSA with direct access to the servers of the largest US providers), whose magnitude was first revealed in 2013 by former CIA agent Edward Snowden.[18] Those programmes are based on numerous laws and legal precedents, including the Foreign Intelligence Surveillance Act (FISA), the Executive Order 12.333 (E.O. 12.333) and the aforementioned PATRIOT Act.[19]

---

[7] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 Article 8, in addition to Article 7 enshrining the right to Privacy

[8] 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 [1995] OJ L 281

[9] Christopher Kuner, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' (1 October 2010) TILT Law & Technology Working Paper No. 016/2010, Tilburg Law School Research Paper No. 016/2010, 39-41 <https://ssrn.com/abstract=1689483>

[10] Article 44 GDPR

[11] Kuner (n 9)

[12] Article 3(1) GDPR (where an entity of the US company is established in the EU) and Article 3(2) (where there is no linked establishment, but the US company engage in specific activities); The GDPR can also indirectly applies through contractual arrangements (see e.g. Article 28(3) GDPR); See Chapter 4 of this paper

[13] Stored Communications Act, Pub.L. 99-508, 100 Stat. 1848 (21 October 1986)

[14] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub.L. 115-141, 132 Stat. 348 (23 March 2018)

[15] See United States v. Microsoft Corp., 584 U.S. (2018)

[16] Tess Blair and Tara S. Lawler, 'Possession, Custody or Control: A Perennial Question Gets More Complicated' *The Legal Intelligencer* (Philadelphia, 5 February 2018) <https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/05/possession-custody-or-control-a-perennial-question-gets-more-complicated/> accessed 06 January 2021

[17] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT ACT), Pub.L. No. 107-56, 115 Stat. 272 (24 October 2001)

[18] See Ewen MacAskill and Gabriel Dance, 'NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained' (*The Guardian*, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded> accessed 5 January 2021

[19] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§1801–85 (2012); Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200; PATRIOT ACT (n 17); A comprehensive corpus of US Intelligence Law was published by the US Office Of The Director Of National Intelligence and is available at <https://heinonline.org/HOL/P?h=hein.usfed/incolrb0005&i=1>

As will be developed, the CJEU considered that US law offered insufficient guarantees regarding the right of EU citizens to the protection of personal data enshrined in the Charter. It was, *inter alia*, lacking effective remedies for data subjects even under the specific arrangements of both the Safe Harbor and the Privacy Shield, leading to their invalidation in the two *Schrems* judgements. More fundamentally, the US Constitution and its Fourth Amendment recognise a right to privacy only for US citizens, thereby excluding – in some instances – any redress for unlawful or unfair processing to European citizens.[20]

As long as these profound systemic incompatibilities are not overcome, the transfer of personal data between the EU and the US will not be hampered. This does not mean that data transfers can never be conducted, as they can be based on other transfer tools and backed up with technical safeguards which constitute a sort of last joker for companies that cannot avoid transfers and have the means to bring them into compliance. However, as will be seen, the viability and foreseeability of such tools and measures remain limited and subject to caution, as the *Schrems II* ruling is putting great pressure and responsibilities on the actors who rely on them. These actors are compelled to engage in a thorough review of US law and/or implement complex technical solutions. The EDPB released subsequent Recommendations on additional measures[21] and essential guarantees[22] that will be examined in this thesis. The Commission also quickly announced that it was working with the US Department of Commerce to provide new solutions in the future[23] and released new SCCs,[24] whose added value will also be analysed to give a comprehensive overview of the situation.[25] While the first key question that will be raised is how a (European) company can continue to operate data transfer in a legal way, a second fundamental issue is how such a system can be enforced and not just remain wishful thinking.

Although the GDPR has been criticised multiple times for being 'too formalistic' and disconnected from reality,[26] the recent *Schrems II* judgement, along with the increased power of the Data Protection Authorities (DPAs) and the higher fines put in place since the GDPR[27] (compared to the former DPD at the time of the *Schrems I* judgement), might potentially be a turning point for data protection in practice.[28] Whatever the conceptual or practical weaknesses and limits of the GDPR as it is today, it is claimed in this thesis that it would be possible to achieve a higher level of effectiveness. And, perhaps surprisingly, in a way that would generate less penalizing spill-over effects for companies subject to the GDPR than those currently suffered because of the current disorganized and insecure vacuum. Indeed, there are different

---

[20] U. S. Const. Article IV; Since 2008, the FISA "allows for the collection of communications without a warrant, where at least one end of the communications is a non-US person"; Ewen MacAskill and Gabriel Dance (n 18); It is also striking to note that the Executive Order 12.333 goes so far as to state: 'The Director of the Central Intelligence Agency shall: (1) Collect (*including through clandestine means*), analyze, produce, and disseminate foreign intelligence and counterintelligence' (emphasis added)

[21] EDPB draft Rec. 01/2020 (n 181) and EDPB Rec. 01/2020 Version 2.0 (n 184)

[22] EDPB Rec. 02/2020 (n 201)

[23] Commission, 'Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross' (10 August 2020) <https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836>

[24] New SCCs (n 183); See also Draft SCCs (n 182)

[25] Chapter 3 of this paper

[26] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal 881 <https://ssrn.com/abstract=2732346>; See also, for a sharp criticism: W Kuan Hon, *Data Localization Laws and Policy* (Edward Elgar Publishing 2017) <https://doi.org/10.4337/9781786431974>

[27] Article 83(3), (4) and (5) GDPR

[28] Paul Lambert, *Understanding the New European Data Protection Rules* (ProQuest Ebook Central 2017) <https://ebookcentral.proquest.com> ch 26, 251ff

actors that can be targeted by, and different ways at the disposal of, European institutions, DPAs and the Member States to realistically enforce the data transfers scheme and individual's rights.

In particular, an extremely significant part of the global internet traffic involves GAFAM companies (Google, Apple, Facebook, Amazon, and Microsoft, all US-based companies)[29]. In addition to the services offered directly to consumers (B2C), these companies offer services to businesses (B2B) and often intervene in one way or another in the chain of activity of European companies. In other words, the infrastructures and even operations of many businesses are in fact largely entrusted to these GAFAM as well as other huge American companies[30]. More than intermediaries, they are the main and strongest actors of today's web. Consequently, European companies cannot move out of those '*superproviders*'[31] overnight. This thesis supports that it would be hypocritical and unrealistic to argue otherwise and to pursue enforcement solely on companies that are more dependent on these superproviders than they are able to supervise them through contractual arrangements.[32] The common myth that superproviders are processors acting 'on behalf' and 'under the instructions' and authority of the controller[33] could mislead to the view that they are second-tier players. This thesis contends that they are not, and points out that the fact that superproviders are based in the US does not, in theory, prevent enforcement towards them for two reasons: First, the scope of applicability of the GDPR extends to companies outside the EU, and secondly, those companies usually have entities within the EU jurisdiction[34]. Case law has interpreted the applicability of these leverages broadly and flexibly[35].

Whilst it seems unrealistic in practice today to get US companies to refuse legally binding injunctions from US LEAs for the sake of GDPR compliance – leaving a sense of deadlock –, it might be possible for them to act upstream. Do they really need to send data to the US and/or require their business customers to undertake data transfers in the first place? There is room for European regulators to gradually push and compel them to act in such a way that the data are not directly stored or easily accessible from the US and finally try to escape the scope of the 'possession, custody or control' notion. In fact, superproviders might have enough resources to do so as their data are often already cached and replicated all around the globe. The possible regulatory means to achieve that goal will be explored in this thesis, distinguishing between US and EU entities of a same superprovider and considering the various roles each entity can play under the GDPR.

---

[29] According to a 2019 Sandvine report, GAFAM and Netflix combined account for 43% of the total internet traffic. This metric does not represent the amount of personal data processed but rather the amount of personal and non-personal data flowing from and to them, but it does provide an insight into the prominence of these actors; Sandvine, 'The Global Internet Phenomena Report' (September 2019) 17 <https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf>

[30] Netskope INC (n 5); See for the breakdown between these actors: RapidValue, 'Amazon Web Services – Ruling the Cloud' <https://www.rapidvaluesolutions.com/infographics/amazon-web-services-ruling-the-cloud/>

[31] They will be referred to as such for the clarity of the discussion

[32] Privacy professionals' consensus is probably reflected in this Brian Hengesbaugh's article: 'At the end of the day, no one realistically expects that EU DPAs will immediately launch investigations against thousands of companies that have built and deployed strong privacy programs in reliance on Privacy Shield.'; Brian Hengesbaugh, 'What Privacy Shield Organizations Should Do In The Wake Of 'Schrems II' (*IAPP*, 17 July 2021) <https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/> accessed 7 January 2021

[33] Article 4(8), 28 and 29 GDPR

[34] See (n 12)

[35] As will be examined in Chapter 4 of this paper

Ultimately, a minimal alignment of US legislation with European law must be obtained. A few key changes would have to be made on the US side to achieve a smooth and lawful flow of data, which otherwise seems destined to become increasingly bogged down.

1.2 Problem Statement

Over the years, the EU has taken a clear stance on data protection, making European legislations a world leader in this area.[36] The *Schrems II* judgement is in line with those developments. However, such a level of protection must, as any other law, be observed in order to be relevant. Today, while the exact scope and implications of the judgement are being hotly debated, it is clear that to ensure compliance, companies must engage in extremely thorough assessments that appear to be difficult to carry out. This issue directly relates to the question of how to enforce the ruling in an effective and realistic way.

The objective of this thesis is to capture the insights of the *Schrems* judgements, analyse the transfer tools available today to all companies subject to the GDPR and highlight their limits, and explore certain avenues directed towards the few largest US superproviders in order to pursue the efficiency of the data transfer regime and therefore the level of protection of personal data. Hence, this thesis will answer the following main question:

> *In the post-Schrems II era, how can the EU enforce the level of protection of personal data provided by the Charter when it comes to data transfers to US-based providers subject to US FISA legislation?*

To answer this question, the following sub-questions will be answered:

1. *How did EU law allow transfers to the US before the Schrems II judgement and why the Privacy Shield was invalidated?*
2. *Since the Schrems II judgement, how can personal data be transferred to US-based companies subject to US laws?*
3. *How to enforce GDPR data transfers requirements towards major US superproviders despite the apparent weaknesses inherent to the current implementation of the GDPR?*

1.3 Methodology and limitations

This thesis will rely on a doctrinal legal research approach. The material that will form the backbone of the study will consist of primary sources – mainly the EU Charter, the GDPR, EU case law, the Commission implementing acts and the EDPB/DPAs guidelines – as well as, insofar necessary to comprehend the conflicts with European law, US laws and case law. To further analyse those statutory legislations and weave the relationships between them, academic literature on data protection will be considered. As the *Schrems II* judgement is fairly recent, the literature will include recent relevant developments – occasionally closer to data protection professionals than to legal scholar *per se* – for which it should be borne in mind that they may sometimes potentially lack certain hindsight, despite our best selection efforts. Furthermore, the practical constraints require us to delimit this thesis to the situation and resources existing at the date of 27 June 2021.

[36] Lambert refers to a 'draconian' regime; Lambert (n 28)

After having adopted a neutral and factual perspective to examine European and US positive law up to the outcome of the *Schrems II* judgement which highlighted the risks for data subjects, the thesis will adopt a data exporter perspective by analysing the remaining transfer tools enabling data transfer to the US. Such analysis will necessarily involve official regulatory guidelines and, to a limited extent, technical considerations, so that it will engage in an interdisciplinary approach. Later on, a regulatory perspective (i.e. from EU and Member States regulatory bodies) will be adopted to propose a strategic direction for future enforcement actions, involving a detailed examination of the ability, under the law in its current form, to target US superproviders and hold them accountable.

It is acknowledged that not all possible enforcement solutions will be developed in this thesis. Achieving true data transfer compliance from companies will not be a smooth ride; it will be a long road involving different steps. Rather than looking at the – currently quite unlikely – long-term solutions in this area (e.g. an agreement with the US or a complete re-localisation of the entire digital business to Europe), this thesis will focus on the possibility of taking concrete and immediate actions to pave the way for a progressive strategy after the *Schrems II* judgement. As the core of the problem is intrinsically linked to the dependence of European individuals and European companies on US superproviders, the current and potential role of major US superproviders in data transfers will be examined in the B2C and B2B contexts, and certain avenues enabling enforcement against them will be elaborated, keeping in mind a longer-term enforcement orientation. This thesis will not provide specific recommendations for particular real-world cases, nor will it suggest legislative changes in the EU. Moreover, this thesis will be confined to transfers for commercial purposes, for which Cloud solutions are mostly used,[37] rather than transfers in the law enforcement context which were not formerly covered by the Privacy Shield.[38]

1.4 Narrative structure

After this introductory chapter, the second chapter will set out the legal context and basic concepts as well as the chronological twists and turns relevant to understanding the friction with US laws that led to the invalidation of the Safe Harbor and then the Privacy Shield, and will unveil the outcome of the *Schrems II* judgement (Chapter 2). Afterwards, remaining ways to transfer data to the US, combining both GDPR transfer tools and additional technical safeguards, will be assessed. A conclusion will be drawn as to the effectiveness of these tools and the concrete situation of data controllers since *Schrems II* (Chapter 3). To provide an enforcement strategy, the last chapter will identify different enforcement techniques from traditional direct enforcement by DPAs to new certifications (such as the New European Data Protection Seal) and other governance mechanisms. A map of the different actors involved will then be drawn and the legal roles that US superprovider's entities can take under the GDPR dichotomy will be examined. In order to put US superproviders at the forefront of the transition for lawful data transfers, an extensive legal analysis of the applicability of the GDPR and the relevant rules will be carried out – including a proposal for the requalification of US superproviders –, followed by an overview of the current impediments to enforcement in practice. An outlook on the potential outcome will then be contemplated (Chapter 4). The Conclusion will finally summarise the findings and outline an optimistic way forward.

[37] Netskope INC (n 5); Hon (n 26) 5ff

[38] European Union Agency for Fundamental Rights (FRA), *Handbook on European data protection law* (2nd edn Publications Office of the European Union 2018) 257

Chapter 2 – Lawfulness of data transfers in EU law up to the *Schrems II* judgement and the invalidation of the Privacy Shield

"We are not fit to lead an army on the march unless we are familiar with the face of the country — its mountains and forests, its pitfall sand precipices, its marshes and swamps."

Sun Tzu [39]

2.1 Introduction

The regime for international data transfers has evolved (and been discussed)[40] since the genesis, in 1980, of the Guidelines of the Organisation for Economic Co-operation and Development.[41] These were followed by Convention 108,[42] the DPD and finally the GDPR.

[39] Protection of privacy is a matter of struggle between various and complex interests, in particular between Europe and other continents, including the United States; between regulators and very powerful multinationals; between the necessary repression of crime on the one hand and the protection of privacy and free will on the other; between flesh-and-blood data subjects and fictional legal personalities; between the law as it is written and judged, and the law as it is actually applied. It is to illustrate these tensions, these power relations, that it was chosen to illustrate each of the three main chapters of this paper with a quotation from Zun Tsu, the ancestral author of the Chinese classical text "The Art of War" which is today considered as a source of reference and inspiration in our contemporary societies and their new forms of confrontation. Jean Lévy explains, in the preface to his French translation:
"[The Art of War] is naturally the object of all sorts of distortions, since it is asked to solve all the questions raised by the madness of men. The prestige of *Sun-tzu* [...] is due first of all to its exoticism, but also to the vagueness of its formulas which find all sorts of fields of application. Moreover, it fits perfectly into the warlike and combative phraseology of our time, where war, while withdrawing from our daily life as a lived reality, invades under phantasmatic or real forms civil domains from which it was in principle excluded: the social, commercial and economic relations are thought only in terms of total war, of struggle to excess and extermination. The ideology conveyed by the dominant economic discourse is shaped by a warlike terminology. The word strategy has become the watchword of economists and business leaders for whom the reading of Master Sun's *Art of War* is an indispensable step in their training. […] The manuals on the art of Chinese warfare, after having been the prerogative of the military for a long time, have thus become the thing of industrialists and business leaders. They are periodically updated, and, due to public expectations, the share of illustrations borrowed from the struggles between large firms and from commercial competition, becomes preponderant.
Thus, Sun Tzu's theories are in fashion. There is nothing better than a mysterious and distant object to adorn it with all the features that one feels lacking in oneself. China is a mirror because it is an elsewhere. The success of the revolutionary armies in the Far East (China, Korea, Vietnam), then the commercial success of the "Asian dragons" contributed to adorn with the prestiges of the real what was already endowed with the virtue of dream." (translated from French). Although these quotations can hopefully lull the reflection, one should not lose sight of the fact that such contemporary interpretations of this several thousand years old work will remain, as Jean Lévy writes, "anachronistic and utilitarian"; Zi Sun and Jean Levi, *L'art de la guerre* (2015);
J Dyer Ball, 'Sun Tzŭ on the Art of War. Translated from the Chinese, with Introduction and Critical Notes, by Lionel Giles M.A., London: Luzac & Co.' (1910) 42 Journal of the Royal Asiatic Society 961

[40] See for instance Peter Swire and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press 1998)

[41] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980

[42] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS No. 108

After a brief overview of the main rationales behind the GDPR (section 2.2) and an outline of the data transfer notion as well as the legal basis for international data transfers in the context of Chapter V of the GDPR (section 2.3), this chapter will present a commented evolution of the conclusions of the *Schrems I* (section 2.4) and *Schrems II* (section 2.5) judgements with a focus on their concrete findings. A brief conclusion will then be drawn on the state of affairs left in the aftermath of the *Schrems II* judgment (Section 2.6).

2.2 The GDPR regime and the 'accountability' principle

The protection of personal data was formerly governed mainly by the DPD and is now regulated with direct effect by the GDPR.[43] The scheme aims to protect data subjects' rights by requiring the processing of personal data to be based on one of the six legal grounds[44] and by imposing obligations on data controllers and processors[45]. The data controller is the entity determining 'the purposes and means of the processing of personal data',[46] while the processor is only acting 'on behalf of the controller'[47], under its authority and in accordance with a contract.[48] The boundaries between these two concepts, as well as the scope of application of the GDPR, will be analysed later in more detail in Chapter 4.

One of the core principles of the current regime is the 'accountability' of data controllers.[49] The entity collecting and/or processing personal data, and therefore qualifying for the legal status of controller, 'shall be responsible for, and be able to demonstrate compliance with,' the GDPR[50] at any time, in particular in the event of requests from DPAs[51]. Under the GDPR (in comparison with the DPD), processors are also faced with their own obligations and duties, and are therefore considered to be equally subject to the accountability principle.[52] This has been illustrated in practice by two decisions in 2021 from the French and Italian DPAs.[53]

It follows that both controllers and processors that transfer personal data to third countries or international organisations (hereinafter data exporters) must be able to demonstrate compliance with the relevant data transfers provisions of the GDPR described below.[54] This is not the case, however, when data do not leave the EU/EEA area as, pursuant to the principle of

[43] Needless to say, the protection of personal data was and is also protected by a plethora of other instruments – such as the "ePrivacy" Directive 2002/58/EC, the Directive 2016/680 with regards to data protection in law enforcement, and the Regulation 2018/1725 (formerly 45/2001) targeting EU institutions and bodies – which will not be scrutinised in this thesis

[44] Article 5(a) and 6 GDPR

[45] Although Chapter IV of the GDPR is specifically entitled "Controller and Processors", their obligations are set out in the entire GDPR

[46] Article 4(7) GDPR

[47] Article 4(8) GDPR

[48] Article 28 and 29 GDPR

[49] Article 5(2) GDPR

[50] Ibid and Article 24 GDPR

[51] Article 558(1)(a) as well as Article 31 GDPR

[52] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation – A practical guide* (2017) 80

[53] Italian DPA (Garente per la Protezione dei Dati Personali), 'Ordinanza di ingiunzione nei confronti di Roma Servizi per La Mobilita S.r.l. [9562831]' (11 February 2021) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9562831> (in Italian); French DPA decision unpublished, see French DPA (Commission Nationale de l'Informatique et des Libertés, CNIL), '« Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant' (27 January 2021) <https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant> (in French)

[54] As confirmed in EDPB Rec. 01/2020 Version 2.0 (n 184), in particular [6]

free movement of personal data within the EU, data can move freely to and from Member States and EEA countries without restrictions.[55]

2.3 The notion of data transfer and the scheme of Chapter V GDPR

The GDPR recognises that 'flows of personal data to and from countries outside the Union […] are necessary for the expansion of international trade and […] cooperation' but, since entities located in non-EU countries are not necessarily subject to the GDPR, it conditions the possibility for EU controllers to transfer data.[56] Article 44 GDPR establishes that Chapter V shall be applied in order 'to ensure that the level of protection of natural persons guaranteed by the regulation is not undermined'.

The ambit of the notion of data transfer is not as straightforward as it may seem. There is no definition within Article 4 GDPR, and Article 44 simply refers to personal data transferred to a third country or an international organisation that are, or are intended to be, processed in that country or within that organisation.[57] While this appears to exclude personal data simply *in transit* – i.e. 'just electronically routed through' a third country but not geared towards it –,[58] it stems from the European Data Protection Supervisory (EDPS) and the EDPB guidance that the *transfer* notion is quite broad and not limited, as one could think, to the permanent copy of information to a server located in a third country.

For instance, the EDPB reaffirmed in its 2020 Frequently Asked Questions that the mere access to data from a third country constitutes a transfer in the meaning of the GDPR[59]. Therefore, when a controller grants access to a set of its data to a company located in a third country, this constitutes a transfer subject to limitations. This is the case regardless of where the controller's data are physically located. Onward transfers – i.e. transfers from a third country to another third country – are also covered[60]. Furthermore, it is in principle sufficient for the controller to be subject to the GDPR to trigger the data transfer regime, without necessarily being located in the EU.[61] The EDPS had previously proposed to define data transfers as the 'communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it',[62] and even went so far as to take the stance that, in some cases, the mere

[55] Article 1(3) GDPR
[56] Recital 101 GDPR
[57] For the sake of clarity, 'international organisations' will not be mentioned in this thesis; For an analysis on data transfers to international organisations, see Ioannis Ntouvas, 'Exporting personal data to EU-based international organizations under the GDPR' (2019) 9 [4] *International Data Privacy Law* 272
[58] See for instance this United Kingdom DPA's guide published before Brexit: United Kingdom DPA (Information Commissioner's Office, ICO), 'Guide to the General Data Protection Regulation (GDPR)', <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> (2 August 2018); See also EDPS (n 62)
[59] European Data Protection Board, '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' (23 July 2020) 5 <https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf>
[60] Article 44 GDPR
[61] There is no mention of the origin of the data in Article 44, but there is no reason for the regime not to be applicable as soon as the processing activities of the controller are covered by Article 3 defining the territorial scope of the GDPR.
[62] European Data Protection Supervisory, 'The transfer of personal data to third countries and international organisations by EU institutions and bodies [Position paper]' (15 July 2014) 7 <https://edps.europa.eu/data-protection/our-work/publications/papers/transfer-personal-data-third-countries_en>

'publication of personal data on the Internet by an EU controller' may constitute a data transfer if 'certain information is deliberately made available to recipients in a third country'.[63] Such a loose concept of data transfer – virtually encompassing a broad range of situations, hence highlighting the importance of ensuring transfer compliance – is more a legal fiction than a palpable reality, which brings us back to the criticisms of the GDPR mentioned in the Introduction.[64] This has led some authors to speak rather of "international processing".[65]

Nevertheless, to be lawful, data transfers to a third country such as the US must rely, in addition to the legal ground for processing[66], on one of the bases enshrined in Chapter V GDPR on international data transfers[67] which already existed in substance in the DPD.[68]

Article 45 GDPR establishes the first mechanism for data transfers, namely the adequacy decision. By means of an implementing act, the Commission can declare that a third country ensures an adequate level of protection, thus allowing data exporters to proceed with data transfers without any further authorisation nor safeguards.[69] Article 45(2) enumerates the criterion on which the Commission's assessment shall be based, including *inter alia* the rule of law and respect of human rights in the third country, the effectivity of the data subject's rights and the access to effective remedies, as well as the existence of a DPA, and international agreements entered into by the third country. The Article 29 Working Party released an Adequacy Referential,[70] now endorsed by the EDPB,[71] identifying the core elements and minimum requirements to be taken into account during such assessment.[72] From the data exporter perspective, such a basis for data transfer is obviously the most convenient.

In the absence of an adequacy decision, data exporters can only transfer data by implementing appropriate safeguards as listed in Article 46 GDPR and providing data subjects with enforceable rights and effective remedies.[73] The list includes *inter alia* reliance on pre-approved/pre-reviewed standard data protection clauses (also referred as Standard Contractual Clauses or SCCs) to be embedded, unaltered,[74] in a contract between a controller and/or a processor, Binding Corporate Rules (BCRs) within a group of undertakings, approved code of

---

[63] Ibid; This position is derived by contrast with the *Lindqvist* case in which the CJEU held that a publication on the Internet 'in circumstances such as those in the case in the main proceedings' was not a data transfer; Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECLI:EU:C:2003:596 [61]

[64] Kuner (n 26)

[65] Paul M. Schwartz, 'Information Privacy in the Cloud' (2013) 161 University of Pennsylvania Law Review 1623

[66] Article 5(a) and 6 GDPR; This is inferred from Article 4(2) GDPR, according to which 'disclosure by transmission, dissemination or otherwise making available' is a processing activity, thus requiring a legal ground under Article 6 GDPR.

[67] Voigt and von dem Bussche (n 52)

[68] Paul Van den Bulck, 'Transfers of Personal Data to Third Countries' (2017) 18 ERA Forum 229, 229 and 232

[69] Article 45(1) GDPR; See also Commission, Communication COM/2017/07 final from the Commission to the European Parliament and the Council, 'Exchanging and protecting personal data in a globalised World' (10 January 2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN>

[70] Article 29 Working Party, 'Adequacy Referential' WP 254 rev.01 (6 February 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>

[71] European Data Protection Board, 'Endorsement 1/2018' (25 May 2018) <https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_fr>

[72] See also Julian Wagner, 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?' (2018) 8 International Data Privacy Law 318 <https://doi.org/10.1093/idpl/ipy008>; See also Article 29 Working Party, 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' WP 12 (1998) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf>

[73] Article 46(1) GDPR; See also Van den Bulck (n 68) 240

[74] Recital 109 GDPR

conduct, and approved certification mechanism. Article 46(3) allows for other safeguards subject to case-by-case prior authorisation from the competent DPA. As will be seen, it has now been confirmed that in order to fulfil the requirements of Article 46, data exporters often have to combine several of the mechanisms mentioned above and take, on a case-by-case basis, supplementary (technical) measures[75] that will be further developed in Chapter 3.

Finally, and only in the absence of an adequacy decision and of appropriate safeguards,[76] Article 49 lays down 7 derogations for specific situations in occasional[77] circumstances, as well as a derogation for non-repetitive, small-scale transfers necessary for compelling legitimate interests if suitable safeguards are provided. The EDPB specified in 2018 and reinstated in 2020 that those restrictions have 'an exceptional nature', 'must be interpreted restrictively'.[78] This legal base remains very limited for controllers and processors wishing to engage in data transfers and will therefore not be considered further in this thesis.

2.4 The Safe Harbor and the *Schrems I* judgement: First opening of the Pandora's box

In 2000, at the time of the DPD, the Commission took the so-called "Safe Harbor" decision allowing data transfers to the US.[79] It considered that the Safe Harbor self-certification mechanism put in place in the US[80] was ensuring an adequate level of protection, thus allowing EU data exporters to transfer data to US self-certified companies without any other requirements.[81] In 2013, Maximilian Schrems lodged a complaint[82] with the Irish Data Protection Commissioner (DPC) to challenge the validity of Facebook Ireland's reliance on the Safe Harbor for transferring his personal data to Facebook INC established in the US.[83] Mr Schrems argued that the law and practice in force in the US did not ensure an adequate level of protection given the surveillance activities of the NSA revealed by Edward Snowden (as exposed in the Introduction).[84] The DPC rejected the complaint and refused to investigate because it considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA, and because the transfer was based on the Commission's decision.

Mr Schrems appealed before the Irish High Court, which stayed the proceedings and referred the matter to the CJEU for a preliminary ruling. The CJEU examined in substance (i)

[75] See in particular EDPB Rec. 01/2020 Version 2.0 (n 184)
[76] This hierarchy is deduced from Article 49(1), and Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' WP 114, 8ff (25 November 2005) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>
[77] Recital 111 GDPR
[78] See EDPB Rec. 01/2020 Version 2.0 (n 184) and European Data Protection Board, 'Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679' (25 May 2018) <https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en>
[79] 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) [2000] OJ L 215
[80] Incorporated as Annex I in the Safe Harbor Decision (n 79)
[81] Safe Harbor Decision (n 79), in particular Recital 2 and 5 and Article 1
[82] Under Article 28 DPD, curent Article 77 GDPR
[83] *Schrems I* judgement (n 4) [26-36]
[84] See Chapter 1, Section 1.1 of this paper

whether the DPD had to be interpreted as granting the power to DPAs (such as the DPC) to investigate despite a Commission's decision[85] and (ii) the validity of the decision itself.[86]

Regarding the first issue, the CJEU declared that a DPA retains the right to investigate an individual complaint because a Commission's decision 'cannot eliminate or reduce the powers expressly accorded to the national [DPA]' by the Charter and the Directive.[87] However, the Court recalled that it has sole jurisdiction to invalidate such a decision, so that if a DPA were to consider a claim as well-founded, it would then have to initiate legal proceedings. As will be developed later on, this paved the way for the introduction of the *Schrems II* ruling.

Regarding the second issue, the Court began by specifying that an 'adequate' level of protection[88] does not require an 'identical' one, but requires that the third country '*in fact* [ensures], by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union'.[89] When conducting its assessment, the Commission shall not only ensure that the third country's legal order is prescribing such a level of protection, but also that it is effective in practice.[90] Moreover, the Court held that the Commission has to periodically review the relevance of such a decision, especially when doubts are raised on its validity[91] – a requirement that has now been incorporated in Article 45(3) GDPR.

In species, the Court raised a series of observations with respect to the Safe Harbor and US law and concluded that the Commission's decision was invalid. Firstly, the Safe Harbor principles[92] were solely applicable to self-certified companies, excluding US public authorities.[93] They may in addition be limited for national security reasons, public interests, LEAs requirements, and even 'overriding legitimate interests'.[94] The Safe Harbor also provided that in case of conflicting obligations with US law, the latter should always prevail without limitations.[95] Secondly and concurrently, the Commission's decision did not assess whether there were US rules ensuring an adequate level of protection[96] and limiting the interferences at stake.[97] Thirdly, US law did not provide data subjects with effective legal remedy, since the FCC's jurisdiction referred in the Safe Harbor was limited, and in particular unable to rule on against interferences originating from the State.[98] The Court recalled that EU law requires interference to private life and the data protection right limited to what is strictly necessary,[99] which, in view of the above considerations, the Court found as not being the case in this instance.[100] Besides, Article 3(1) of the Commission's Decision precluding DPA(s) from

[85] *Schrems I* judgement (n 4) [37-66]
[86] Ibid [67-106]
[87] Ibid [53]; Article 8(3) Charter and Article 28 DPD
[88] Required by Article 25(6) DPD, current Article 45 GDPR
[89] *Schrems I* judgement (n 4) [73]; Emphasis added
[90] Ibid (n 4) [74-75]
[91] Ibid (n 4) [76]
[92] Included in Safe Harbor Decision (n 79) Annex I
[93] *Schrems I* judgement (n 4) [82]
[94] Ibid [84]
[95] Ibid (n 4) [85-86]
[96] Ibid (n 4) [83]
[97] Ibid (n 4) [88]
[98] Ibid [89]; The Court noted that the Commission itself had formerly raised the deficiency in a communication; *Schrems I* judgement (n 4) [90]
[99] *Schrems I* judgement (n 4) [91-92]; e.g. Case C-293/12 and C-594/12 *Digital Rights Ireland and Other* [2014] EU:C:2014:238
[100] Ibid (n 4) [93-95]

exercising their investigative powers with respect to the Safe Harbor was contrary to the DPD.[101]

In this ruling, the Court mainly conducted a review of the Safe Harbor regime as elaborated in the Commission's decision, which was sufficient to conclude that there was *de facto* no adequate level of protection of data subject's rights. While it appears clear that the US mass surveillance practices revealed in 2013 played a role in the case,[102] only two paragraphs (§93 and §94) make explicit reference to US law, giving rise to a straightforward but relatively cursory examination by the Court on that respect. Emphasis was placed on the shortcomings of the Commission's assessment with regard to EU law and the lack of effective remedies.

As a result of the ruling in 2015, EU data exporters were left with only the legal bases of Articles 46, 47 or 49 mentioned *supra* to conduct data transfers.[103] The available SCCs were swiftly amended 'to avoid a possible invalidation by the CJEU for not appropriately recognising the powers of supervisory authorities',[104] and, exactly one year later, the Commission issued a new adequacy decision: The Privacy Shield.[105]

2.5 The Privacy Shield and the *Schrems II* judgement: A logical follow-up

2.5.1 The Commission's decision declaring that the Privacy Shield programme offered an adequate level of protection

The Privacy Shield[106] adopted in July 2016 authorised again data transfers to the US without additional requirements. Similar to the Safe Harbor, this was a partial adequacy decision enabling transfers to companies that self-certified under the programme.[107] While the Safe Harbor decision consisted of approximately 45 pages (including Annexes) in the Official Journal of the EU, the Privacy Shield consisted of nearly 115 pages[108] describing the privacy principles[109] and mechanisms supposed to address the issues raised in the *Schrems I* judgement.

The US Department of Commerce (hereinafter USDC) was tasked to 'monitor and actively verify that companies' privacy policies are in line with the relevant Privacy Shield principles and readily available to the public'[110], while the Privacy Shield established several different remedies to data subjects.[111]

---

[101] Ibid [99-104]
[102] See in particular the observations of the Irish High Court; *Schrems I* judgement (n 4) [30-33]
[103] The Article 29 Working Party suggested a three-month 'grace period' for enforcement action; Article 29 Working Party, 'Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)' (16 October 2015) <https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>
[104] Van den Bulck (n 68) 244
[105] 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 (notified under document C(2016) 4176) [2016] OJ L 207
[106] Privacy Shield Decision (n 105)
[107] Ibid
[108] Safe Harbor Decision (n 79) and Privacy Shield Decision (n 105)
[109] Privacy Shield Decision (n 105) Annex II
[110] Commission, 'Fact Sheet EU-U.S. Privacy Shield: Frequently Asked Questions' (12 July 2016) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462>
[111] Sebastian Klein, 'First Annual Review of the EU-US Privacy Shield' (2017) 3 Eur Data Prot L Rev 512, 514

First, the data subject could file a complaint with the relevant organisation (but was not compelled to);[112] second, it may lodge a complaint with a national DPA in the EU, that would then be forwarded to the USDC;[113] third, US companies had the opportunity to set up independent recourse mechanism (i.e. alternative dispute resolution)[114] – in either the EU or in the US but providing effective enforcement mechanisms – available to data subject free of charge.[115] Ultimately, individuals had the right 'to invoke binding arbitration under the Privacy Shield Panel'.[116] There was no hierarchy between those mechanisms, except for the latter.[117] Interestingly, the Privacy Shield also provided for an Ombudsman appointed to remedy disputes with US authorities and supposed to be 'independent from the Intelligence Community'.[118]

It is clear from the Privacy Shield that the Commission had paid particular attention to the establishment of multiple effective remedies, with the aim of responding to the criticisms of the *Schrems I* ruling.[119] Still, at the dawn of the Privacy Shield, EU data exporters were already having doubts about its legality and tended to rely instead on SCCs, 'the main reason [being] that an unclear legal situation remain[ed] in view of the concerns voiced by an Irish human rights organisation.[120] Indeed, two months after the Privacy Shield entered into force, an Irish association sought its annulment before the CJEU.[121] The case was declared inadmissible for lack of interest in bringing proceedings, but the unanswered issues remained nonetheless relevant. An in-depth analysis from the European Parliamentary Research Service in 2018[122] stated that the Working Party 29 pointed out in the first annual review of the Privacy Shield 'some issues […] unresolved'[123] and that a (non-binding) Parliament resolution[124] later raised, in particular, the implications of the then-new US CLOUD Act.[125] Concurrently, a 2017 CJEU opinion about a draft data exchange agreement with Canada enshrined a strict standard as to the European law level of protection.[126] Ultimately, the *Schrems II* case[127] was initiated in May 2018, further undermining confidence in the Privacy Shield.[128]

---

[112] Privacy Shield Decision (n 105) Annex II, III(11)(d)(i)
[113] Ibid Recital 52
[114] Klein (n 111)
[115] Privacy Shield Decision (n 105) Recitals 39 and 40
[116] Ibid Recital 42
[117] Ibid
[118] Ibid Recital 65
[119] See, for instance, Privacy Shield Decision (n 105) Recital 41 reinstating that the Privacy Shield 'provides data subjects with a number of possibilities to enforce their rights'
[120] Klein (n 111); See also IAPP-EY (n 238)
[121] Case T-670/16 *Digital Rights Ireland v Privacy Shield* [2017] ECLI:EU:T:2017:838
[122] European Parliamentary Research Service (Shara Monteleone and Laura Puccio), 'The Privacy Shield – Update on the state of play of the EU-US data transfer rules' (July 2018) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2018)625151>
[123] Article 29 Working Party, 'EU-US Privacy Shield- First annual joint Review' WP 255 (28 November 2017) <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782>
[124] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html>
[125] On the Cloud ACT, See Chapter 1, Section 1.1 of this paper
[126] Opinion 1/15 of the Court (Grand Chamber) [2017] ECLI:EU:C:2017:592; For an analysis, see Monika Zalnieriute, 'Developing a European Standard For International Data Transfers After Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' [2018] SSRN Electronic Journal <https://www.ssrn.com/abstract=3330357>
[127] *Schrems II* judgement (n 1)
[128] Klein (n 111)

2.5.2 The comprehensive *Schrems II* judgement

Background — In 2015, pursuant to the *Schrems I* judgement, the Irish High Court overturned the DPC's decision dismissing Mr Schrems' complaint. The DPC undertook before the Court to promptly reach a decision on the initial complaint seeking suspension or prohibition of transfer to Facebook INC.[129] Because Facebook Ireland could no longer transfer its data to the US under the invalidated Safe Harbor, it was henceforth relying on SCCs to keep data transfers going.[130] Afterwards, Mr Schrems reformulated his complaint at the request of the DPC, reinstating in substance that Facebook, even when bound by SCCs, was compelled under US law to make his data available to US authorities, in particular LEAs, which process personal data in a manner incompatible with the EU Charter, and that there were no effective remedies available to individuals.[131]

In May 2016, the DPC published a draft decision with the provisional view that Mr Schrems' claim was well-founded[132] and, in particular, that the SCCs at stake were not capable of remedying those issues.[133] Nevertheless, the reasoning developed in the *Schrems I* judgement that the CJEU has sole jurisdiction to invalidate an adequacy decision emanating from the Commission[134] applies *mutatis mutandis* to decisions approving SCCs. Therefore, the DPC filed a lawsuit against Facebook and Mr Schrems with the aim of a preliminary ruling.[135] In turn, the Irish High Court referred 11 questions to the CJEU[136] in relation to the SCCs as well as the Privacy Shield that was adopted in the meantime. It is worth noting that the DPC had the power to take a decision on the complaint at stake prior to a CJEU outcome on the overall validity of the SCCs and the Privacy Shield[137] (and had even undertaken before the Irish Court to swiftly do so), but nevertheless decided to pause the ongoing complaint during the whole time of the CJEU proceedings – a move that has been criticized by Mr Schrems.[138]

At the time of the ruling, the transfers were occurring under the GDPR which had meanwhile entered into force; for this reason, the Court answered the questions in *Schrems II* 'in the light of the […] GDPR rather than […] the [DPD]'.[139] Interestingly enough, the Court also confirmed that transfer of personal data potentially subject to further processing for national security purposes in a third country falls under the scope of the GDPR.[140] Although Article 2 on material scope excludes some kinds of processing of personal data, notably those by competent authorities regarding criminal offences and public security,[141] the mere transfer between two economic operators is a processing activity in itself subject to the GDPR and

[129] *Schrems II* judgement (n 1) [77]
[130] Ibid [54]
[131] Ibid [54-55]
[132] Ibid [60-65]; The Irish High Court notably found that the US authorities' intelligence activities are based, among others, on FISA and Executive Order 12.333 (see (n 19)) and that EU citizens have not the same rights as US citizens under US Constitution, as already developed in Chapter 1, section 1.1 of this paper
[133] *Schrems II* judgement (n 1) [56]
[134] See this Chapter, Section 2.4
[135] *Schrems II* judgement (n 1) [57]
[136] Ibid [68]
[137] As was confirmed by the CJEU, see end of this Section
[138] 'Is the DPC actually stopping Facebook's EU-US data transfers?! ..maybe half-way!' (*noyb*, 9 September 2020) <https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way> accessed 1 March 2021
[139] *Schrems II* judgement (n 1) [77-79]
[140] Ibid [80-89]
[141] Article 2(2)(d) GDPR; Regarding Member States' enforcement authorities, another Directive is applicable – See Recital 19 GDPR

Chapter V, irrespective of the fact that the data may subsequently be processed by said authorities.[142] Similar reasoning was followed a few months later in the *Privacy International* judgement.[143]

Privacy Shield invalidity[144] —After the Court recalled that EU law enshrines the rights to respect for private life and data protection, the principle of proportionality of Article 52(1) Charter and the case law establishing that interferences must be limited to what is strictly necessary,[145] it then proceeded to examine in-depth US law and its compatibility with those requirements. It found that the United States Foreign Intelligence Surveillance Court is only 'designed to verify whether th[e] surveillance programmes relate to the objective of acquiring foreign intelligence information, but […] does not cover the issues of whether individuals are properly targeted',[146] that the FISA[147] 'does not indicate any limitations on the power it confers to implement surveillance programmes'[148], and that neither the Presidential Policy Directive 28 (imposing to some extents limitations for 'signals intelligence' operations)[149] nor the E.O. 12.333[150] confers enforceable rights against US authorities.[151] The Court held consequently that surveillance and bulk-interception programmes based on those provisions are not limited to what is strictly necessary as required by the Charter and do not ensure an essentially equivalent level of protection.[152]

In addition to the finding of a violation of Article 7 and 8 Charter (establishing the privacy and data protection rights), the Court ruled that the Privacy Shield violated Article 47 Charter enshrining the right to an effective remedy, which is part of the EU level of protection and should therefore have been taken into account by the Commission's assessment.[153] It held that, despite the remedies enshrined within the Privacy Shield, no effective remedy was actionable against US authorities acting under surveillance programmes, even with the appointed Ombudsman.[154] In particular, the Ombudsperson was not truly independent as they were appointed by and reported directly to the Secretary of State.[155]

This invalidation goes further than the previous *Schrems I* judgement on significant aspects. In the *Schrems I* judgement, the Court focused mainly on the Commission's assessment and the way it was carried out in relation to EU secondary law, i.e. the DPD. This seems to have led the Commission to underestimate the deeper systemic issues raised in the ruling, as powerfully illustrated in one of the first recitals of the Privacy Shield decision stating that: 'Without examining the content of the Safe Harbour Privacy Principles, the Court [in *Schrems I*] considered that the Commission had not stated in that decision that the United States in fact

[142] *Schrems II* judgement (n 1) [85-89]
[143] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790 [38-49]
[144] *Schrems II* judgement (n 1) [150-202]; [150-162] exposes the reasons why the Court assessed the validity of the Privacy Shield even though this was not literally requested
[145] *Schrems II* judgement (n 1) [168-177]
[146] Ibid [179]
[147] FISA (n 19)
[148] *Schrems II* judgement (n 1) [180]
[149] Privacy Shield Decision (n 105) Recital 69; See in particular *Schrems II* judgement (n 1) [183]
[150] E.O. 12.333 (n 19)
[151] *Schrems II* judgement (n 1) [181-182]
[152] Ibid [184-185]
[153] Ibid [186-189]
[154] Ibid [190-197]
[155] Ibid [195]

'ensured' an adequate level of protection by reason of its domestic law or its international commitments'.[156] In the new *Schrems II* judgment, the Court carried out a thorough examination of the US law itself and loudly affirmed its incompatibility with the level of protection of EU law, ultimately concluding that the Privacy Shield programme as well as US law were in direct violation of Articles 7, 8 and 47 of the Charter (which are part of European primary law), in addition to Article 45(1) GDPR (secondary law). [157]

Regarding the consequences of the immediate invalidation, the Court noted that other data transfers mechanisms exist under GDPR, so that it does not create a 'legal vacuum'.[158] The Court is notably referring to SCCs, that have been reviewed in the remaining parts of the ruling.

SCCs validity — It follows from the judgment that SCCs are not intended to guarantee *per se* an appropriate level of protection, but rather constitute a tool at the disposal of the data exporter to achieve that aim.[159] Indeed, because of their inherently contractual nature, SCCs are unable of binding the authorities of the third country and therefore the recipient cannot guarantee adequate protection (although there may theoretically be instances where such clauses might be sufficient).[160] Since Article 46 GDPR on transfers subject to appropriate safeguards is directed towards data exporter, this is up to the data exporter to provide, on a case-by-case basis, additional guarantees to ensure the level of protection.[161] As a corollary, when issuing SCCs the Commission is not required to assess the level of protection in the third countries to which data can be transferred,[162] but must nevertheless aim at incorporating 'effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection […]'.[163]

Regarding the validity of the SCCs 2010/87 at stake,[164] the Court, after having ascertained *inter alia* that the decision did not infringe the powers of the DPAs,[165] found nothing affecting their validity.[166]

The last remaining piece of the puzzle was to determine the level of protection that the data exporter must pursue when implementing appropriate safeguards under Article 46 GDPR, as well as the criteria to be considered.[167] The Court held that Article 46 GDPR must be read in conjunction with Article 44 which provides for the principle that data subject rights may not be undermined when data transfers are conducted.[168] The Court followed the Advocate General's Opinion according to which appropriate safeguards and guarantees under Article 46 must therefore ensure 'a level of protection *equivalent* to that which is guaranteed within the

[156] Privacy Shield Decision (n 105) Recital 9
[157] *Schrems II* judgement (n 1) [198-201]
[158] Ibid [202]
[159] Ibid [131-135]
[160] Ibid [125 ,126, 132]
[161] Ibid [131-134]
[162] Ibid [130]
[163] Ibid [137]
[164] Commission Decision 2010/87/EC of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 [2010] OJ L 39; Amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [2016] OJ L 344
[165] See (n 87)
[166] *Schrems II* judgement (n 1) [149]
[167] Ibid [90-105]
[168] Ibid [92-93]

European Union'[169] and more specifically in the Charter.[170] In other words, the reference level to be sought by the data exporter is the same as the level determined in the *Schrems I* judgement when the Commission drafts an adequacy decision.[171] Therefore, the relevant assessment criteria are the same as those non-exhaustively enumerated in Article 45(2) GDPR.[172] Hence, the data exporter using SCCs must take into account, in addition to their content, 'the relevant aspects of the legal system of that third country' in particular with regard to any access by the third country's public authorities to the personal data transferred.[173] Following the judgement, some professionals have consequently used the term 'Transfer Impact Assessment' despite its absence in the *Schrems II* ruling.[174]

DPAs duties — In the last question, the Court asserted that in the absence of an adequacy decision, DPAs not only have the power but also the obligation to suspend or prohibit a transfer of data pursuant to SCCs if it is established that 'those clauses […] cannot be complied with in the third country' and thus do not enable an equivalent level of protection from being ensured.[175] The DPAs can therefore exercise independently their powers of investigation as well as enforcement in the context of SCCs, as opposed to the situation where a DPA investigation considers that an adequacy decision is invalid, thus necessitating referral to the CJEU.

In summary, the Court confirmed and reinforced the lessons of its *Schrems I* ruling, and coherently invalidated the Privacy Shield while leaving the SCCs available as one of the transfer tools available to data exporters.

2.6 Conclusion: Combined judgements that are not without significance

Although the *Schrems II* judgment may have surprised some early observers *prima facie*[176] by invalidating the Commission's adequacy decision while not invalidating the SCCs issued by the Commission, it is in fact consistent with both the *Schrems I* judgement as well as the scheme of Article 46, which is not intended to create a quasi-automatic right of transfer as did the Privacy Shield and the Safe Harbor under Article 45.

It can be further concluded that since the *Schrems* saga, the responsibility to conduct an adequate processing of transferred data is no longer predominantly vested in self-certified US data importers who are concurrently obliged to comply with US laws (which takes precedence over contracts), but is now heavily entrusted to data exporters subject to investigation and enforcement.

---

[169] Ibid [96]; Emphasis added
[170] Ibid [97-101]
[171] Ibid [96]; See (n 89)
[172] *Schrems II* judgement (n 1) [102-105]
[173] Ibid
[174] Richard Cumbley, Tanguy Van Overstraeten and Georgina Kon, 'The Schrems judgment – Transfer Impact Assessments for international data transfers?' (*Linklaters Blogs*, 16 July 2020) <https://www.linklaters.com/en/insights/blogs/digilinks/2020/july/the-schrems-judgment> accessed 28 February 2021
[175] *Schrems II* judgement (n 1) [106-121]
[176] 'BREAKING: Unexpected Outcome of Schrems II Case: CJEU Invalidates EU-U.S. Privacy Shield Framework but Standard Contractual Clauses Remain Valid' (*Hunton Privacy Blog*, 16 July 2020) <https://www.huntonprivacyblog.com/2020/07/16/breaking-unexpected-outcome-of-schrems-ii-case-cjeu-invalidates-eu-u-s-privacy-shield-framework-but-standard-contractual-clauses-remain-valid/> accessed 20 November 2021

While the SCCs and safeguards of Article 46 survived *Schrems II*, the next chapter will review to what extent they can palliate the sudden disappearance of the Privacy Shield in the field. Many economic actors have started to rely extensively on those, yet it is clear from the *Schrems II* judgment that the use of SCCs and other safeguards must be accompanied by thorough checks and supplemental measures to form a lawful basis.

Chapter 3 – Transfer tools and technical safeguards remaining available to data controllers, and limitations thereof

"Country in which there are precipitous cliffs with torrents running between, deep natural hollows, confined places, tangled thickets, quagmires and crevasses, should be left with all possible speed and not approached."

"When in difficult country, do not encamp. In country where highroads intersect, join hands with your allies. Do not linger in dangerously isolated positions. In hemmed-in situations, you must resort to stratagem. In a desperate position, you must fight."

Sun Tzu [177]

3.1 Introduction

The post-*Schrems II* situation unsurprisingly generated a strong reaction in the community of privacy professionals, with European companies (as well as third-country companies subject to the GDPR)[178] worried about being out of compliance. Because of the very broad notion of transfer, any company is potentially affected.[179] Numerous resources and strategies, such as what some call a 'defensible position', have proliferated in an attempt to minimize non-compliance risk and ultimately conduct lawful transfers under GDPR transfer tools.[180] This Chapter will focus on how data exporters can still lawfully conduct data transfers since *Schrems II* in light of the new EDPB Recommendations and the new Commission's SCCs.

The chronological timeline is an important element in understanding the developments since the *Schrems II* judgment. A *draft* of the EDPB Recommendations 01/2020 'on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'[181] was published in November 2020 for public consultation, followed two days later by a *draft* of new SCCs by the Commission.[182] Then, a *final* version of the SSCs was adopted early-

[177] See (n 39)
[178] As per the extra-territorial scope of Article 3(2) GDPR, further analysed in Chapter 4 of this paper
[179] As developed *supra*, Chapter 2, Section 2.3 of this paper
[180] See, for an example among others, Anonos website <https://www.anonos.com/schremsii-solution> accessed 12 April 2021
[181] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020, version for public consultations) <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en>
[182] Draft Commission implementing decision (EU) 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 Ares(2020)6654686 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries> accessed 8 January 2021

June 2021,[183] and the *final* version of the EDPB Recommendations was issued mid-June 2021.[184]

Section 3.2 will examine the backbone of the EDPB Recommendations – which is the same in both versions – by exposing the EDPB's methodology and the additional measures that, combined with the traditional transfer tools, can in practice enable lawful data transfers. Then, Section 3.3 will assess the added value of the modernised SCCs, and to what extent they provide new possibilities regarding the issues raised in *Schrems II*. Section 3.5 will ascertain the adaptations that were made in the *final* version of the EDPB Recommendations after the public consultation. Finally, Section 3.6 will conclude on the current state of affairs for data exporters.

Besides, it should be noted that, shortly after the invalidation of the Privacy Shield, the European Commissioner for Justice and the US Secretary of Commerce issued a joint statement announcing that they had 'initiated discussions to evaluate the potential' of a new adequacy decision.[185] Six months later, in March 2021, the European Commission stated that they were 'intensifying negotiations'.[186] However, such an undertaking remains risky in light of the *Schrems* developments and especially when, as noted by Christakis, the US is actively pushing to exclude international surveillance and "direct access" from the negotiations even though their supporting arguments are similar to those that were brought in the past.[187] Among others, the US argues that there is a 'double standard' because the EU allegedly allows similar international surveillance practices in its Member States as in the US. This argument could be somewhat backed up by the *Privacy International* case mentioned above which seems to grant a wider margin of appreciation to the Member States than in the CJEU's previous case law.[188] Given the fragility of this track and for the sake of space, these negotiations will not be dealt with further. On another note, it will also be interesting to keep an eye on the evolution of the post-Brexit negotiations for an adequacy decision between the EU and the United Kingdom,[189] since the latter might also consider an adequacy decision with the US,[190] as the EDPB has already stressed in its opinion on the UK adequacy decision.[191]

---

[183] Commission Implementing Decision (EU) 2021/914 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 [2021] OJ L 199

[184] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Version 2.0' (18 June 2021, version after public consultations) <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>

[185] Commission Joint Press Statement (n 23)

[186] Commission, 'Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo' (25 March 2021) <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_144>

[187] Theodore Christakis, 'Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)' (*European Law Blog*, 12 April 2021) <https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/> accessed 12 April 2021

[188] Ibid; *Privacy International* judgement (n 143)

[189] See Commission, 'Data protection: European Commission launches process on personal data flows to UK' (19 February 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661>; See for more insights Kenneth Propp, 'Do continued EU data flows to the United Kingdom offer hope for the United States?' (Atlantic Council, 14 April 2021) accessed 20 May 2021

[190] See this interesting article by UK Minister for Media and Data: John Whittingdale, 'The UK's new, bold approach to international data transfers' (Privacy Laws & Business, March 2021) <https://www.privacylaws.com/uk114data> accessed 30 April 2021

[191] European Data Protection Board, 'Adopted Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the

3.2 The EDPB's methodology and proposed supplementary measures

3.2.1 The EDPB's methodology

As stated multiple times now, transfer mechanisms laid down in Article 46 GDPR should be seen as *tools* available to data exporters to ensure that personal data are transferred in a way that does not undermine the level of protection conferred by EU law to individuals. The substantial requirement of Article 46(1) is for data exporters to 'compensate for the lack of data protection in a third country',[192] while Article 46(2) and (3) provides a *non-exhaustive* list of such appropriate safeguards.

As a result, data exporters have to assess the level of data protection established in the (specific territory of a) third country by *law* and in *practice*, and adopt safeguards able to guarantee to data subjects an essentially equivalent level of protection. The EDPB made it clear that *Schrems II*'s conclusions apply *mutatis mutandis* to transfer tools other than SCCs.[193] The Recommendations provide a step-by-step guide on how to comply with Chapter V GDPR in general and with Article 46 GDPR in particular. When no adequacy decision or applicable derogation is available,[194] the steps can be summarized as follows:

Step 1 — Data transfer mapping:[195] The data exporter should be 'fully aware' of its current or intended transfers, including onwards transfers.

Step 2 — Choosing a transfer tool: the data exporter should choose on which tool(s) of Article 46(2) it will rely on:[196] This may be the current SCCs or, if within groups of undertakings, Binding Corporate Rules (BCRs), as well as the adherence, with binding commitment, to an approved code of conduct or certification mechanism.

Step 3 — Assessment of the level of protection in the third country when relying on the sole transfer tool(s):[197] The EDPB recalls that each tool enumerated in Article 46 'mainly contains appropriate safeguards of a contractual nature' that are subordinate to the law and may therefore need supplementary (technical) measures.[198] As a consequence, data exporters are required to assess, by law and in practice,[199] whether the foreign law impedes the commitments resulting from the chosen transfer tool.[200] In order to conduct the assessment of the level of protection of the third country with regard to interferences to fundamental rights by States and LEAs, the EDPB issued separate Recommendations detailing the substance of the 'essential guarantees' enshrined in the EU Charter which shall be met in the third country to conclude to an *essentially equivalent* level of protection.[201] For the US, an overall assessment has already

United Kingdom' (13 April 2021) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en>

[192] Recital 108 GDPR

[193] EDPB draft Rec. 01/2020 (n 181) [58]; EDPB Rec. 01/2020 Version 2.0 (n 184) [62]; See also EDPB Rec. 02/2020 (n 201) [5]

[194] Article 47 GDPR, as developed in Chapter 2, Section 2.3 of this paper

[195] EDPB draft Rec. 01/2020 (n 181) and EDPB Rec. 01/2020 Version 2.0 (n 184) [8-13]

[196] EDPB draft Rec. 01/2020 (n 181) and EDPB Rec. 01/2020 Version 2.0 (n 184) [14-27]

[197] EDPB draft Rec. 01/2020 (n 181) [28-44]; EDPB Rec. 01/2020 Version 2.0 (n 184) [28-49]

[198] EDPB draft Rec. 01/2020 (n 181) [23 and 58]; EDPB Rec. 01/2020 Version 2.0 (n 184) [23 and 62]

[199] EDPB draft Rec. 01/2020 (n 181) [28, 29, 30, 34 and 41]; EDPB Rec. 01/2020 Version 2.0 (n 184) [28, 29, 30, 36, 39 and 42]

[200] EDPB draft Rec. 01/2020 (n 181) [30 and 34]; EDPB Rec. 01/2020 Version 2.0 (n 184) [30 and 36]

[201] European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020) <https://edpb.europa.eu/our-work-tools/our-documents/recommend

been conducted thoroughly in the *Schrems II* judgement concluding that additional measures may be required,[202] but a data exporter must nevertheless assess any relevant applicable rules for the transfer at stake, e.g. depending on the sector, *etc*.[203] For instance, if the recipient is 'specifically protected by [the third] country's law, e.g., for the purpose to jointly provide medical treatment for a patient, or legal services to a client', then requirements are reduced.[204] As discussed below, the degree of stringency in pursuing this assessment appears to be the main element that has changed between the *draft* and the *final* versions of the Recommendations.

Step 4 — Adoption of supplementary measures:[205] They must be decided on a case-by-case basis and can be of a contractual, technical or organisational nature. Some of them are examined below.

Step 5 — Procedural steps once supplementary measures have been identified:[206] The supplementary measures might require the data exporter to re-assess on which transfer tool it is relying, for instance when the supplementary measures contradict the SCCs, or require contractual changes incompatible with the SCCs.[207]

Step 6 — Re-evaluation at an appropriate interval:[208] The data exporter must monitor – with the help of the data importer(s) if necessary – the developments in the third country because accountability is a continuing obligation.

3.2.2 Supplementary measures

Annex 2 of the EDPB Recommendations reviews, through several use cases, various additional measures (either contractual, technical or organisational) that may be implemented by a data exporter (in Step 4) in order to provide adequate safeguards under Article 46. At that point, the EDPB requires an assessment of the 'most effective measures' to address the risks.[209] Given the space available and the scope of this thesis, which is focused on transfers to major providers to the US, the analysis will be limited to an overview of the main technical measures proposed – to be used alone or in combination – and their limitations, excluding contractual and organisational measures which are of little help in this instance.[210]

Pre-transfer Encryption[211] — This is probably the most frequently mentioned solution. If the data exporter properly encrypts its data before transferring them (without decryption keys) to the third country, then those data are unreadable by the recipient and are therefore adequately

ations/recommendations-022020-european-essential-guarantees>; Also, Annex 3 'Possible sources of information to assess a third country' in EDPB draft Rec. 01/2020 (n 181) and EDPB Rec. 01/2020 Version 2.0 (n 184)

[202] While the draft version stated straightforwardly that, according to the *Schrems II* judgment, US law in its current form automatically imposes additional measures for data transfers, the final recommendations are less straightforward and leave the final assessment to the data exporter, who must take into account the *Schrems II* judgment; EDPB draft Rec. 01/2020 (n 181) [44]; EDPB Rec. 01/2020 Version 2.0 (n 184) [49]

[203] EDPB draft Rec. 01/2020 (n 181) and EDPB Rec. 01/2020 Version 2.0 (n 184) [33]

[204] EDPB draft Rec. 01/2020 (n 181) [85]; EDPB Rec. 01/2020 Version 2.0 (n 184) [91]

[205] EDPB draft Rec. 01/2020 (n 181) [45-54]; EDPB Rec. 01/2020 Version 2.0 (n 184) [50-58]

[206] EDPB draft Rec. 01/2020 (n 181) [55-61]; EDPB Rec. 01/2020 Version 2.0 (n 184) [59-66]

[207] EDPB draft Rec. 01/2020 (n 181) [56-57]; EDPB Rec. 01/2020 Version 2.0 (n 184) [50-61]

[208] EDPB draft Rec. 01/2020 (n 181) [62-63]; EDPB Rec. 01/2020 Version 2.0 (n 184) [67-68]

[209] EDPB draft Rec. 01/2020 (n 181) [49]; EDPB Rec. 01/2020 Version 2.0 (n 184) [54]

[210] Such measures could be relevant when the US data importer is specifically not targeted by US surveillance laws or, in other words, when the main surveillance laws are not applicable (and not applied in practice)

[211] EDPB draft Rec. 01/2020 (n 181) [79]; EDPB Rec. 01/2020 Version 2.0 (n 184) [84]

protected.[212] However, such encryption is only relevant when the importer does *not* need to access the data content in order to perform necessary processing activities on it, e.g. if the data importer is a Cloud backup provider.[213] Real-world use cases remain therefore quite limited.

It is also ironic to note that in late 2020, the Council of the EU passed a (non-binding) resolution to require encryption services to introduce mandatory backdoors allowing LEAs to access data upon request,[214] an old debate that re-emerged recently.[215] According to Kosta and Koops, however, history shows that such an approach is fundamentally flawed.[216]

Encryption in Transit[217] — In its Recommendations, the EDPB examined the possible interception of communications merely transiting through a third country before reaching a recipient in another country providing adequate protection. By interpreting the mere interception of communication in transit as a transfer, the EDPB seems to loosen even more the notion of transfer (in comparison with how it was interpreted so far by the EDPS, as explained above).[218] Encryption in transit protects data in transit while enabling the data importer to decrypt it upon arrival to read and process it thereafter. This solution is only efficient against interception, i.e. when data has not yet reached the importer. The EDPB considers this basic measure[219] and recommends it even when the data importer is specifically exempted from surveillance by the importer's law.[220] This makes sense since the functioning of the Internet does not allow one to know with certainty in which country the data could potentially transit.

End-to-end Data Encryption (E2EE)[221] — Traditional encryption in transit can be completed with additional E2EE between the exporter and the importer to make sure that only they have access to the data. Another implementation of E2EE not considered by the EDPB and that should be pointed out is the implementation, by the parties, of protocols that allow their users to end-to-end encrypt their communications between them. This is particularly relevant for consumer messaging applications: The application can, by design, encrypt any message on the data subject's own device before it goes through the data controller's server and then reaches the recipient of the message. As a result, even the data controller is unable to exploit the data, so that it can be freely transferred to a data importer that will not be able to do so either. The

---

[212] For a technical overview on cryptography, see Jinying Jia and Fengli Zhang, 'K-Anonymity Algorithm Using Encryption for Location Privacy Protection' (2015) 10 International Journal of Multimedia and Ubiquitous Engineering 155, 512–516

[213] This is the example given by the EDPB, see (n 211)

[214] Council Resolution of 24 November 2020 on Encryption, Security through encryption and security despite encryption <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf> ; See for an unfavourable reaction: Eduard Kovacs, 'Encrypted Services Providers Concerned About EU Proposal for Encryption Backdoors' (*Security Week*, 29 January 2021) <https://www.securityweek.com/encrypted-services-providers-concerned-about-eu-proposal-encryption-backdoors> accessed 15 February 2021

[215] See for instance in the US: Patrick Howell O'Neill, 'Barr's call for encryption backdoors has reawakened a years-old debate' (*Technology Review*, 24 July 2019) <https://www.technologyreview.com/2019/07/24/134062/trumps-justice-department-calls-for-encryption-backdoor-law/> accessed 6 May 2021

[216] Bert-Jaap Koops and Eleni Kosta, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 Computer Law & Security Review 890

[217] EDPB draft Rec. 01/2020 (n 181) [84]; EDPB Rec. 01/2020 Version 2.0 (n 184) [90]

[218] See Chapter 2, Section 2.3 of this paper, in particular EDPS (n 62)

[219] Encryption in transit is already broadly adopted, see for instance the Google statics on the evolution of the total number of https requests through Google Chrome: <https://transparencyreport.google.com/https/overview?hl=en&time_os_region=chrome-usage:1>

[220] See (n 204)

[221] EDPB draft Rec. 01/2020 (n 181) [84 and 85]; EDPB Rec. 01/2020 Version 2.0 (n 184) [90 and 91]

drawback of this technique is that it prevents lots of processing activities by the controller and the importer(s), even for potential legitimate purposes. Such an implementation could be seen as a kind of strong implementation of data protection 'by design and by default' as referred to in Article 25 GDPR, but is not always relevant.

Pseudonymisation[222] — This process is defined in the GDPR[223] and mentioned several times in it as a way to protect personal data. If transferred data are sufficiently pseudonymized beforehand, then the data importer is not able to attribute those data to specific individuals. Therefore, the level of protection of natural persons is not undermined. However, such a process is not easy and requires thorough technical assessments to determine if it would be possible, in particular for LEAs, to single out individuals behind a specific data set. Proper pseudonymisation is a challenge and ultimately a matter of reidentification risks, especially as recombination and data deduction techniques are evolving very rapidly. In fact, even *anonymized* data can potentially be de-anonymized in the future (as recalled by the EDPS),[224] which raises the limits of such techniques and requires data controllers to monitor technological developments.[225]

Split or multi-party processing[226] — Data is shared between several processors in different jurisdictions, in such a way that each data set cannot be attributed to an individual without additional information. In reality, this seems similar to the pseudonymisation technique, except that the data can be split between two or more processors in different third countries without requiring the data controller to own the reidentification information needed to reattribute the data. The EDPB requires an extra layer of security by prescribing that the data controller must ensure that LEAs in the processor's countries will not cooperate to recombine the data and gain access to personal data.

As one can observe, all those solutions – that are in fact trying to ensure that the essential element to 'unlock' the data is out of 'possession, custody or control' of the data importer in the wording of US law –[227] are intended for specific, and relatively limited, real-world use cases. In addition, they often require significant resources that most companies are unlikely to be able to afford. It must be concluded that, at least from the EDPB recommendations, all other transfers can no longer take place, which is not inconsequential, to say the least. The EDPB expressly refers to the case where a data importer is subject to intrusive data surveillance law and is required to have access to data 'in the clear' as a '[s]cenarios in which *no* effective measures could be found' ('Use case 6').[228] As T. Christakis commented,

> 'If we follow the EDPB guidance, companies in Europe will be unable to share their HR and employee data, customer files, or to operate any other intra-group transfers including personal data with their counterparts outside Europe. The branch of a

[222] EDPB draft Rec. 01/2020 (n 181) [80-83]; EDPB Rec. 01/2020 Version 2.0 (n 184) [85-89]
[223] Article 4(5) GDPR
[224] European Data Protection Supervisory, 'AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation' (27 April 2021) 5 <https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en> accessed 29 April 2021
[225] See Chris Reed, 'Information 'Ownership' in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No. 45/2010, 21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461>; For several real world examples, *inter alia* on supposedly 'anonymized' medical records, this blogpost is an interesting read: Richie Koch, 'The truth about anonymized data' (*Protonmail Blog*, 30 April 2020) <https://protonmail.com/blog/truth-about-anonymized-data/> accessed 7 May 2020
[226] EDPB draft Rec. 01/2020 (n 181) [86]; EDPB Rec. 01/2020 Version 2.0 (n 184) [92]
[227] As mentioned in the Introduction Chapter of this paper, Section 1.1
[228] EDPB draft Rec. 01/2020 (n 181) [88-89]; EDPB Rec. 01/2020 Version 2.0 (n 184) [94-95]; Emphasis added

European company in the US might not even be able to consult the agenda of its European members in order to fix a call. All this could lead to huge disruption for the everyday operations of international corporations.'[229]

3.3 First stage: Rejection, in the *draft* EDPB Recommendations, of the risk-based approach in the assessment of the third country law and practices

The assessment of the third country (Step 3) can be truly cumbersome and uncertain for companies, and regularly results, as stated by the EDPB itself,[230] in the conclusion that the transfer cannot take place. Consequently, some companies advocated for a 'risk-based approach' regarding data transfer. They argued that the risk-based approach enshrined in several GDPR articles[231] should also apply to data transfers. Data exporters would accordingly need to conduct a 'Transfer Impact Assessment'[232] to gauge the *risk* resulting from the transfer at stake rather than the third country's level of protection as such.[233] This subjective approach had however already been put forward, among others in a 2020 white paper by the think-thank Centre for Information Policy Leadership,[234] and was initially not followed by the EDPB in the *draft* Recommendations. *Noyb* (the non-profit organization co-founded by Mr Schrems) commented that the risk-based approach was not enshrined in Chapter V GDPR:

> 'We are […] concerned to see an increasing number of papers and statements suggesting that transfers should be assessed on a case-by-case basis, following a "risk-based approach". [… S]uch an approach is not a general principle applicable to all provisions of the GDPR. Like in many other texts, the EU legislators adapted the obligations and requirement of the GDPR on the basis of the risk for the individuals. This is the case in the following instances: […]
>
> Nothing in Article 46(1) or 46(1)(c) indicates that a transfer may take place when it presents a low risk (risk of interception by a public authority for example), or that it would require a so-called "transfer impact assessment".'[235]

---

[229] Theodore Christakis, '"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)' (European Law Blog, 16 November 2020) <https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/> accessed 23 April 2021

[230] EDPB draft Rec. 01/2020 (n 181) [48, 95]; EDPB Rec. 01/2020 Version 2.0 (n 184) [53, 101]

[231] See Gabriel Maldoff, 'White Paper – The Risk-Based Approach in the GDPR: Interpretation and Implications' (*IAPP*, March 2016) <https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/> accessed 14 March 2021

[232] See Cumbley, Van Overstraeten and Kon (n 174)

[233] See European Broadcasting Union, 'International data transfers need a flexible and risk-based approach' (17 December 2020) <https://www.ebu.ch/news/2020/12/international-data-transfers-need-a-flexible-and-risk-based-approach> accessed 26 April 2021; See also Odia Kagan, 'Businesses Urge EU to Take Risk-Based Approach to Data Transfers' (*Foxrothschild*, 27 January 2021) <https://www.foxrothschild.com/publications/businesses-urge-eu-to-take-risk-based-approach-to-data-transfers/> accessed 28 April 2020

[234] Centre for Information Policy Leadership, 'A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision' (September 2020) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf>

[235] '*noyb*'s comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679' 3 (*noyb*, December 2020) <https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf> accessed 24 April 2020

The tension between a risk-based and 'right-based' approach is not new and was analysed by Gellert, among others.[236] Quelle examined the question of whether a risk-based approach is conceptually incompatible with the protection of fundamental rights and concluded that it was not necessarily the case.[237]

3.4 Second stage: The new SCCs to the rescue?

Among the available transfer tools laid down in Article 46 GDPR, SCCs are by far the most used tool. Even before the *Schrems II* judgement, the IAPP's 2019 Governance Survey concluded that 88% of respondents relied on SCCs, while only 60% were relying (solely or in addition) on the Privacy Shield.[238] Until now, there were two sets of SCCs, one for transfers from a controller to another controller,[239] the other from a controller to a processor.[240]

The new modernised SCCs[241] were adopted in early June 2021 after public feedback.[242] The Commission intentionally waited for the *Schrems II* outcome before issuing the draft, which had been underway for some time.[243] The new SCCs, on which data exporters will henceforth be able to rely, will repeal the former SCCs late-September 2021; Contracts still relying on former clauses at that time will remain valid for a further 12 months.[244]

The new SCCs intend to be modular.[245] They address in one document four different scenarios, namely:

- Controller-to-controller transfers
- Controller-to-processor transfers
- Processor-to-processor transfers
- Processor-to-controller transfers.[246]

While the first two were covered individually by the former SCCs, the latter two had never been covered by any SCCs set before. The new SCCs fulfil the requirements of a processing contract required under Article 28 GDPR; In addition, they allow for multiple parties to adhere or accede to the same set of contractual clauses, thus facilitating the contractual procedures.[247] These changes are likely to be warmly welcomed by companies, especially given the ever-increasing reliance on chains of sub-processors.[248]

---

[236] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)
[237] Claudia Quelle, 'Does the Risk-Based Approach to Data Protection Conflict with the Protection of Fundamental Rights on a Conceptual Level?' [2015] SSRN Electronic Journal <https://www.ssrn.com/abstract=2726073>
[238] IAPP-EY, 'Annual Governance Report 2019' (2019) <https://iapp.org/store/books/a191P000003Qv5xQAC/> accessed 14 April 2021
[239] Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L 181; Amended by Commission Decision 2004/915/EC 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 L 385
[240] Commission Decision 2010/87/EC (n 164)
[241] New SCCs (n 183)
[242] Draft SCCs (n 182); Feedback documents available by visiting the link in (n 182)
[243] See Jetty Tielemans, 'What to expect on revised standard contractual clauses' (*IAPP*, 29 September 2020) <https://iapp.org/news/a/revised-standard-contractual-clauses-what-to-expect/> accessed 6 April 2021
[244] New SCCs (n 183) Recital 24 and Article 4
[245] Ibid Recital 10
[246] Ibid Recital 7
[247] Ibid Article 1(2) and Recital 7
[248] Caitlin Fennessy, 'New EU SCCs: A modernized approach' (*IAPP*, 13 November 2020) <https://iapp.org/news/a/new-eu-standard-contractual-clauses-a-modernized-approach/> accessed 14 April 2021

In essence, the new SCCs include *inter alia* some new duties of information between parties, in particular in the case where a party is, or 'has reasons to believe' that it is, 'unable to comply with the clauses, for whatever reason'.[249] Logically, 'whatever reason' potentially includes – and this makes a first connection with the *Schrems II* ruling – the inability to comply due to a law in the third country and/or due to specific (legally binding) requests from the Authorities of that country.[250] However, the *final* SCCs added the words 'where possible', absent in the *draft* version.[251] New SCCs also noticeably 'require the parties to assist each other in responding to inquiries and requests made by data subjects',[252] which seeks to ensure that data subjects' rights are enforceable.

Recital 19 recalls that data transfers may only take place if the third country law does not prevent the data importer from complying with the SCCs. This is in line with the CJEU's view that, ultimately, the clauses must be enforceable in practice for the transfers to be lawful. In particular, it is stated that all parties shall warrant that 'they have no reason to believe that the laws applicable to the data importer are not in line with these requirements'. Regarding the criteria to conduct the assessment, the *draft* version of Recital 20 provided:

> '[The Parties] should in particular take into account the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data transferred, the type of recipient, the purpose of the processing and *any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred*), the laws of the third country of destination relevant in light of the circumstances of the transfer and any additional safeguards […].'[253]

The highlighted part raised interesting questions. As pointed out by *noyb*[254] as well as Fennessy (Research Director at the International Association of Privacy Professionals),[255] this subjective approach appeared to be incompatible with the *Schrems II* judgement and the *draft* EDPB Recommendations. In their feedback, *noyb* recalled that the *Schrems II* judgement requires an assessment of the practices only once the law assessment is satisfactory:

> 'This wording seems to [be] interpreted by some […] as meaning that even when there are third-country laws that violate the GDPR this can be ignored when these laws were not used , or not used enough by a third country government. In essence this would lead to a "law ***or*** practice" approach where either the law or the subjective practice is compliant with EU law. This approach was pleaded in Schrems II and rejected by the CJEU. The EDPB equally rejected this idea and instead highlighted that organisations should rely on objective factors when assessing the impact of the law ***and*** practices […] on the effectiveness of the safeguards provided in the SCCs. In other words: There needs to be a proportionate law and third countries must follow these laws in practice.'[256]

As per the overall effectivity of a subjective approach, *noyb* further noted that '[i]n practice most representatives of an organisation will […] not know about secret surveillance within their

[249] New SCCs (n 183) Recital 17 and 21
[250] Ibid Recital 21 et 22
[251] In comparison with Draft SCCs (n 182) Recital 21 et 22
[252] New SCCs (n 183) Recital 16
[253] Emphasis added
[254] *Noyb* (n 235) 2ff
[255] Fennessy (n 248)
[256] *Noyb* (n 235) 2; Formatting is identically reproduced; The reference to the EDPB concerns the draft version

own organisation and therefor by definition take the (subjectively correct) view that there is no such surveillance', so that it is 'almost impossible for a supervisory authority and even less any data subjects to know that such access took place in the past and to invoke their rights under the SCCs'. It added that 'subjective approach usually leads to very different results for different data subjects. By definition most access only concerns a small subset of users (e.g. journalists, activists, politicians, […]). In such cases, any assessment that is based on the general population is usually incorrect for the specific data subject.'[257]

Fennessy nuances the criticism by pointing to the EDPB guidelines that mention among others 'the nature of the data' as a criterion to be examined.[258] This thesis does not, however, agree with this observation, because this paragraph lists criteria for assessing the implementation of potential *additional measures* (according to the very wording of Paragraph 49), not for assessing the risk flowing from the level of protection of the third country to which data transfers are contemplated.[259]

In the end, Recital 20 was kept in the adopted version, although the Commission took, in response to the EDPB *draft* Recommendations, a small step backwards by adding the words 'under strict conditions' and requiring the practical experience to be 'documented'.

Beyond this debate, the potential of the new SCCs in addressing the challenges of *Schrems II* remains limited. The new SCCs, by their very contractual nature, suffer from the same limitations as the current ones.[260] Perhaps the obligation of data importers to guarantee that they have no reason to believe that they are subject to surveillance could in some cases make it easier for the data exporter to engage their liability, but this remains to be seen.

It can be concluded on the SCCs that, whilst they may improve, in comparison with the current ones, the operations of privacy professionals and contribute to some extent to the implementation of 'appropriate safeguards' in the meaning of Article 46 GDPR, their impact will remain limited. This is arguably not surprising in view of the substance of the CJEU's case law development. In addition, when the SCCs come into force, they will put much pressure on all data exporters who are using the old SCCs and will have to upgrade them.

3.5 Third stage: The *final* EDPB Recommendations

While the backbone of the EDPB Recommendations – exposed *supra* – subsisted in the adopted version, some key changes were made. The new Paragraph 43.1, related to the assessment of the third country (Step 3) provides:

> '[…] Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the

[257] *Noyb* (n 235) 2
[258] Fennessy (n 248)
[259] See (n 209); For a more insightful illustration see the point 'pseudonymization' under Sub-Section 3.2.2 of this Chapter
[260] The laws of the third country take precedence

same sector and/or related to similar transferred personal data and the additional sources of information described further below.'

By adding this part, the EDPB has in fact embraced the risk-based approach that it initially rejected in its *draft* version while the Commission supported it in the (draft) new SCCs. Both the EDPB and the Commission seem to have taken a step backwards, ultimately leading to a point of convergence that is somewhat in favour of the risk-based approach. It must be concluded that, *according to the EDPB and the Commission*, data exporters can sometimes include subjective elements in their assessment.

3.6 Conclusion: A minefield with few immediate satisfactory solutions

The EDPB has taken strict Recommendations in the wake of the *Schrems II* judgement that do not leave much wiggle room for data exporters. Probably few third countries would be eligible for an essentially equivalent level of protection,[261] and certainly not the US with its current legislation. As recently as April 2021, the US Foreign Intelligence Surveillance Court issued yet another opinion expressing "concern[] about the [FBI's] apparent widespread [Section 702] violations" in domestic matters where US law is supposed to offer more protection than to non-US citizens.[262]

Furthermore, few technical measures are able to compensate for an unsatisfactory level of protection, so that only a small portion of data transfers could be kept lawful with appropriate technical measures, the rest of the usual business activities being prohibited. If followed in practice, the Recommendations would drastically reduce the number of lawful transfers.

The Commission pushed for a more flexible approach focused on the specific (lack of) risks involved in each transfer. The central question at stake was: at what stage should the risk be considered? When the third-country level is assessed and confronted with the EU level (current view of the Commission), or only afterwards in order to assess the effectiveness of additional measures (former stance of the EDPB in the *draft* Recommendations)? In the end, the EDPB has given in and allowed data exporters to adopt a risk-based approach. From a data exporter perspective, this last adjustment will probably be appreciable. However, a sword of Damocles would hang over any data exporter relying on it because of a likely incompatibility with the *Schrems* judgements, so that data exporters would use them at their peril, just as when the Privacy Shield was avoided by companies that did not trust it. Therefore, it would be, ironically enough, quite *risky* for data exporters to adopt the risk-based approach.

At the end of the day, it is certain that the implementation of transfers by data exporters will be highly challenging in the coming years. In particular, small and medium-sized enterprises cannot realistically imagine conducting satisfactory assessments of their partners' third countries. In this respect, *noyb* calls on the Commission to consider a means of centralising information about levels of protection in third countries.[263] Still, even with appropriate documentation available (as is the case with the US since the *Schrems II* assessment), all transfers must be assessed on a case-by-case basis, which represents an extremely heavy burden. Moreover, additional measures are complex to implement, if they are possible at all,

[261] Christakis (n 229)
[262] 'Surveillance Court Finds FBI Repeatedly Misused FISA Program to Conduct Unlawful Surveillance of Americans' (*Epic*, 29 April 2021) <https://epic.org/2021/04/the-foreign-intelligence-surve-1.html> accessed 4 May 2021
[263] *Noyb* (n 235) 3

and large companies or institutions are no exception. For example, and ironically, there is an ongoing EDPS investigation of the European Parliament's website following a complaint about allegedly illegal transfers to the US.[264] Three weeks later, the EDPS issued a statement where it 'strongly encourages [European Institutions] to avoid transfers of personal data towards the United States for new processing operations or new contracts with service providers.'[265] Incidentally, the EDPB also issued on 20 April 2021 a statement calling on the Member States to reassess their international agreements, including transfers,[266] heralding a huge task of analysis and renegotiation in public institutions as well.

In practice, it is likely that many data exporters will work towards implementing additional measures and new SCCs, reducing transfers and the amount of data involved, *etc*. in order to show compliance efforts, without stopping transfers that do not reach the level required by the EDPB Recommendations.

To conclude, there is every reason to believe that most of the current data transfers should cease, leading the EU to retreat to a kind of data protectionism – but also that such rigidity is realistically not going to be followed.[267] However, more nuanced paths are available from a regulatory point of view.

[264] See <https://noyb.eu/sites/default/files/2021-01/NOYB%20COMPLAINT%20C035_Redacted.pdf> accessed 6 May 2021

[265] European Data Protection Supervisory, 'The EDPS opens two investigations following the "Schrems II" Judgement' (27 May 2021) <https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en>

[266] European Data Protection Board, 'Statement 04/2021 on international agreements including transfers' (13 April 2021) <https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-042021-international-agreements-including_en>

[267] See for more insights: 'Companies can't say how they comply with CJEU ruling' (*noyb*, 25 September 2020) <https://noyb.eu/en/companies-cant-say-how-they-comply-cjeu-ruling> accessed 25 December 2020; See also Hengesbaugh (n 32)

Chapter 4 – How to enforce the European Union's level of protection: a focus on GAFAM and US superproviders

"If asked how to cope with a great host of the enemy in orderly array and on the point of marching to the attack, I should say: 'Begin by seizing something which your opponent holds dear; then he will be amenable to your will.'"

"Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."

Sun Tzu [268]

4.1. Introduction

The finding that most data transfers are carried out in breach of the GDPR raises the key question: How can the EU enforce Chapter V GDPR and thereby ensure the European level of protection?

In practice, taking all-out enforcement action against each and every company that transfers data to the US would be unrealistic and certainly have its fair share of unwanted effects. As long as the EU does not get the US to change its legislation and intelligence agency practices (an overarching goal that does not seem to be yet on the US agenda), there will be no 'one size fits all' solution.

Nevertheless, the latter statement does not prevent EU institutions and DPAs to actively pursue compliance, quite the contrary. As in every regulatory ambition, EU institutions and (national) authorities can move away from a binary approach of legal prosecution followed by conviction to a more comprehensive approach. They have at their disposal multiple ways of action that, taken together and not in isolation, can improve compliance with data transfer rules. In particular, they can strategically choose which enforcement actions are first carried out, against whom, and in what ways, taking into account the interests of the different stakeholders and the (diplomatic) power relations involved (Section 4.2).

This thesis argues that the EU's enforcement strategy should first focus on GAFAM and major US-based multinationals that decide to require data transfers in the first place. Such multinationals can avoid or limit transfers, or take the technical measures to make them compliant, and are therefore best placed to (strongly contribute to) solve the alleged current impasse regarding data transfers to the US. They also represent a valuable part of the US economy, and therefore a vector of pressure on the latter. **These US-based multinationals, whether they provide services to consumers or to businesses, will be referred to as *US superproviders* in this chapter. This generic term, when used in the singular, will refer to all the entities (whether US or EU) of such a multinational as a whole.**

[268] See (n 39)

Section 4.3 will be entirely focused on US superproviders and propose a shift of enforcement against them. It will assess to what extent the GDPR is applicable to US superproviders, which set of rules apply to them, and what are consequently the means of action available to DPAs, individuals, and organisations that engage in strategic litigation.

Section 4.4 will close this chapter with a look at the recent follow-up to the *Schrems* procedure, and will highlight some current inefficiencies in the enforcement mechanisms of the GDPR which lie at the intersection between the sourcing of DPAs, the one-stop-shop mechanism, as well as the coordination and consistency of fines.

The next concluding chapter will take stock of these findings and initiate discussion on potential future avenues.

4.2. A look at strategies for regulating technologies

Regulators have multiple ways at their disposal to achieve a certain aim. Proper and efficient regulation of technology in general and privacy in particular often requires more than the enaction of a law (e.g. GDPR) and the enforcement of the rules towards all non-compliant actors (e.g. by DPAs).

According to Raab and de Hert,[269] '[…] states do more than just enact laws. Their toolbox is considerably better stocked, and there are few limits to the combinations of regulatory tools that are possible in theory, and very often in practice, in spite of political, economic, legal, ethical and other limitations'.[270] The authors argue for a 'polytechnic or hybrid approach'[271] to regulation involving not only laws,[272] but also technological solutions,[273] adoption of standards, non-coercive processes and a degree of shift from government to governance. While States (and, it should be added, supranational institutions) play a crucial role in encouraging but also shaping privacy instruments, it is pointed out in the article that 'States do not have a monopoly of the means of detecting and effecting; in societies with plural centres of power and a private sector, we easily see that these means are widely dispersed'.[274] To sum up, 'it is not only the state and its agencies that are involved in regulatory governance'.[275]

As regards EU data protection law, the EU legislator has involved many actors in the compliance and enforcement scheme. For example, the legislator has deliberately chosen to grant the *private sector* with the ability to influence data protection compliance by providing mechanisms for the drawing up of Code of Conducts (Article 40 GDPR). Furthermore, the GDPR ensures that *data subjects* can easily lodge a complaint with DPAs (Article 77) and gives the possibility for *not-for-profit organisations* to represent data subjects as well as, depending on the Member States law,[276] to act independently (Article 80). By doing so, the concerns of individuals and civil society become in themselves a means of enforcing the GDPR at a broader level. This is well illustrated with Mr Schrems who is undoubtedly changing the EU data

[269] Charles D Raab and Paul De Hert, 'The Regulation of Technology: Policy Tools and Policy Actors' [2007] SSRN Electronic Journal <http://www.ssrn.com/abstract=1030263> accessed 5 May 2021
[270] Ibid 21
[271] Ibid 3
[272] A regulation scheme too focused on law would result in a 'static 'command and control' regulatory model'; See (n 280)
[273] In particular, the paper mentions Privacy-Enhancing Technologies (PETs)
[274] Raab and De Hert (n 269) 17-18
[275] Ibid
[276] This is for instance the case in Belgium; See 'noyb approved as a "qualified entity" to file class actions in courts in Belgium' (*noyb*, 29 octobre 2020) <https://noyb.eu/en/noyb-approved-qualified-entity-file-class-actions-courts-belgium> accessed 5 April 2021

protection landscape through his relentless judicial actions since 2013. The not-for-profit organisation *noyb* has, since it was cofounded by Mr Schrems, lodged multiple other complaints[277] and issued several initiatives and propositions with regard to EU data protection regulation. For instance, since mid-June 2021, *noyb* has been promoting the 'Advanced Data Protection Control', a privacy-enhancing technology aimed at achieving real, genuine and not-annoyingly-requested consent regarding cookies banners.[278] Finally, and as already covered, the GDPR enables *DPAs* to investigate and take enforcement measures *ex post* (Article 58(1) and (2)), and to adopt guidelines and recommendations to promote compliance *ex ante* (Article 58(3)). It also enables DPAs (as well as public or private *certification bodies* approved under specific criteria) to issue certifications to controllers or processors about specific processing operations such as data transfers (Articles 42 and 43). A common certification, referred to as the European Data Protection Seal, may be achieved in the future under approbation of underlying criteria by the *EDPB*, which oversees and coordinates the DPAs.[279]

In summary, the private sector, as well as data subjects and not-for-profit organisations through strategic litigation, complaints and awareness-raising, play a crucial role in day-to-day privacy governance, in addition to the work of the many independent DPAs across the Union and their coordination by the EDPB. This interweaving of actors creates a comprehensive regulatory system, rather than a limited 'static 'command and control' regulatory model'.[280]

That being said, Raab and de Hert acknowledge that a situation 'gains immeasurably in complexity' when involving multiple actors and mechanisms in the regulation scheme.[281] This can give a confusing picture of where and how enforcement should be initiated regarding specific issues, such as data transfers. In order to develop a regulation strategy, the authors call for a close examination of all the actors in the field to reveal a 'political system with distribution of power'.[282] They purport that 'only by carefully mapping the actors and their interactions can we more completely understand the effects of the different regulatory instruments that are used in each field of application'.[283]

Following this approach, the next Section will map the actors and contractual relationships that take place when data is transferred to the US; whereas this mapping will be non-exhaustive and simplified, it will enable an analysis of the applicability of the GDPR as well as the proposal for a requalification of the entities at stake. This will sketch a tiered enforcement strategy, which could, ultimately, have an impact on diplomatic negotiations with the US.

---

[277] See, for an example among others: 'noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints' (*noyb*, 31 May 2021) <https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints> accessed 5 June 2021

[278] 'New browser signal could make cookie banners obsolete' (*noyb*, 14 June 2021) <https://noyb.eu/en/new-browser-signal-could-make-cookie-banners-obsolete> accessed 14 June 2021; See also the Advanced Data Protection Control website <https://www.dataprotectioncontrol.org/>

[279] See the EDPB's document on the European Data Protection Seal, updated after the *Schrems II* judgement: European Data Protection Board, 'EDPB Document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal' (28 January 2021) <https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en>

[280] Raab and De Hert (n 269) 11, referring to: Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (1st ed, Routledge-Cavendish 2006).

[281] Raab and De Hert (n 269) 17

[282] Ibid 6ff; As a side comment, this last element fits into the reading grid that is proposed in this paper by structuring it in the form of chapters with different perspectives, illustrated by quotations from Sun-Tzu, see (n 39)

[283] Raab and De Hert (n 269) 7

4.3. Taking targeted enforcement actions against, and gaining compliance from, superproviders

This whole section will focus on the applicability of the GDPR towards US superproviders, and whether and on which grounds enforcement actions can be taken against them.

More precisely, the starting point will be to map their legal entities and their relationships with data subjects and other EU companies (Sub-section 4.3.1). Then, the applicability of the GDPR,[284] the legal role of US superproviders under GDPR as well as the means of action available against them will be identified; the analysis will be broken down into two parts, namely the Business-to-Consumer (B2C) context (Sub-section 4.3.2) and the Business-to-Business (B2B) context (Sub-section 4.3.3). While the former will involve some analysis of the territorial scope of the GDPR, the latter will require, in addition, a closer look at the actual qualification of the superproviders and the need to requalify them.

4.3.1 Mapping of relationships between US superproviders, data subjects and EU companies

Data processing, and in particular data transfers, can take place in very different legal situations. Facebook is a straightforward example of a US superprovider that deliberately chooses to transfer, to the US, the data that it collects directly from individuals in a B2C context. Besides this, many data transfers are resulting from a B2B relationship between a US superprovider and an EU company, without the individuals related to the data being aware of it. In fact, if one takes a closer look at the data transfers carried out by European companies, one realizes that such transfers are often imposed on European companies as part of a complete service package rather than being the result of a specific choice. This is due to the fact that, as already mentioned, companies are now heavily relying on "ready-to-use" services such as SaaS, PaaS and IaaS (Software, Platform, and Software as a Service),[285] for which they have relatively little negotiating power.[286] In both contexts, US superproviders are in a strong position to impose their *modus operandi* on consumers and other companies.

Figure 1 represents the different successions of intermediaries through which personal data can – somewhat abstractly – pass before being transferred to the US. The different legal situations that arise from each of the possibilities (represented by numbers ① and ② for the B2C context, and ③ and ④ for the B2B context) will be analysed.

[284] Notably in light of: European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation' (12 November 2019) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en>

[285] See for more insights on those terms: European Data Protection Board, 'Opinion 16/2021on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe' (19 May 2021) [6] <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_nl>; See also Netskope INC (n 5)

[286] See Netskope INC (n 5) and Millard (n 5)

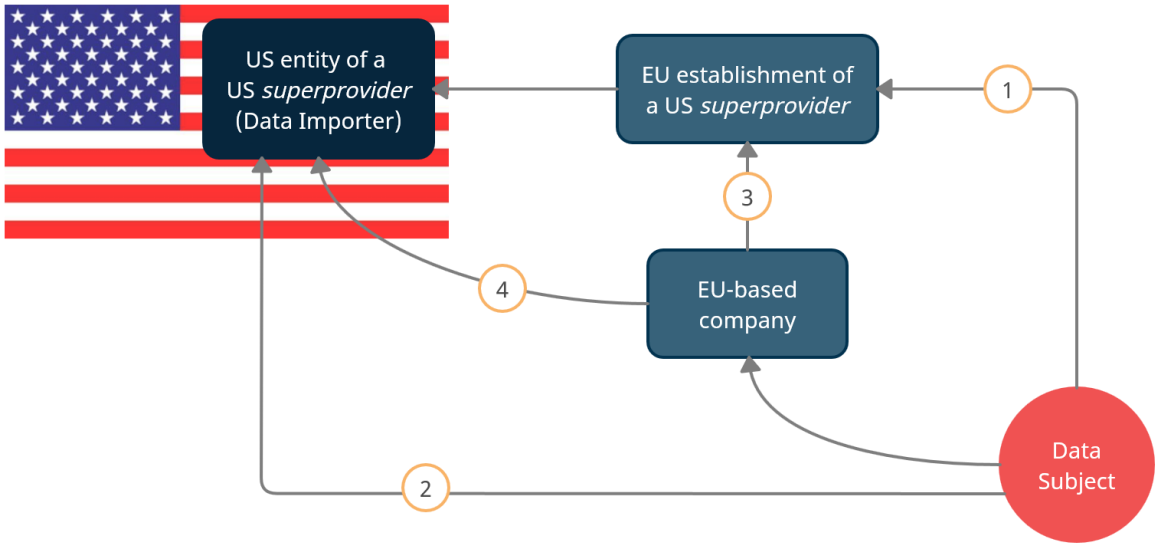

FIGURE 1: MAPPING OF LEGAL ENTITIES POTENTIALLY INVOLVED IN B2C (1, 2) AND B2B (3, 4) TRANSFERS [287]

In this figure, data originates from the data subject on the bottom right and follows one of the arrows. All rectangles represent a company established, in the meaning of the GDPR, in the Union,[288] with the exception of the US entity of the US superprovider (the data importer) represented on the US flag.

The term '*EU establishment of a US superprovider*' means, for the purpose of this paper, an entity established in the EU which is mainly controlled by a superprovider based in the US. This 'control' criterion is important because, under the US CLOUD Act, US LEAs can compel companies established in the US to provide access to data over which they have 'possession, custody or control', so that LEAs can require US superproviders to disclose data even if they are stored and processed by subsidiaries in the EU.[289] The CLOUD ACT and its extensive extraterritorial scope came into existence right after the US government sued Microsoft[290] to access data from its facility in Ireland.[291]

Conversely, the term '*EU-based company*' means an EU controller established in the EU and not (mainly) owned by a foreign entity.

4.3.2 B2C context analysis: Consumer using the services of a US superprovider

This Sub-section examines the applicability of the GDPR and the feasibility of enforcement actions towards US superproviders when they provide services *directly* to data subjects.

---

[287] This illustration was created by Janvier Parewyck and is licensed under CC BY 4.0. You can share and adapt it if you give credit to the author. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

[288] Article 3(1) GDPR; See in particular Recital 22 GDPR

[289] See Chapter 1, Section 1.1 of this paper, in particular CLOUD ACT (n 14), United States v. Microsoft Corp (n 15), and Blair and Lawler (n 16)

[290] United States v. Microsoft Corp (n 15)

[291] See Jennifer Daskal, 'Microsoft Ireland, CLOUD Act, and International Law-Making 2.0' (2018) 71 STAN.L.REV.ONLINE9 <https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/> accessed 10 June 2021

In situation ①, data are collected by the establishment of a US superprovider in the EU. This EU establishment determines the purposes and the means of processing and therefore qualify as the data controller.[292]

This is the exact situation surrounding the *Schrems* complaint. Mr Schrems is a data subject who is using a service (the Facebook website and apps) provided to him by Facebook Ireland.[293] The data is then transferred from the Facebook entity established[294] in Ireland to Facebook INC in the US. Facebook Ireland is unambiguously a data controller, which is therefore responsible to demonstrate compliance with (chapter V of) the GDPR, while Facebook INC is the US data importer. The applicability of the GDPR towards Facebook Ireland is not disputed since, according to its Article 3(1), GDPR applies 'to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union or not*'.[295] Because the data controller is established in Ireland, the Irish DPA (the DPC) is the lead supervisory authority competent to handle the complaint, as per the *one-stop-shops mechanism* of Article 56 GDPR that will be further analysed later.[296]

In such a scenario, the data subject concerned by the data transfers or the further processing of their data in the US can act against the data controller – i.e. the EU establishment – through the competent DPA, as Mr Schrems did. If the DPA grants the request, then it has, as already seen in the *Schrems* judgements analysis, the duty to prohibit the data transfers in dispute but also to prohibit the data controller from exporting any data, since DPAs have the mission to monitor and enforce the GDPR under Article 51 and 57(1)(a).[297] A DPA can also take the initiative to start investigation and enforcement actions on its own, without waiting for a complaint.[298]

Yet, data transfers to Facebook INC are still ongoing at the time of writing of this thesis although Mr Schrems' complaint was initiated in 2013. Barriers to efficiency (in particular related to the *one-stop-shop mechanism*) as well as recent developments will be discussed further in Sub-section 4.4.

Situation ② is an alternative scenario occurring in the B2C context where the US superproviders does not have any establishment in the EU. While large service providers usually have various establishments in different regions of the world including the EU, it may not be the case (yet). In this event, the data are not collected from the data subject by an EU establishment, but directly by the US entity of the US superprovider. The legal entity contracting with the consumer is the US entity. Hence, the question arises whether the GDPR is applicable to that foreign entity.

Article 3(2) extends the GDPR's territorial scope to a controller or processor not established in the Union if it processes 'personal data of data subjects who are in the Union' in relation with either '(a) the offering of good or services […] to such data subject in the Union' or '(b) the monitoring of their behaviour as far as their behaviour takes place within the Union'.

---

[292] As per the definition of data controller, Article 4(7) GDPR
[293] Facebook Ireland is the legal entity mentioned in the Facebook's Terms and Conditions, see <https://www.facebook.com/about/privacy> accessed 9 April 2021
[294] In accordance with the definition of establishment in Article 4(16) GDPR
[295] Emphasis added
[296] Chapter 4, Sub-section 4.4.2 of this paper
[297] As confirmed by the Court in the *Schrems II* judgement (n 1) [107]
[298] Article 58(1) GDPR

The EDPB published guidelines on how to interpret these provisions and dealt with what it calls the 'targeting criterion'.[299] With regard to provision (b), a straightforward example given by the EDPB is the monitoring, by an app developer established in Canada, of the localisation of data subjects within the Union.[300] Regarding provision (a), Recital 23 GDPR provides guidance on how to determine whether goods or services are offered to a data subject in the Union. The criteria referred to appear to be strongly inspired from the 2010 *Pammer Alpenhof* judgment[301] interpreting whether products and services were 'geared towards' consumers in the sense of the 'Brussels I' Regulation.[302] The 2016 Amazon ruling[303] confirmed the applicability of these criteria to the DPD and, *a fortiori*, to the GDPR. While the mere accessibility to a website is not sufficient to establish that a processor or controller is directing its services towards data subjects in the EU, several factors may hint so, for instance the translation of the website in other languages,[304] the use of a certain currency[305] or the booking of a keyword intended to display advertising in specific regions.[306]

Consequently, US superproviders operating internationally and offering services to individuals within the Union and/or monitoring the behaviour of such individuals will fall within the extraterritorial scope of application of the GDPR. Therefore, if Facebook were hypothetically to dissolve its establishment in Ireland and offer its consumer services exclusively from Facebook INC, it would nonetheless remain subject to the GDPR under Article 3(2)(a) because there is no doubt that it offers products and services to data subjects in the Union, as well as under Article 3(2)(b) because it monitors behaviours of Internet users.

In addition, Article 27 GDPR requires foreign entities not having an establishment in the EU but falling under Article 3(2) to appoint a representative[307] within the Union, notably to facilitate enforcement actions. In a recently issued decision, the Dutch DPA held[308] that a website supposedly run by a Canadian entity and revealing 'the full addresses and sometimes also the telephone numbers of people who are unaware of how their details came to appear there' was offering goods and services to data subjects in the Union and was therefore subject to the GDPR and its Article 27.[309] The applicability analysis in the decision is unfortunately very succinct and does not make it clear which factors were actually taken into account to determine the 'direction of activity', but what is sure is that Article 3(2) GDPR, already broad in itself, will probably regularly be further widened, so that DPAs will also have jurisdiction

[299] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2 September 2020) <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en>
[300] Ibid [20]
[301] Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECLI:EU:C:2010:740
[302] 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 L 12
[303] Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612
[304] Recital 23 GDPR
[305] Ibid
[306] *Pammer Alpenhof* judgment (n 301) [81]
[307] As defined in Article 4(17) GDPR
[308] Dutch DPA (Autoriteit persoonsgegevens), 'Dutch DPA imposes fine of €525,000 on Locatefamily.com' (12 May 2021) <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-imposes-fine-%E2%82%AC525000-locatefamilycom> accessed 15 May 2021; For the complete decision in Dutch, refer to: <https://www.linkedin.com/feed/update/urn:li:activity:6798175539480821760/?updateEntityUrn=urn%3Ali%3Afs_feedUpdate%3A%28V2%2Curn%3Ali%3Aactivity%3A6798175539480821760%29> accessed 1 June 2021
[309] The foreign entity had to appoint a representative under Article 27 GDPR and was fined for not doing so.

over foreign entities. The Dutch DPA claims to have worked with nine other DPAs and the Office of the Privacy Commissioner of Canada, which suggests that the effectiveness of the decision may be achieved. In fact, this tends to show that international cooperation may enable DPAs to enforce the GDPR on foreign entities. This matter would merit a separate further analysis that will not be conducted here.

4.3.3 B2B context analysis: EU-based controller using services of a US superprovider

A significant part of small, medium and large EU-based companies relies on Cloud services offered by US superproviders such as Microsoft Azure, Amazon AWS, Google Cloud and CloudFlare hosting.[310] Regardless of enforcement actions that can be taken against the EU-based companies relying on such services, this Sub-section concentrates on the ability to take measures against US superproviders.

While the contractual nature of the procurement of such services depends on the case, the contracting entity of the US superprovider is often qualified as a processor by the parties (or, more likely, by the US superprovider itself since small and medium companies often have no power of negotiation).[311] A processing agreement is therefore, as required by Article 28 GDPR, concluded between the EU-based company (for the sake of simplicity, it is assumed in this paper that this is a controller) and the relevant entity of the US superprovider.

One could assume that, when an EU-based company is using a service offered by a US superprovider that *has* an establishment in the EU, this EU-based company is contracting with that EU establishment of the US superprovider (situation ③). This can indeed be the case when, for instance, an EU-based company uses Facebook services: Facebook Ireland has usually the role of a processor of the EU-based company and, in turn, transfers data to its headquarters in the US.[312] The Facebook terms state that the EU-based company 'instruct[s] Facebook Ireland Limited to transfer EU Data to Facebook Inc. in the US for storage and further Processing'.[313]

On top of that, the matter can get blurrier (situation ④). When an EU-based company uses, for instance, Google or Amazon's services, they have a contractual relationship with, respectively, the Google establishment in Ireland[314] or the Amazon establishment in Luxembourg,[315] **except** with regard to data transfers related to some services for which they are required to enter directly into the 'Model Contract Clauses' with Google LLC in the US[316], or into the Amazon 'GDPR Data Processing Addendum'.[317] As a result, the EU-based company is, at least fictionally, the sole data exporter, while the EU establishment seems completely absent from the contractual relationship with regard to data transfers, so that enforcement against the US superprovider seems, at first glance, even less feasible. Nevertheless, it is usually still the US superprovider that decided to transfer data to the US, not the EU-based data controller.

---

[310] See for insights: Kinsta, 'Azure Market Share: Revenue, Growth & Competition (2021)' <https://kinsta.com/azure-market-share/> accessed 10 June 2021; See also Netskope INC (n 5) and Millard (n 5)
[311] See Netskope INC (n 5) and Millard (n 5)
[312] See <https://www.facebook.com/legal/EU_data_transfer_addendum> accessed 5 May 2021
[313] Ibid
[314] See <https://cloud.google.com/terms/google-entity> accessed 5 May 2021
[315] See <https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-French_2020-11-30.pdf> accessed 5 May 2021 17
[316] See <https://cloud.google.com/terms/data-processing-terms#10.-data-transfers> accessed 5 May 2021
[317] See <https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf > (page 9) accessed 5 May 2021

The first question arising in each situation is, again, whether the GDPR applies towards US superproviders' entities involved (bullet *a*). The second question concerns their respective role under the GDPR as well as the rules that apply to each of them, and therefore requires an evaluation of the fictional relationship between the EU-based company and the entity(ies) of the US superprovider (bullet *b*). A requalification will then be argued to enable further liability and enforcement actions (bullet *c*). Some longer-term consequences will then be considered (bullet *d*).

a. Extraterritorial applicability of the GDPR

In situation ③, the EU establishment is clearly referred to as the entity conducting the data transfer to the US. There is, therefore, no doubt that the GDPR is applicable towards this establishment under Article 3(1) GDPR. In situation ④, where the data is (fictionally) transferred from the EU-based company directly to the US entity of the US superprovider, DPAs and Courts would first have to establish their jurisdiction towards the US importer or its establishment in the EU. Two possibilities can be contemplated:

(i) Relying on Article 3(1) GDPR, according to which the GDPR applies 'to the processing of personal data *in the context* of the activities of an establishment […] in the Union',[318] in order to take enforcement measures against the EU establishment of the US superprovider (if any), even though this establishment is *not* the data exporter *in the contract*.
In the light of the CJEU case law, the said context is to be interpreted broadly: in the 2014 Google Spain ruling,[319] it was sufficient to find that Google Spain was responsible for the billing of the services offered by Google INC to conclude that the activities of Google INC were carried out 'in the context' of the activities of Google Spain, and that therefore the Court had jurisdiction against Google Spain with regard to the activities of Google INC. Therefore, the fact that, for instance, Google Ireland is the main contracting party in the Terms and Conditions mentioned *supra*[320] should bring this entity under the Court's jurisdiction with respect to the data transfers operated by Google LLC.[321]

(ii) Triggering the applicability of the extraterritorial scope of the GDPR in order to take enforcement actions against the US entity of the US superprovider, in its role of the company offering services and/or monitoring behaviour under Article 3(2) GDPR. However, while it raises not doubt that Google LLC is 'offering services' to data subjects in the Union, the services at stake in a B2B relationship may be considered as offered to EU-based companies, not directly to the data subject. As a consequence, this Article may not be applicable. Similarly, it is not clear whether US entities providing online tracking technologies for advertising purposes to other EU-based companies fall under provision (b) of Article 3(2) if they do not monitor themselves the behaviour of data subjects.
Yet, such interpretations rely on the assumption that the US entity is passive vis-

[318] Emphasis added
[319] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317
[320] (n 316)
[321] Google LLC is the successor in law of Google INC. For the record, see: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CC0507>

à-vis the data subject, a relationship existing only between the EU-based company (the controller) and the US entity of the US superprovider (the processor). If the latter is requalified as a (joint) controller, as it will be supported below, then it could be acknowledged that since the US entity decides on some purposes and means of the processing, it should be considered as offering services to / monitoring data subjects. Nevertheless, solution *(i)* appears to be more promising and relevant in the context of US superproviders.

To sum up, the GDPR generally allows for enforcement actions against an EU establishment of the US superprovider, and may potentially extend to the US entity of said superprovider. That being said, another obstacle stands in the way of efficient enforcement: The qualification of the entity(ies) of the superprovider as a processor.

b. The qualification of the US superprovider as a processor and the impact on its duties and liability

A US superprovider's entity qualified as a processor is theoretically required to comply with Chapter V GDPR, since this Chapter especially refers to processors in addition to controllers. However, when looking at situation ③, enforcement against Facebook Ireland in its role of processor would be much less straightforward than enforcement against Facebook Ireland in its role of data controller (as it was in situation ①). The difficulty comes from the fiction that Facebook was 'instructed' by the EU-based company to transfer data, which is rarely true. Under this fiction, data are deemed to have been transferred to the US at the EU-based controller's request, whereas the EU establishment of the US superprovider can claim to be not responsible because it is deemed to have passively processed the data. This observation holds in situation ④: the US entity is acting on behalf of the EU-based company and is deemed not to carry out any processing for which it determines the purposes and means.

On the liability of processors, Article 82(2) GDPR states that 'a processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or when it has acted outside or contrary to lawful instructions of the controller'. Is that to deduce that processors may be held liable when transferring data in circumstances where the data controller who commissioned them does not rely on a proper legal basis for transfers? This could be argued but, again, would certainly lead to a lot of discussions since it seems inconsistent with the central idea that a processor is acting on behalf of its controller and does not decide on the data transfer mechanism.

For those reasons, and regardless of the situation at hand, enforcement by DPAs against a US superprovider (either the parent entity in the US or the establishment in the EU) seems in practice far less practicable than against an EU-based company – unless a requalification is operated.

c. The necessary requalification

The paradoxical impunity in situations ③ and ④ is inherently related to the qualification of the US superprovider as a mere processor and, more fundamentally, to the somewhat vague and artificial distinction between the notions of controller and processor. Terstegge argues that this fictional separation does not reflect the interplay between private economic actors in practice:

> ‘With the introduction of cloud computing, the artificial distinction between data controller and data processor was already questioned. However, the GDPR still makes that distinction for no specific reason. Professional service providers, who now technically qualify as processors […] are more often than not taking far-reaching decisions with respect to the personal data they process. Not only how the data is processed, but also where and by whom the data is processed. And they increasingly also advise - or as part of their services even determine - which personal data are processed [… .S]ervice providers often have a huge impact on the processing and protection of the personal data. Business models have become very complex, and often involve a number of parties that operate in data processing chains. It is only logical to make a service provider more accountable for the way he processes the data than only the 10 GDPR obligations that now apply to data processors […]’[322]

Terstegge proposes amending the GDPR to avoid overlapping liability, and ‘mak[ing] clear that the principle of accountability does not exceed a contracting party's administrative sphere of influence. [… T]he client [… that] did a proper due diligence on the service provider, […] should never be liable for the mistakes of the service provider, nor should he be risking a fine for violating the principle of accountability. If every party is only responsible and liable for its own actions and its own compliance, that would make doing business so much easier’.[323] By allocating clearer and sometimes narrower liability to each of the actors, it might indeed (perhaps counter-intuitively) be more difficult for major providers to escape liability. However, if such a change were to occur, it would in any case not be any time soon.

It would be possible, without amending GDPR, to extend the accountability of US superproviders by requalifying them as joint controllers. According to Article 26 GDPR, ‘[w]here two or more controllers jointly determine the purpose and means of processing, they shall be joint controllers’. In the case of joint controllership, the joint controllers are jointly accountable, so that enforcement actions regarding a processing activity can be conducted against any of them. Indeed, each joint controller is liable, towards the data subject, for the *entire* damage caused by ‘the same processing’ which infringed the RGPD (Article 82(4)). The joint controller which paid full compensation is, in a second stage, entitled to claim back the part of the compensation corresponding to the part of the responsibility of the other joint controller (Article 82(5)).

A broad interpretation of the concept of joint controllership was historically adopted and advocated in 2006 by the Article 29 Working Party in the SWIFT opinion[324] in order to ensure the most efficient protection of data subjects’ rights.[325] In 2020, the EDPB developed a more detailed and nuanced analysis in its guidelines on the concepts of controller and processor.[326] According to the EDPB, ‘[j]oint participation can take the form of a *common decision* taken by two or more entities or result from *converging decisions* by two or more entities, where the decisions complement each other and are necessary for the processing to

---

[322] Jeroen Terstegge, ‘Do we need a new GDPR?’ (*Netkwesties*, 4 February 2020) <https://www.netkwesties.nl/1421/do-we-need-a-new-gdpr.htm?u%E2%80%A69-feb-2020&utm_medium=e-mail&utm_term=do-we-need-a-new-gdpr> accessed 22 May 2021

[323] Ibid

[324] Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’ WP 128 (22 November 2006) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf>

[325] European Union Agency for Fundamental Rights (FRA) (n 38) 107 and 109

[326] EDPB Guidelines 07/2020 (n 299)

take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing'.[327] More precisely, the EDPB states that '[d]ecisions on the purpose of the processing are clearly always for the controller to make',[328] while decisions on the means are often 'left to the discretion of the processor'.[329] Still, it acknowledges that certain decisions on the means can be inherent to the status of controller. While a processor acting under the instruction of a controller may have some leeway when it comes to deciding on 'non-essential' means,[330] '[e]ssential means are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller'.[331] It follows that a processor co-deciding on essential means should be considered as a (joint) controller. Quite interestingly, the EDPB classifies under the category of essential means the determination of 'the categories of recipients'.[332]

In the situations discussed above, whilst the EU-based company decides on its own to share its data with the US superprovider, the latter decides on some means, i.e. how and which sub-processing activities are conducted, and in particular to transfer the data to the US. Given the sensitive nature of data transfers and its relationship to the determination of recipients, this thesis strongly supports that the technical decision to conduct data transfers should be considered as a common decision on *essential* means, so that it would be coherent to requalify the US superprovider as a joint controller regarding this decision. Such requalification would be entirely consistent with the concept of controllership developed by the EDPB, according to which 'a controller is a body that decides certain key elements about the processing',[333] 'by virtue of an exercise of decision-making power'.[334] The qualification in the contract should not be sufficient to prevent it since, according to the EDPB '[t]he assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties'.[335]

It must however be acknowledged that a quasi-automatic reclassification of all processing activities as 'jointly controlled' as soon as entities have taken a common decision would create considerable legal uncertainty. In this respect, the CJEU seems to have struck a reasonable balance in the recent *Fashion ID* case.[336] On the one hand, the Court qualified Facebook as joint controller together with Fashion ID with regard to Facebook 'like' buttons installed, *by Fashion ID*, as a feature on its website and further used, *by Facebook*, to track the visitor across websites. On the other hand, the Court held that each joint controller was only *liable* for their respective activities for which it determined the purposes and means. It appears from a careful reading that the Court decision amounts to interpreting Article 82 GDPR (formerly Article 23 DPD) in such a way that the 'same processing activity' referred to in it must be closely, and not broadly, scrutinised. To be liable, the entity must have decided (how) to engage in a specific processing, or, in other words, it must be (one of) the controller(s) of

[327] Ibid 3; Formatting is identically reproduced
[328] Ibid [37]
[329] Ibid [37-39]
[330] Ibid [38-39]
[331] Ibid [38]
[332] Ibid
[333] Ibid [19]
[334] Ibid
[335] Ibid [20]
[336] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629

that specific (sub)activity. According to de Hert, this enshrines '*decisional controllership*, clearly distinguishable from *abstract controllership*'.[337] He concludes that the overall ruling constitutes a fair balance, in which the joint controllership qualification is 'a necessary evil, satisfactorily compensated by the limitation […] of [the joint controller]'s liability to the processing operations that it actually determines'.

Treating data transfers as a joint decision – while attributing the other processing activities to their respective controller and therefore limiting the joint liability of each party to the decision they actually co-determine – would considerably increase the ability for DPAs to act (upon complaint or on their own) against US superproviders imposing the data transfers, without creating too much legal uncertainty for companies.[338] To conclude on the requalification, it is supported in this paper that DPAs along with the EDPB (through their Guidelines and decisions) and the (inter)national Courts (through their rulings), could and should actively requalify the legal nature of the US superproviders as (joint) controllers. This shift in focus would finally allow real compliance in the sense of Kuner's analysis,[339] whereas at this stage many EU-based companies find themselves spending a lot of resources trying to comply with the GDPR and the *Schrems II* ruling more on form than substance.[340]

d. Going further: Longer-term consequences of such requalification

Although in theory the accountability principle of the GDPR also applies (in part) to processors, the qualification of 'processor' has led so far, and as demonstrated, to an artificial disaccountability of US superproviders in practice. The requalification of processors as joint controllers not only allows DPAs to carry out enforcement actions *ex post* on a punctual basis, but also and mainly makes superproviders more responsible and accountable *ex ante*.

Regarding data transfers, Mr Schrems pointed out in the EU Parliament's debate on data transfers of 3rd September 2020 that 'US multinationals […] do have a lot of options to change the [state of play] because they can actually split some of their processing operations and make it actually happen in Europe without direct access from the US. A lot of processing already happens in Europe because of latency, because of a lot of technical issues,… Most of these companies have the infrastructure in Europe, it is just still connected to the US in a way that possibly the US can still reach in'.[341] US superproviders could therefore (develop and) take beforehand technical[342] and organisational measures to limit transfers or render them compliant. DPAs are not required to impose fines right away. They may first investigate and ask what

[337] Paul de Hert and Georgios Bouchagiar, 'Fashion ID on decisive influence over the processing. A fair approach to single and joint controllership' (to be published) European Data Protection Law Review
[338] Since the EU-based controller would remain exclusive controller for all the other activities it solely determines
[339] Kuner (n 26)
[340] Ibid
[341] Hearing of the European Parliament of 3 September 2020 (13:45 - 15:45), 'Committee on Civil Liberties, Justice and Home Affairs' <https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20200903-1345-COMMITTEE-LIBE_vd?auth_cloudf=c3e8a8d1-e536-ac08-b5a9-1a4fbc1f3951>; See the (unofficial) summary: 'European Parliament Debates the Impact of Schrems 2 on EU-US Data Transfers' (*Cooley*, 8 September 2020) <https://cdp.cooley.com/european-parliament-debates-the-impact-of-schrems-2-on-eu-us-data-transfers/> accessed 12 November 2020
[342] See, for example, the Oasis protocol project, based on blockchain technology and aiming, among other things, to allow companies and data subjects to keep track of every access to their data, which could perhaps solve the problem of opacity of data access by U.S. LEAs (e.g. under gag order). Google entered in a first partnership with the Oasis team; See <https://oasisprotocol.org/> and <https://medium.com/oasis-protocol-project/bringing-gcps-confidential-vms-to-oasis-parcel-95952df06937>

actions have been or could be taken in the future, impose deadlines for taking further action, and ultimately impose fines for non-compliance if necessary.

More broadly, paving the way for requalification would have a range of far-reaching consequences. For instance, the GDPR information requirements (Article 13 and 14) for controllers would become applicable to processors requalified as joint controllers.[343] This would render US superproviders much more accountable on the whole, as they would be constrained to actively seek compliance with all provisions of the GDPR.

Meanwhile, EU-based companies will remain accountable for their choices with regard to the processing activities they determine, including their choice of US superproviders. This means in practice that an EU-based company who decides to use the services of a US superprovider and transfer data to it may also be held liable and fined.[344] EU companies – but also EU public entities – (will) therefore have to avoid non-compliant economic partners. As a result, the US superproviders which make the least effort to comply should gradually be put at a disadvantage compared to competitors who take steps to comply. One thing leading to another, the market will favour GDPR compliant providers, while the others will see their attractiveness decrease. Providers who do not want to lose their customers, and therefore incur significant economic losses in addition to potential fines, will have to pursue compliance. For this to work, however, US superproviders attempting to comply need to be clearly identified. As already mentioned, the European legislator has incorporated a series of soft law mechanisms in the GDPR, such as adherence to codes of conduct and certification mechanisms, which are intended to enable everyone to easily identify compliant partners they can trust. A set of processing activities of the EU establishment of a US superprovider could get certified if it successfully avoids or limits data transfers (e.g. by acting on the isolation of infrastructures as proposed by Mr Schrems),[345] while a set of processing activities of the US entity could get certified if sufficient safeguards are implemented when conducting data transfers.[346] This can be seen as a kind of 'regulation by the market' in Lessig's terms,[347] since US superproviders would have economic interests in getting certified and adhering to code of conducts (as their customers would naturally adapt their choices of partners depending on such factors). Currently, there are very few mature developments regarding these certifications, and no common certification yet (no European Data Protection Seal).[348]

To conclude, there is room for compliance efforts at multiple levels, as well as for gradual enforcement by DPAs in a way that distributes responsibility in the most coherent manner possible.

---

[343] See Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019) [261-268]

[344] According to the EDPB (interpreting the *Fashion ID* case), 'the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision'; EDPB Guidelines 07/2020 (n 299) and *Fashion ID* judgement (n 336)

[345] Article 42(2) GDPR, first part

[346] Article 42(2) GDPR, second part; See for an in-depth analysis on certification mechanisms: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc Van Lieshout and Gabriela Bodea, *Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679: Final Report*, (Commission - DG Justice & Consumers 2019) <https://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en> 174ff

[347] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999)

[348] Irene Kamara, '4 GDPR-certification myths dispelled' (*IAPP*, 28 January 2020) <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> accessed 14 March 2021

4.4 Internal challenges in the EU: The efficiency of DPAs, the one-stop-shop mechanism and the coordination of fines between DPAs

Data protection depends ultimately on the effectiveness of the DPAs, the real arm of the GDPR. The integration, into the enforcement strategy, of DPAs actions – whether against US superproviders as developed above or against EU-based companies – assumes that DPAs are indeed effective and coordinated. However, almost eight years after Mr Schrems' initial complaint, the DPC has still not taken any concrete action, even though its competence is not in dispute. On the merits of the case, Facebook Ireland would not even need requalification as it is already a controller.[349]

After a review of the ongoing *Schrems* procedure to better comprehend its progress and slowdowns and the DPC's share of responsibility (Sub-section 4.4.1), the *one-stop-shop mechanism* will be scrutinized as one of the culprit and potential workarounds will be examined in the light of recent developments (Sub-section 4.4.2); Finally, the crucial question of (coordination of) fines between DPAs will be touched upon (Sub-section 4.4.3).

4.4.1 The ongoing Schrems procedure

The course of the *Schrems* procedure until the release of the *Schrems II* judgment has already been explained *supra*.[350] The cautious approach, up to that last judgement, of the DPC – which basically asked the Court each time for confirmation of its powers and suspended/joined its procedures several times – was criticised by Mr Schrems at the time.[351] The complete procedure, including developments in the year following the *Schrems II* judgement, is illustrated in **Figure 2** from the *noyb* website.[352]

Following the *Schrems II* judgement, the DPC started a new procedure against Facebook Ireland,[353] and paused indefinitely Mr Schrems' complaint,[354] despite the DPC's 2015 undertaking before the Irish Court to decide swiftly on the complaint.[355] Both Facebook and Mr Schrems challenged this decision before, once again, the Irish High Court: In a nutshell, Facebook contested the DPC's ability to start its own, separate investigation, while Mr Schrems argued that the DPC had 'locked him out of his own case, as the subject matter would be dealt with in an "own volition" case between Facebook and the DPC alone'.[356]

---

[349] As a reminder, see situation ① *supra* (Sub-section 4.3.2)
[350] See Chapter 2 of this paper
[351] See in particular *noyb* (n 138)
[352] 'Decision by Irish High Court - DPC must now implement CJEU decision and stop EU-US transfers.' (*noyb*, 13 May 2021) <https://noyb.eu/en/decision-irish-high-court-jr> accessed 13 May 2021
[353] Facebook received confidentially a preliminary decision, see: Sam Schechner and Emily Glazer, 'Ireland to Order Facebook to Stop Sending User Data to U.S.' (*Wall Street Journal*, 9 September 2020) <https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980?mtc=j> accessed 15 February 2021
[354] *Noyb* (n 352)
[355] See *noyb* (n 138)
[356] *Noyb* (n 352); See also 'Irish High Court: Judicial Review against DPC admitted' (*noyb*, 14 September 2020) <https://noyb.eu/en/irish-high-court-judicial-review-against-dpc-admitted> accessed 3 April 2021

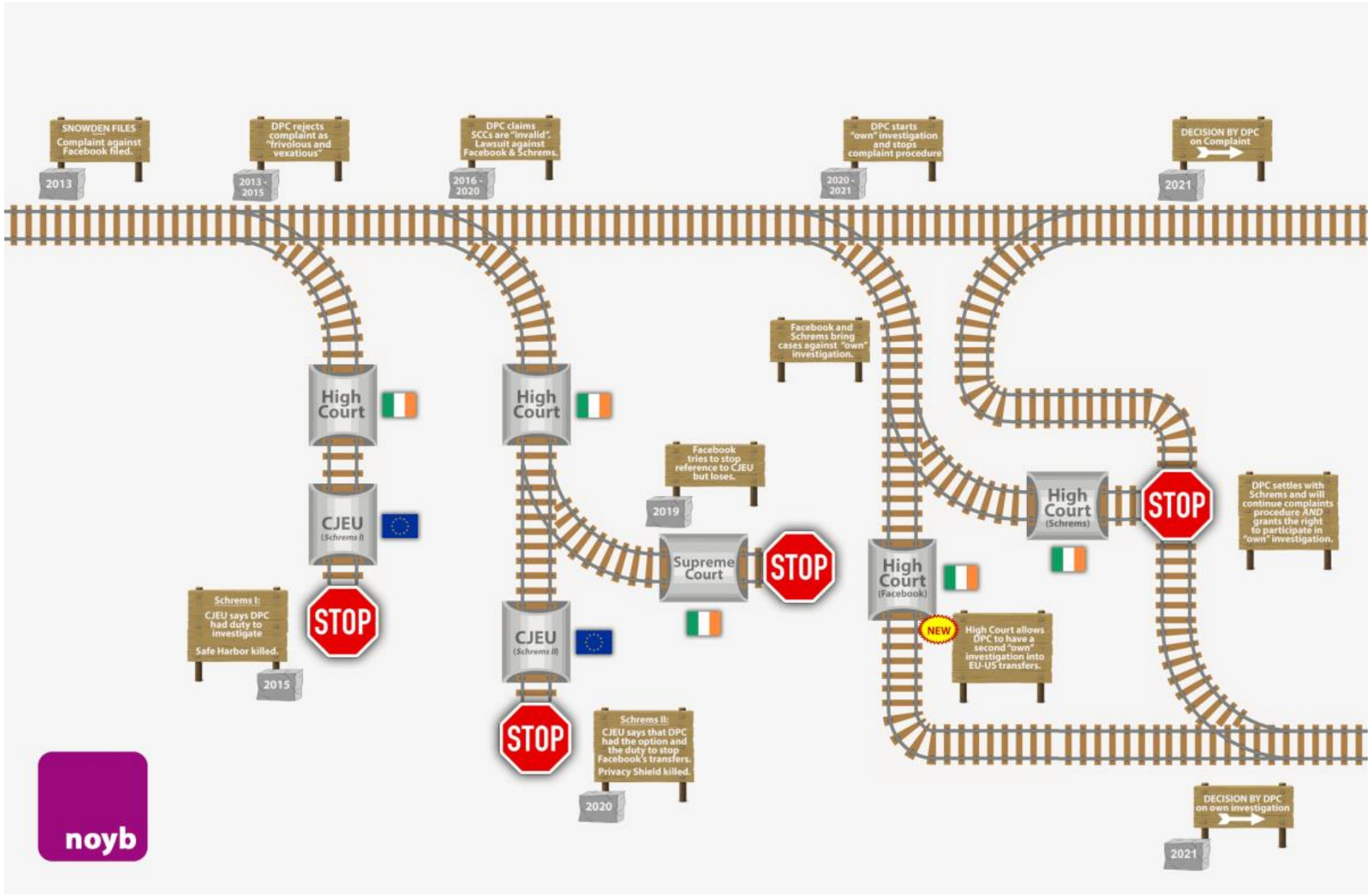

FIGURE 2: COMPLETE SCHREMS PROCEDURE ILLUSTRATED BY NOYB

Mr Schrems then reached a settlement with the DPC to swiftly take a decision on its own complaint once the Irish Court had made its decision on Facebook's objections.[357] In 13 May 2021, the Irish Court dismissed Facebook's main claims, so that the DPC can indeed start its own investigation, in addition to addressing Mr Schrem's complaint as settled.[358] As a result, there are now two separate ongoing procedures in the DPC's hands with the very same root issue: the data transfers to the US conducted by Facebook Ireland.

The DPC's upcoming draft decision(s) is (are) more than likely to be subject to an opinion from the EDPB[359] (composed of the representatives of all the other DPAs)[360] according to Article 64(2) to (6) of the *consistency mechanism*.[361] Such opinion shall be adopted within 8 weeks, extendable by a further 6 weeks.[362] If the DPC does not intend to follow the opinion of the Board, the *dispute resolution mechanism* of Article 65 GDPR would be triggered, starting its own new procedural deadlines.[363] A rough calculation shows that if the DPC issues its draft decision in early July 2021 (which would already be a year since the *Schrems II* judgment!) and thereafter challenges the EDPB's opinion on it, the final decision could theoretically be taken up to 17 weeks later, i.e. in mid-November 2021.

This series of procedures seems simply endless. The DPC was accused of mismanagement by *noyb*,[364] that concluded that 'the DPC is acting as a bottleneck for Europeans' right to privacy. The procedure is Kafkaesque'.[365] *Noyb* asserted that 'the DPC has not even provided all relevant document to its European counterparts' and that 'even if the DPC has now performed a first of six steps, we are still lacking documents from that first step'.[366] Overall, it appears that although Ireland is a major hub for the establishment of IT companies, only 6 or 7 formal decisions were made in 2020,[367] which represents 0.07% of all GDPR complaints reported by the DPC that year…[368] In the DPC's defence, it must be admitted that its tasks are daunting given the number of IT establishments in Ireland and the fact that the DPC is now the only DPA available whose official language is English since the Brexit. Yet, the Irish state itself aims to be the European technology hub and have the obligation, under Article 52(4) GDPR, to provide sufficient resources, premises and infrastructures to its DPA. On 20

---

[357] 'Irish DPC agrees to decide swiftly on Facebook's EU-US transfers' (*noyb*, 13 January 2021) <https://noyb.eu/en/irish-dpc-agrees-decide-swiftly-facebooks-eu-us-transfers> accessed 3 April 2021; See also *Noyb* (n 352)

[358] Ibid; See also Douglas Busvine and Conor Humphries 'Facebook faces prospect of 'devastating' data transfer ban after Irish ruling' (*Reuters*, 14 May 2021) <https://www.reuters.com/business/legal/facebook-data-transfer-ruling-irish-court-due-friday-2021-05-14/> accessed 15 June 2021

[359] Because it would obviously 'produc[e] effects in more than one Member State' as per Article 64(2) GDPR

[360] Article 68 GDPR

[361] Article 63 GDPR

[362] Article 64(3) GDPR

[363] Article 64(8) and 65 GDPR

[364] See *Noyb* (n 138); See also 'Irish High Court allows Judicial Review to stop Facebook EU-US transfers' (*noyb*, 12 October 2020) <https://noyb.eu/en/irish-high-court-allows-judicial-review-stop-facebook-eu-us-transfers> accessed 19 June 2021

[365] 'Judicial Review against DPC over slow procedure granted' (*noyb*, 6 July 2021) <https://noyb.eu/en/judicial-review-against-dpc-over-slow-procedure-granted> accessed 13 May 2021

[366] Ibid

[367] Conor Humphries, 'EU-U.S. data flows could face 'massive disruption' - Irish regulator' (Reuters, 25 February 2021) <https://www.reuters.com/article/uk-facebook-privacy-dixon-interview-idINKBN2AP005> accessed 20 June 2021

[368] *Noyb* therefore refers to the DPC the 'Bermuda triangle' of GDPR complaints; 'Irish DPC "handles" 99,93% of GDPR complaints, without decision?' (*noyb*, 28 April 2021) <https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision> accessed 28 April 2021

May 2021, the EU Parliament adopted a resolution[369] calling on the Commission to start infringement procedures against Ireland. In reality, giving priority to efficient enforcement action against big players (e.g. US superproviders) as is argued in the thesis would result in many situations being brought into compliance at once and thus alleviate the work of the DPC.

What is perhaps even more surprising is that a US superprovider used extensively throughout the Union but established in Ireland (such as Facebook, Goole, Apple, and Twitter) appears to only be subject to a decision imposed by the Irish authority. This results from the *one-stop-shop mechanism*.

4.4.2 The one-stop-shop-mechanism, a device that unwittingly hinders the GDPR effectiveness

When a processor or controller carries out cross-border (i.e. among several Member States)[370] processing activities, Article 56 GDPR lays down that the *lead supervisory authority* (hereinafter lead DPA) is solely competent for those processing activities (with a few exceptions),[371] although it shall cooperate with the other DPAs *concerned*.[372] The lead DPA is the DPA in the country in which the controller/processor has its *main establishment*. According to Article 4(16), the main establishment is usually the place of the central administration[373], although it can in some circumstances be the place of the establishment that actually decides on the purposes and means (for a controller) or where the processing activities actually takes place (for processors). In case of conflicting views between DPAs regarding the determination of the lead authority, the *dispute resolution mechanism* may be triggered.[374]

A first observation can already be drawn: If a US superprovider does not have any establishment in the Union, then there is no lead authority, and any DPA can take enforcement actions. In the context of US superproviders, it is rather unlikely (although possible).[375]

Conversely, if there is a lead DPA that decides, according to Article 56(4), to handle a case against a main establishment but, in reality, does not take action, the other DPAs have, with few exceptions,[376] no choice but to wait for the lead DPA. Put simply, this means that DPAs cannot make decisions instead of the DPC regarding data transfers based on the DPC's deficiency. In a recent CJEU preliminary ruling[377] regarding a Belgian case where the Belgian DPA was seeking to take measures against Facebook,[378] the Court clarified the powers of *concerned* DPAs that do not qualify as lead DPA. Despite several press headlines suggesting that the Court has extended the ability of non-lead DPAs to take enforcement action,[379] the

---

[369] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html>

[370] Article 4(23) GDPR

[371] Exceptions in Articles 56(2), 61(8) and 66 GDPR

[372] Articles 53(1) and 60 GDPR; On DPA concerned: Article 4(22) GDPR

[373] Further developed in Recital 36 GDPR

[374] Article 65(1)(b) GDPR

[375] As it was considered in situations ② and ④ *supra* (Sub-section 4.3.2 and 4.3.3(a)(i) respectively).

[376] See (n 371)

[377] Case C-645/19 *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483

[378] With regard to its collection of information on the browsing behaviour of Internet users

[379] See for instance 'EU court gives data watchdogs more bite against Facebook, big tech firms' (*Free Malaysia Today* 15, June 2021) <https://www.freemalaysiatoday.com/category/business/2021/06/15/eu-court-give-data-watchdogs-more-bite-against-facebook-big-tech-firms/> accessed 20 June 2021; Foo Yun Chee, 'EU data watchdogs ruling sharpens focus on Facebook, big tech' (*Reuters*, 15 June 2021)

Court has in fact confirmed the application of the *one-stop-shop mechanism*, and simply reiterated the narrow exceptions that are already provided for in the GDPR.[380] Those exceptions require urgency, and produce effects limited in time and to the Member State's territory.[381] Interestingly enough, the German DPA took on 21 May 2021 a preliminary order against Facebook Ireland regarding the forced consent to the new privacy policy of WhatsApp (owned by Facebook).[382] It may be that DPAs will try to invoke more frequently those currently rare exceptions, but their effects will nonetheless remain limited.

There is, however, one point that has been overlooked so far and that this thesis wants to raise: The interplay between, on the one hand, the extended interpretation of Article 3(1) since the Google Spain judgement,[383] and, on the other hand, the determination of the lead DPA. The general assumption so far seems to be that whenever a US superprovider

- has an establishment in the EU
- which falls under the scope of the GDPR thanks to Article 3(1) together with the Google Spain judgement
- and which can therefore be subject to investigative and coercive measures with regard to the processing activities carried out by a US entity,

then the lead DPA is *ipso facto* the DPA of the place of said EU establishment. However, the criteria to trigger Article 3(1) GDPR, and the criteria of Article 56 GDPR read in conjunction with Article 4(16) GDPR to determine the lead authority, are *not* the same, even though they can occasionally pinpoint to the same establishment. For instance, in the Google Spain judgement, the processing activities were deemed to be taken in the context of the activities of Google Spain. Does this mean that Google Spain was the central administration of the Google multinational, or that it decided on the purposes and means of these specific processing activities (as required per the definition of the main establishment in the GDPR)? If applying Recital 36 GDPR and determining the main establishment 'according to objective criteria', it is clear that the answer should be *no*, so that in reality the Spanish DPA was probably not the lead DPA, but rather a DPA *concerned*.[384] Similar reasoning was adopted in the French DPA decision imposing a €50 million fine on Google Ireland even though the French DPA was not qualifying as the lead DPA.[385] The French DPA devoted a significant part of its decision to

<https://www.reuters.com/world/europe/top-eu-court-says-national-watchdogs-may-act-against-violations-blow-facebook-2021-06-15/> accessed 24 June 2021

[380] See (n 371)

[381] Articles 61(8) and 66 GDPR; As a side note, Gömann pointed out a lack of clarity as to which law should apply when a DPA makes a decision under one of these exceptions (while the GDPR has direct effect, some aspects are left to the Member States): Merlin Gömann, 'A Hidden Revolution – Domestic Application of Foreign Public Law under the GDPR' (*Verfassungsblog*, 17 June 2021) <https://verfassungsblog.de/a-hidden-revolution/> accessed 20 June 2021

[382] German (Hamburg) DPA (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit), 'Order of the HmbBfDI: Ban of further processing of WhatsApp user data by Facebook' (11 May 2021) <https://datenschutz-hamburg.de/assets/pdf/2021-05-11-press-release-facebook.pdf> accessed 20 June 2021

[383] See *supra*; *Google Spain* judgement (n 319)

[384] In the meaning of Article 4(22) GDPR

[385] French DPA (Commission Nationale de l'Informatique et des Libertés, CNIL), 'Délibération de la formation restreinte no SAN-2020-012 du 7 décembre 2020 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED' (7 December 2020) <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706> (in French); An English translation of the version of the deliberation dating from before the appeal mentioned under (n 386) is available: French DPA, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC [SAN-2020-012]' (21 Janvier 2019) <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>

demonstrating that the DPC was *not* the lead DPA with respect to the processing activities at issue. Its decision was challenged and upheld by the highest French administrative Court, the *Conseil d'Etat*.[386]

Such a reconsideration of the notion of lead DPA is promising. Of course, it could be objected that such an approach amounts to jeopardizing legal certainty and the unifying approach pursued by the GDPR,[387] but is such a solution not better than a total lack of coercion by the lead DPA? It goes without saying that the DPAs should ideally cooperate in good faith and constructively and simply agree on which of them should handle which case, but in the meantime, this alternative solution appears to be useful to fill the gap in enforcement.

The one-stop-shop mechanism and the determination of the main establishment, as well as their interplay with other rules of the GDPR, had already been heavily debated during the drafting of the GDPR,[388] including the situation of controllers and processors not established in the Union.[389] There is certainly room for legislative enhancements of the one-stop-shop mechanism (the draft of the EU Digital Service Act[390] is interesting in that respect)[391], but such change is not for anytime soon and would be out of the scope of this thesis. For the time being, it is urgent that the Commission and the European institutions bring the DPC to order.

4.3.3 The DPAs' fines and their coordination

One of the major innovations of the GDPR is the fines that can be imposed on controllers and processors. They can be up to 4% of the total worldwide annual turnover of the preceding financial year.[392] This system and methodology for determining the fine are inspired by European competition law.[393] In 2019, Nemitz wrote:

> '[t]he European experience in competition law shows that the public enforcement […] is the main driver of compliance. Private enforcement and actions for damages […] play a smaller role, with the later often being efficient only as a follow on of public enforcement findings of illegality. A fortiori the private enforcement or damages claims

[386] Conseil d'État (France), Decision N° 430810 (19 June 2020) <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil>; The decision holds (translated from French): 'It follows [...] that Google Ireland Limited could not be considered as the central administration of the controller of the disputed processing operations and that Google LLC, which alone determined their purposes and means, did not have, at the date of the contested sanction, a principal place of business within the European Union, within the meaning and for the application of the RGPD. As no lead authority could therefore be designated under the conditions provided for in Article 56 of the RGPD, the CNIL was competent to investigate the complaints of the associations None of Your Business and La Quadrature du Net regarding the processing of personal data of French users of the Android operating system operated by the company Google LLC and to impose the contested sanction on the latter.'

[387] On the unifying approach see Balboni, Pelino and Scudiero (n 388)

[388] See this comprehensive analysis: Paolo Balboni, Enrico Pelino and Lucio Scudiero, 'Rethinking the One-Stop-Shop Mechanism: Legal Certainty and Legitimate Expectation' (2014) 30 Computer Law & Security Review 392

[389] Ibid, 396-397

[390] See Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2020] COM/2020/825 final <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>

[391] Under Article 46 of the Digital Service Act, where a lead *Digital Services Coordinator* does not act the Commission can step in and request the lead *Digital Services Coordinator* to enforce the Regulation

[392] Article 83 GDPR

[393] Paul Nemitz, 'Fines under the GDPR' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019) 233ff <http://www.bloomsburycollections.com/book/data-protection-and-privacy-the-internet-of-bodies>

> in data protection law have so far in practice played no significant role in Europe. […] In addition, the usual enormous asymmetry of economic power and information between the individual and the controllers and processors in the digital economy is a key argument for strong public enforcement: the individual simply cannot be left alone in this asymmetry'.[394]

It is indeed beyond debate that the private damages that Mr Schrems could hypothetically claim in his complaint will not act as a deterrent,[395] and that appropriate fines from DPAs are needed.

The largest GDPR fine ever imposed to date is the €50 *million* ($56.6 million) fine imposed on Google Ireland in 2020 by the French DPA, mentioned above.[396] Although it may seem large, Google's global turnover in 2020 was $162 billion ($162,000,000,000).[397] The highest fine that could have been imposed in 2020 was therefore 4% of that amount, or $6.48 *billion*. Freeman notes that "[t]his is reminiscent of the old U.K. Data Protection Act 1998, where businesses found it cheaper to budget for fines than to actually comply with the law".[398] Unsurprisingly, for a fine to be useful, it is necessary for 'the amount of the fine [to] be significantly higher than any profit derived from the violation of the GDPR'.[399]

Not only does this highest fine seem quite low, but the total amount of all fines imposed since the entry into force of the GDPR is surprisingly low for a regulation that is intended to be the 'gold standard' (in the words of a Commission statement),[400] especially when compared to US fines for privacy breaches as shown in **Figure 3**.

[394] Ibid 234-235

[395] Yet, such action can in itself draw attention to the underlying problem and bring other measures into motion, as in the Schrems case (the DPC could totally forbid data transfers to the US). In this sense, private action can also have a role to play in the regulation and enforcement strategy and have concrete non-monetary impacts, as developed in Chapter 4, Section 4.2 of this paper

[396] Decision of the French DPA (n 385)

[397] See <https://www.webrankinfo.com/dossiers/google/resultats-financiers> accessed 21 June 2020

[398] In Neil Hodge, 'Reported Amazon fine ($425M) 'biggest test' of GDPR enforcement yet' (*Compliance Week*, 15 June 2021) <https://www.complianceweek.com/gdpr/reported-amazon-fine-425m-biggest-test-of-gdpr-enforcement-yet/30479.article> accessed 20 June 2021

[399] Nemitz (n 393) 239

[400] Commission, 'Joint Statement by Vice-President Jourová and Commissioner Reynders ahead of Data Protection Day' (27 January 2021) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_208>; Lambert refers to a 'draconian' regime; Lambert (n 28)

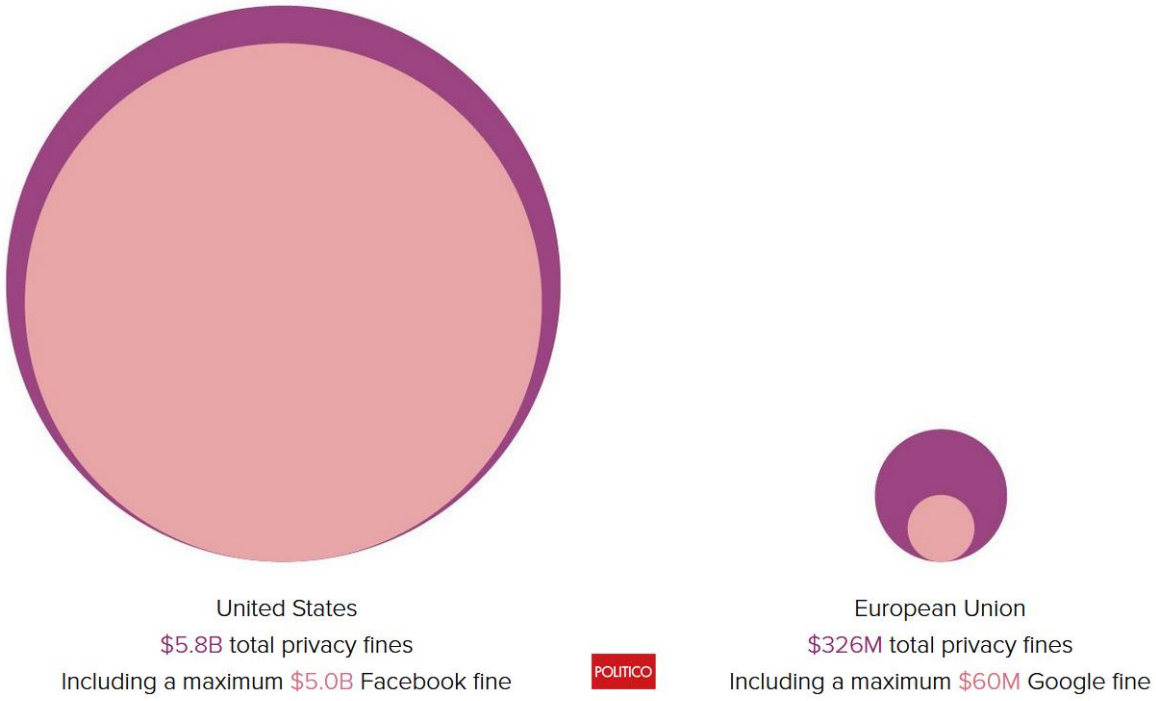

FIGURE 3: PRIVACY FINES ISSUED BY THE U.S. FEDERAL TRADE COMMISSION COMPARED TO GDPR FINES LEVIED BY DPAS, COLLECTIVELY, SINCE MAY 2018 WHEN THE GDPR CAME INTO FORCE [401]

In addition to showing the relatively low fines imposed under GDPR, this figure also highlights the EU's general approach – which this thesis calls for to be reviewed – to focus less on GAFAM.

Things could however gradually change: The DPA in Luxembourg, where Amazon is mainly established, recently took a draft decision against Amazon imposing a €350 million fine.[402] Such amount remains quite modest, leading some to say that it "sends a mixed message",[403] but this procedure can initiate coordination between DPAS, as the lead Luxembourg DPA sent its draft to the other DPAs according to the *consistency mechanism*.[404] A consensus may be difficult to achieve given the widely divergent views of DPAs. For example, in another case concerning Twitter, the DPC proposed a €135,000 fine while Germany proposed between €7.3 million and €22 million...[405] Ultimately, the *dispute resolution mechanism* will probably be triggered, and will be the opportunity for the EDPB to give a trend for fine amounts 'before regulators lose patience and find legal means to mete out penalties under national laws instead of the [GDPR]'.[406] There is indeed an urgent need for the DPAs to

[401] Vincent Manancourt and Mark Scott, 'What the US can teach Europe about privacy' (Politico, 10 February 2021) <https://www.politico.eu/article/europe-privacy-fines-tech-what-the-us-can-teach/> accessed 15 April 2021; Sources for the data used by Politico: US Federal Trade Commission, DLA Piper, POLITICO research
[402] Hodge (n 398)
[403] According to Freeman in Hodge (n 398)
[404] *In species*, all DPAs are *concerned* since Amazon's processing activities at stake applies to citizens throughout the EU
[405] According to Freeman in Hodge (n 398)
[406] Neil Hodge, 'GDPR priorities for 2021: Twitter ruling stresses need for harmonization' (*Compliance Week*, 22 December 2020) <https://www.complianceweek.com/gdpr/gdpr-priorities-for-2021-twitter-ruling-stresses-need-for-harmonization/29870.article> accessed 20 June 2021

achieve a harmonised approach to the levels of fines, as otherwise, 'the one-stop shop mechanism benefits companies and not supervisory authorities' because 'the system enables firms to 'forum shop' and choose a perceived 'soft' regulator that is badly resourced, slow to act, and domiciled in a country that is traditionally pro-business to lead complaints against them'.[407]

To conclude, the (extra-)territorial scope of the GDPR, the one-stop-shop mechanism, the financing of DPAs[408] and the harmonisation of fines are intrinsically linked and require a real coordination effort.

4.5 Limitations: Towards a longer-term solution with the US?

At the end of May 2021, the EDPS – responsible for monitoring and enforcing compliance with data protection rules by the European institutions –[409] announced that it launched two investigations, one into the EU institution's use of Amazon Web Services and the other into the EU Commission's use of Microsoft Office 365.[410] Such announcement is encouraging for the future and will probably be insightful on the implementation, in practice, of the EDPB recommendations that followed the *Schrems II* judgement. Yet, this is once again an instance of investigations targeting entities that rely on the services of US super-providers, rather than the US super-providers themselves.

Taking varied enforcement action against US superproviders and more generally raising the level of demands on these key players is promising to limit data transfers, protect some of the data transferred, including in transit, promote the development of methods and technologies capable of making certain transfers compliant, and ultimately regain some sort of control over the current situation. This would also unburden the work of the DPAs by killing several birds with one stone.

Some would nevertheless object that none of these proposals is sufficient on their own to satisfactorily solve the underlying issue of mass surveillance in the US – and they would be right. For example, separating superproviders' infrastructures between the EU and the US may make access to data more complicated and less covert – which would already be an important improvement –, but it would not be enough because US LEAs can compel companies in the US to take the necessary steps to provide access to data over which they have 'possession, custody or control', which will generally be the case with respect to entities in the EU of which they are the parent company.

Still, DPAs' enforcement actions with potential (huge) fines, as well as the pressure that European companies could gradually put on their American partners, should ultimately influence the diplomatic negotiations at the heart of the problem: the clash between US law and European law. As Kuner summarised after *Schrems I*, 'legal issues of data transfer regulation are intertwined with the underlying political positions of the parties, and […] the law cannot by

---

[407] According to Sonia Cissé in Hodge (n 406)

[408] See Nemitz (n 393), in particular 232

[409] The European institutions are not subject to the RGPD but to another (very similar) regulation which includes most of the rules and principles of the RGPD: 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

[410] European Data Protection Supervisory, 'Press Release – The EDPS opens two investigations following the "Schrems II" Judgement' (27 May 2021) <https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en> accessed 15 June 2021

itself provide a resolution of the disagreements between them unless they are willing to go beyond their preconceptions and consider the larger issues at stake'.[411] Indeed, '[p]rocedural mechanisms may satisfy formal requirements of data protection law, but they cannot provide protection against the intelligence surveillance that the Schrems case involved'.[412] This is also what Mr Schrems pointed out throughout his speech to the Parliament, recalling that the main current problem cannot be solved by an executive body.[413]

This thesis acknowledges that the sole enforcement, by DPAs, of EU law as it stands today cannot provide a permanent solution, and therefore agrees with Kuner's conclusion. It does not, however, fully concur with Kuner's observations as strong enforcement turns out to be nevertheless a crucial preliminary step for initiating improvements in the negotiations with the US. When one considers that the EU market represents billions for the tech providers every year, and thus indirectly to the US treasury, one can assume that Europe actually has quite a lot of room to negotiate with the US. Recital 102 GDPR explicitly states that the GDPR does not preclude an agreement between the EU and third countries regarding data transfers. As Mr Schrems says, it would not be unreasonable to demand from the US the same protection for EU citizens as for US citizens[414] if they want to continue to be the Cloud and technology providers of the European market. If concessions were to be made by the US – i.e. granting the same guarantees to EU citizens as US citizens in law and in the practice of intelligence agencies, and implementing efficient redress mechanisms available to individuals – in order to reach a level of protection essentially equivalent to the one of the EU, perhaps some adjustments could or should be made on the EU side, as developed in more detail in the Swire's work.[415]

In short, acting simultaneously against US providers and, in parallel, against EU companies that use their services and are their source of revenue could apply enough pressure on the US companies and government and recall that, in the end, both European individuals, European companies, US providers and the US government have an interest in reaching a fair deal through diplomatic means.

---

[411] Kuner (n 26) 885
[412] Ibid
[413] Hearing of the European Parliament (n 341)
[414] See (n 20)
[415] Peter Swire, 'Testimony by Peter Swire at the U.S. Senate Commerce Committee Hearing on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows"' (*Cross-border Data Forum*, 13 January 2021) <https://www.crossborderdataforum.org/testimony-by-peter-swire-at-the-u-s-senate-commerce-committee-hearing-on-the-invalidation-of-the-eu-u-s-privacy-shield-and-the-future-of-transatlantic-data-flows/> accessed 15 May 2021
[416] 'Privacy 2030 A New Vision for Europe' (*Published by IAPP*, November 2019) 22 <https://iapp.org/resources/article/privacy-2030/> accessed 14 April 2021

Conclusion

Both the former DPD and the GDPR include(d) strict conditions for transferring data to third countries in order to ensure that individuals' rights are not undermined. The concept of data transfer is very broad and includes not only the storing or sending data to third countries, but also the mere fact of providing access to data from a third country. In an increasingly digitalised and globalised world, data transfers in the sense of EU law are commonplace.

The *Schrems I* and *II* judgments reaffirmed the high standards of the EU Charter on data protection and, as a corollary, of the requirements for data transfers. Following a thorough assessment of US intelligence laws and practices, the CJEU concluded that the US did not offer a substantially equivalent level of protection to that of EU law given the practices of mass surveillance and the relevant legal requirements, the lack of protection for non-US citizens, and the absence of effective remedies for individuals. The Court invalidated the Commission's adequacy decisions and reduced the valid use of transfer tools to situations where the rights of individuals are effectively safeguarded. They also confirmed the powers (and duties) of DPAs with regard to the enforcement of transfer rules.

Subsequently, the EDPB published guidelines that draw practical conclusions from the *Schrems II* judgment, and drastically reduce the situations in which data transfers are considered lawful. This leaves many companies with little or no means to lawfully pursue the majority of their transfers, at least until a substantive solution is found between the EU and the US.

Failing to reach an agreement with the US so far, the Commission has come up with new SCCs aimed at making data importers more accountable. Although innovative, their contractual nature will not fundamentally change the balance, as they must abide by US law. The burden of finding solutions on a case-by-case basis rests for the time being with the data controllers and will be very challenging, if not often impossible. The Commission, as well as, with some reluctance, the EDPB, have opened a loophole by adopting a risk-based approach in the third countries assessments, allowing data exporters to rely on the fact that they have no reason to believe – from their practical experience – that the relevant problematic laws will be applied to the transfers at stake. However, the use cases of the risk-based approach remain limited and, above all, it is likely to be incompatible with the *Schrems* judgements and the Charter. This accommodation will certainly not constitute a sustainable truce for data exporters, but at most an interbellum until further progress is made.

To ultimately achieve compliance regarding data transfers, the EU needs an ad-hoc, phased enforcement strategy that is coherently integrated with the broader GDPR regulatory scheme. Taking a step back and mapping the different stakeholders, it is clear that many data transfers are decided, necessitated and implemented by US companies providing services to individuals and businesses in the EU. This thesis has therefore supported a partial, first-stage solution to be sought from the superproviders. They can indeed avoid or limit transfers, or take technical measures to make them compliant, and are the actors which are best placed to solve the alleged current impasse regarding data transfers to the US. More importantly, they represent a valuable part of the US economy, and are therefore a vector of pressure on the latter in a longer-term ambition.

As little progress is currently being made through traditional enforcement focus on EU-based companies relying on US superproviders, there is an urgent need for US superproviders to be directly involved and, more specifically, for the DPAs to take effective gradual action against them. The feasibility, both in terms of jurisdiction and sufficiency of the substantive rules in the GDPR, has been demonstrated in this thesis. In both the B2C and B2B contexts, the GDPR is usually applicable to US superproviders – either territorially or extra-territorially –, and their proactive requalification (where necessary) as joint-controllers by DPAs and Courts would allow all the substantive rules of the GDPR, including Chapter V, to apply to them *ex post* but also *ex ante*.

It now remains for the DPAs to overcome their structural and coordination problems that prevent them from taking surgical measures (and for the Member States to allocate the resources they need). In particular, the one-stop-shop mechanism, while having significant weaknesses in not distributing the workload evenly among DPAs and in preventing non-lead DPAs from intervening in the event of inertia, could be bypassed as far as US companies are concerned. In conjunction, the EDPB's dispute resolution mechanism has the potential to give direction to future enforcement actions and fine levels – regardless of the tenor of the decisions – and put enforcement actions back on track.

Ultimately, such incremental improvements would support the negotiation effort of the Commission. The EU has already influenced many privacy legislations around the world and has in fact significant leverage on future privacy regulation worldwide, including towards the US. Some concessions from the US would simply be fair and beneficial to all parties involved.

There is a lot of work to be done and the solutions provided in this thesis are only an outline in a complex field, but hopefully, the 2030 horizon envisioned by the 'Buttarelli's Manifesto' (the former European Data Protection Supervisor) will find resonance in future developments regarding data transfers. After continually refusing to significantly lower its conceptual standards, the EU must now give itself the means to materialise these aims so that they do not remain merely on paper.

"The EU has enormous leverage for changing the rules of the game — but it is unused because we are torn between our convictions and our aspirations to compete on its rivals' terms."

Buttarelli's Manifesto [416]

Bibliography

PRIMARY SOURCES

Legislation

European Union Law

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

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) [2016] OJ L119/1

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

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 L 12

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 [1995] OJ L 281

United States Statutory Law

Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub.L. 115-141, 132 Stat. 348 (23 March 2018)

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§1801–85 (2012)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT ACT), Pub.L. No. 107-56, 115 Stat. 272 (24 October 2001)

Stored Communications Act, Pub.L. 99-508, 100 Stat. 1848 (21 October 1986)

Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200

Council of Europe

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS No. 108

Case Law

Court of Justice of the European Union

Case C-645/19 *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483

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

Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629

Opinion 1/15 of the Court (Grand Chamber) [2017] ECLI:EU:C:2017:592

Case T-670/16 *Digital Rights Ireland v Privacy Shield* [2017] ECLI:EU:T:2017:838

Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612

Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317

Case C-293/12 and C-594/12 *Digital Rights Ireland and Other* [2014] EU:C:2014:238

Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECLI:EU:C:2010:740

Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECLI:EU:C:2003:596

Supreme Court of the United States

United States v. Microsoft Corp., 584 U.S. (2018)

French Conseil d'Etat

Conseil d'État (France), Decision N° 430810 (19 June 2020) <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil>

SECONDARY SOURCES

European Commission Decisions

Commission Implementing Decision (EU) 2021/914 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 [2021] OJ L 199

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 (notified under document C(2016) 4176), [2016] OJ L 207

Commission Decision 2010/87/EC of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 [2010] OJ L 39; Amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [2016] OJ L 344

Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L 181; Amended by Commission Decision 2004/915/EC 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 L 385

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) [2000] OJ L 215

Official European Union Documents

European Commission

Commission, 'Data protection: European Commission launches process on personal data flows to UK' (19 February 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661>

Commission, 'Joint Statement by Vice-President Jourová and Commissioner Reynders ahead of Data Protection Day' (27 January 2021) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_208>

Draft Commission implementing decision (EU) 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 Ares(2020)6654686 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-

contractual-clauses-for-the-transfer-of-personal-data-to-third-countries> accessed 8 January 2021

Commission, 'Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo' (25 March 2021) <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_144>

Commission, 'Fact Sheet EU-U.S. Privacy Shield: Frequently Asked Questions' (12 July 2016) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462>

Commission, 'Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross' (10 August 2020) <https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836>

Commission, Communication COM/2017/07 final from the Commission to the European Parliament and the Council, 'Exchanging and protecting personal data in a globalised World' (10 January 2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN>

European Parliament

European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html>

Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2020] COM/2020/825 final <https://eur-lex.europa.eu/legal content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>

Hearing of the European Parliament of 3 September 2020 (13:45 - 15:45), 'Committee on Civil Liberties, Justice and Home Affairs' <https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20200903-1345-COMMITTEE-LIBE_vd?auth_cloudf=c3e8a8d1-e536-ac08-b5a9-1a4fbc1f3951>

European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html>

European Parliamentary Research Service (Monteleone S and Puccio L), 'The Privacy Shield – Update on the state of play of the EU-US data transfer rules' (July 2018) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2018)625151>

Council of the European Union

Council Resolution of 24 November 2020 on Encryption, Security through encryption and security despite encryption <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf>

European Data Protection Board

European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Version 2.0' (18 June 2021, version after public consultations) <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>

European Data Protection Board, 'Opinion 16/2021on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe' (19 May 2021) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_nl>

European Data Protection Board, 'Adopted Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom' (13 April 2021) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en>

European Data Protection Board, 'Statement 04/2021 on international agreements including transfers' (13 April 2021) <https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-042021-international-agreements-including_en>

European Data Protection Board, 'EDPB Document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal' (28 January 2021) <https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en>

European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020) <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees>

European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020, version for public consultations) <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en>

European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2 September 2020) <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en>

European Data Protection Board, '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' (23 July 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf>

European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation' (12 November 2019) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en>

European Data Protection Board, 'Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679' (25 May 2018) <https://edpb.europa.eu/our-work-tools/our-documents/directrices/ guidelines-22018-derogations-article-49-under-regulation_en>

European Data Protection Board, 'Endorsement 1/2018' (25 May 2018) <https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_fr>

European Data Protection Supervisory

European Data Protection Supervisory, 'Press Release – The EDPS opens two investigations following the "Schrems II" Judgement' (27 May 2021) <https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en> accessed 15 June 2021

European Data Protection Supervisory, 'The EDPS opens two investigations following the "Schrems II" Judgement' (27 May 2021) <https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en>

European Data Protection Supervisory, 'AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation' (27 April 2021) <https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en> accessed 29 April 2021

European Data Protection Supervisory, 'The transfer of personal data to third countries and international organisations by EU institutions and bodies [Position paper]' (15 July 2014) <https://edps.europa.eu/data-protection/our-work/publications/papers/transfer-personal-data-third-countries_en>

Article 29 Data Protection Working Party

Article 29 Working Party, 'Adequacy Referential' WP 254 rev.01 (6 February 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>

Article 29 Working Party, 'EU-US Privacy Shield- First annual joint Review' WP 255 (28 November 2017) <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782>

Article 29 Working Party, 'Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)' (16 October 2015) <https://ec.europa.eu/justice/article-

29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>

Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP 128 (22 November 2006) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf>

Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' WP 114, 8ff (25 November 2005) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>

Article 29 Working Party, 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' WP 12 (1998) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf>

Official Documents from National DPAs and Courts

Dutch DPA (Autoriteit persoonsgegevens), 'Dutch DPA imposes fine of €525,000 on Locatefamily.com' (12 May 2021) <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-imposes-fine-%E2%82%AC525000-locatefamilycom> accessed 15 May 2021

French DPA (Commission Nationale de l'Informatique et des Libertés, CNIL), '« Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant' (27 January 2021) <https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant> (in French)

French DPA (Commission Nationale de l'Informatique et des Libertés, CNIL), 'Délibération de la formation restreinte no SAN-2020-012 du 7 décembre 2020 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED' (7 December 2020) <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706> (in French)

German (Hamburg) DPA (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit), 'Order of the HmbBfDI: Ban of further processing of WhatsApp user data by Facebook' (11 May 2021) <https://datenschutz-hamburg.de/assets/pdf/2021-05-11-press-release-facebook.pdf> accessed 20 June 2021

Italian DPA (Garente per la Protezione dei Dati Personali), 'Ordinanza di ingiunzione nei confronti di Roma Servizi per La Mobilita S.r.l. [9562831]' (11 February 2021) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9562831> (in Italian)

United Kingdom DPA (Information Commissioner's Office, ICO), 'Guide to the General Data Protection Regulation (GDPR)', <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> (2 August 2010, before Brexit)

Official International Organisations Documents

Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980

Books (and Contributions to Edited Books)

European Union Agency for Fundamental Rights (FRA), *Handbook on European data protection law* (2nd edn Publications Office of the European Union 2018)

Gellert R, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)

Hon WK, *Data Localization Laws and Policy* (Edward Elgar Publishing 2017), <https://doi.org/10.4337/9781786431974>

Kamara I, Leenes R, Lachaud E, Stuurman K, Van Lieshout M and Bodea G, *Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679: Final Report*, (Commission - DG Justice & Consumers 2019) <https://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en>

Lambert P, *Understanding the New European Data Protection Rules* (ProQuest Ebook Central 2017) <https://ebookcentral.proquest.com>

Lessig L, *Code and Other Laws of Cyberspace* (Basic Books 1999)

Millard CJ, *Cloud Computing Law* (Oxford University Press 2014)

Nemitz P, 'Fines under the GDPR' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019) 233ff <http://www.bloomsburycollections.com/book/data-protection-and-privacy-the-internet-of-bodies>

Schwartz PM, 'Information Privacy in the Cloud' (2013) 161 University of Pennsylvania Law Review 1623

Swire P and Litan RE, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press 1998)

Van Alsenoy B, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019)

Voigt P and von dem Bussche A, *The EU General Data Protection Regulation – A practical guide* (2017)

Journal Articles

Balboni P, Pelino E and Scudiero L, 'Rethinking the One-Stop-Shop Mechanism: Legal Certainty and Legitimate Expectation' (2014) 30 Computer Law & Security Review 392

Daskal J, 'Microsoft Ireland, CLOUD Act, and International Law-Making 2.0' (2018) 71 STAN.L.REV.ONLINE9 <https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/> accessed 10 June 2021

Jia J and Zhang F, 'K-Anonymity Algorithm Using Encryption for Location Privacy Protection' (2015) 10 International Journal of Multimedia and Ubiquitous Engineering 155, 512–516

Klein S, 'First Annual Review of the EU-US Privacy Shield' (2017) 3 Eur Data Prot L Rev 512, 514

Koops B-J and Kosta E, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 Computer Law & Security Review 890

Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal 881 <https://ssrn.com/abstract=2732346>

Kuner C, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' (1 October 2010) TILT Law & Technology Working Paper No. 016/2010, Tilburg Law School Research Paper No. 016/2010, 39-41 <https://ssrn.com/abstract=1689483>

Ntouvas I, 'Exporting personal data to EU-based international organizations under the GDPR' (2019) 9 [4] *International Data Privacy Law* 272

Quelle C, 'Does the Risk-Based Approach to Data Protection Conflict with the Protection of Fundamental Rights on a Conceptual Level?' [2015] SSRN Electronic Journal <https://www.ssrn.com/abstract=2726073>

Raab CD and De Hert P, 'The Regulation of Technology: Policy Tools and Policy Actors' [2007] SSRN Electronic Journal <http://www.ssrn.com/abstract=1030263> accessed 5 May 2021

Reed C, 'Information 'Ownership' in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No. 45/2010 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461>

Van den Bulck P, 'Transfers of Personal Data to Third Countries' (2017) 18 ERA Forum 229

Wagner J, 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?' (2018) 8 International Data Privacy Law 318 <https://doi.org/10.1093/idpl/ipy008>

Zalnieriute M, 'Developing a European Standard For International Data Transfers After Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' [2018] SSRN Electronic Journal <https://www.ssrn.com/abstract=3330357>

Online Sources

International Association of Privacy Professionals (IAPP)

Fennessy C, 'New EU SCCs: A modernized approach' (*IAPP*, 13 November 2020) <https://iapp.org/news/a/new-eu-standard-contractual-clauses-a-modernized-approach/> accessed 14 April 2021

Hengesbaugh B, 'What Privacy Shield Organizations Should Do In The Wake Of 'Schrems II' (*IAPP*, 17 July 2021) <https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/> accessed 7 January 2021

Jetty T, 'What to expect on revised standard contractual clauses' (*IAPP*, 29 September 2020) <https://iapp.org/news/a/revised-standard-contractual-clauses-what-to-expect/> accessed 6 April 2021

Kamara I, '4 GDPR-certification myths dispelled' (*IAPP*, 28 January 2020) <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> accessed 14 March 2021

'Privacy 2030 A New Vision for Europe' (*Published by IAPP*, November 2019) 22 <https://iapp.org/resources/article/privacy-2030/> accessed 14 April 2021

IAPP-EY, 'Annual Governance Report 2019' (2019) <https://iapp.org/store/books/a191P000003Qv5xQAC/> accessed 14 April 2021

Maldoff G, 'White Paper – The Risk-Based Approach in the GDPR: Interpretation and Implications' (*IAPP*, March 2016) <https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/> accessed 14 March 2021

Noyb

'Judicial Review against DPC over slow procedure granted' (*noyb*, 6 July 2021) <https://noyb.eu/en/judicial-review-against-dpc-over-slow-procedure-granted> accessed 13 May 2021

'New browser signal could make cookie banners obsolete' (*noyb*, 14 June 2021) <https://noyb.eu/en/new-browser-signal-could-make-cookie-banners-obsolete> accessed 14 June 2021; See also the Advanced Data Protection Control website <https://www.dataprotectioncontrol.org/>

'noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints' (*noyb*, 31 May 2021) <https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints> accessed 5 June 2021

'Decision by Irish High Court - DPC must now implement CJEU decision and stop EU-US transfers.' (*noyb*, 13 May 2021) <https://noyb.eu/en/decision-irish-high-court-jr> accessed 13 May 2021

'Irish DPC "handles" 99,93% of GDPR complaints, without decision?' (*noyb*, 28 April 2021) <https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision> accessed 28 April 2021

‘Irish High Court allows Judicial Review to stop Facebook EU-US transfers’ (*noyb*, 12 October 2020) <https://noyb.eu/en/irish-high-court-allows-judicial-review-stop-facebook-eu-us-transfers> accessed 19 June 2021

‘Irish High Court: Judicial Review against DPC admitted’ (*noyb*, 14 September 2020) <https://noyb.eu/en/irish-high-court-judicial-review-against-dpc-admitted> accessed 3 April 2021

‘Is the DPC actually stopping Facebook's EU-US data transfers?! ..maybe half-way!’ (*noyb*, 9 September 2020) <https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way> accessed 1 March 2021

‘Irish DPC agrees to decide swiftly on Facebook's EU-US transfers’ (*noyb*, 13 January 2021) <https://noyb.eu/en/irish-dpc-agrees-decide-swiftly-facebooks-eu-us-transfers> accessed 3 April 2021

‘*noyb*'s comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679’ (*noyb*, December 2020) <https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf> accessed 24 April 2020

‘noyb approved as a “qualified entity” to file class actions in courts in Belgium’ (*noyb*, 29 octobre 2020) <https://noyb.eu/en/noyb-approved-qualified-entity-file-class-actions-courts-belgium> accessed 5 April 2021

‘Companies can't say how they comply with CJEU ruling’ (*noyb*, 25 September 2020) <https://noyb.eu/en/companies-cant-say-how-they-comply-cjeu-ruling> accessed 25 December 2020

Others

Blair T and Lawler TS, ‘Possession, Custody or Control: A Perennial Question Gets More Complicated’ *The Legal Intelligencer* (Philadelphia, 5 February 2018) <https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/05/possession-custody-or-control-a-perennial-question-gets-more-complicated/> accessed 06 January 2021

Busvine D and Humphries C ‘Facebook faces prospect of 'devastating' data transfer ban after Irish ruling’ (*Reuters*, 14 May 2021) <https://www.reuters.com/business/legal/facebook-data-transfer-ruling-irish-court-due-friday-2021-05-14/> accessed 15 June 2021

Centre for Information Policy Leadership, ‘A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision’ (September 2020) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf>

Christakis T, ‘Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)’ (*European Law Blog*, 12 April 2021) <https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/> accessed 12 April 2021

Christakis T, ‘“Schrems III”? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)’ (European Law Blog, 16 November 2020)

<https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/> accessed 23 April 2021

Cumbley R, Van Overstraeten T and Kon G, 'The Schrems judgment – Transfer Impact Assessments for international data transfers?' (*Linklaters Blogs*, 16 July 2020) <https://www.linklaters.com/en/insights/blogs/digilinks/2020/july/the-schrems-judgment> accessed 28 February 2021

European Broadcasting Union, 'International data transfers need a flexible and risk-based approach' (17 December 2020) <https://www.ebu.ch/news/2020/12/international-data-transfers-need-a-flexible-and-risk-based-approach> accessed 26 April 2021

Gömann M, 'A Hidden Revolution – Domestic Application of Foreign Public Law under the GDPR' (*Verfassungsblog*, 17 June 2021) <https://verfassungsblog.de/a-hidden-revolution/> accessed 20 June 2021

Humphries C, 'EU-U.S. data flows could face 'massive disruption' - Irish regulator' (Reuters, 25 February 2021) <https://www.reuters.com/article/uk-facebook-privacy-dixon-interview-idINKBN2AP005> accessed 20 June 2021

Hodge N, 'Reported Amazon fine ($425M) 'biggest test' of GDPR enforcement yet' (*Compliance Week*, 15 June 2021) <https://www.complianceweek.com/gdpr/reported-amazon-fine-425m-biggest-test-of-gdpr-enforcement-yet/30479.article> accessed 20 June 2021

Neil Hodge, 'GDPR priorities for 2021: Twitter ruling stresses need for harmonization' (*Compliance Week*, 22 December 2020) <https://www.complianceweek.com/gdpr/gdpr-priorities-for-2021-twitter-ruling-stresses-need-for-harmonization/29870.article> accessed 20 June 2021

Kagan O, 'Businesses Urge EU to Take Risk-Based Approach to Data Transfers' (*Foxrothschild*, 27 January 2021) <https://www.foxrothschild.com/publications/businesses-urge-eu-to-take-risk-based-approach-to-data-transfers/> accessed 28 April 2020

Koch R, 'The truth about anonymized data' (*Protonmail Blog*, 30 April 2020) <https://protonmail.com/blog/truth-about-anonymized-data/> accessed 7 May 2020

Kovacs E, 'Encrypted Services Providers Concerned About EU Proposal for Encryption Backdoors' (*Security Week*, 29 January 2021) <https://www.securityweek.com/encrypted-services-providers-concerned-about-eu-proposal-encryption-backdoors> accessed 15 February 2021

MacAskill E and Dance G, 'NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained' (*The Guardian*, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded> accessed 5 January 2021

Manancourt V and Scott M, 'What the US can teach Europe about privacy' (Politico, 10 February 2021) <https://www.politico.eu/article/europe-privacy-fines-tech-what-the-us-can-teach/> accessed 15 April 2021

Netskope INC, 'EMEA Cloud Report' (September 2016) <https://resources.netskope.com/h/i/285920664-september-2016-emea-cloud-report>

O'Neill PH, 'Barr's call for encryption backdoors has reawakened a years-old debate' (*Technology Review*, 24 July 2019) <https://www.technologyreview.com/2019/07/24/134062/trumps-justice-department-calls-for-encryption-backdoor-law/> accessed 6 May 2021

Propp K, 'Do continued EU data flows to the United Kingdom offer hope for the United States?' (Atlantic Council, 14 April 2021) <https://www.atlanticcouncil.org/blogs/new-atlanticist/do-continued-eu-data-flows-to-the-united-kingdom-offer-hope-for-the-united-states/> accessed 20 May 2021

RapidValue, 'Amazon Web Services – Ruling the Cloud' <https://www.rapidvaluesolutions.com/infographics/amazon-web-services-ruling-the-cloud/>

Sandvine, 'The Global Internet Phenomena Report' (September 2019) <https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf>

Schechner S and Glazer E, 'Ireland to Order Facebook to Stop Sending User Data to U.S.' (*Wall Street Journal*, 9 September 2020) <https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980?mtc=j> accessed 15 February 2021

Swire P, 'Testimony by Peter Swire at the U.S. Senate Commerce Committee Hearing on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows"' (*Cross-border Data Forum*, 13 January 2021) <https://www.crossborderdataforum.org/testimony-by-peter-swire-at-the-u-s-senate-commerce-committee-hearing-on-the-invalidation-of-the-eu-u-s-privacy-shield-and-the-future-of-transatlantic-data-flows/> accessed 15 May 2021

Terstegge J, 'Do we need a new GDPR?' (*Netkwesties*, 4 February 2020) <https://www.netkwesties.nl/1421/do-we-need-a-new-gdpr.htm?u%E2%80%A69-feb-2020&utm_medium=e-mail&utm_term=do-we-need-a-new-gdpr> accessed 22 May 2021

Whittingdale J, 'The UK's new, bold approach to international data transfers' (Privacy Laws & Business, March 2021) <https://www.privacylaws.com/uk114data> accessed 30 April 2021

'Surveillance Court Finds FBI Repeatedly Misused FISA Program to Conduct Unlawful Surveillance of Americans' (*Epic*, 29 April 2021) <https://epic.org/2021/04/the-foreign-intelligence-surve-1.html> accessed 4 May 2021

'European Parliament Debates the Impact of Schrems 2 on EU-US Data Transfers' (*Cooley*, 8 September 2020) <https://cdp.cooley.com/european-parliament-debates-the-impact-of-schrems-2-on-eu-us-data-transfers/> accessed 12 November 2020

Acknowledgements

I would like to thank my supervisor, Prof. Dr. Eleni Kosta, for agreeing to supervise my thesis and for her kind support. In particular, her detailed feedback and her lightning-quick answers allowed me to move forward efficiently and serenely.

I would also like to thank my reader, Dr. Irene Kamara, for her attention to this thesis and her comments.

Finally, I would like to thank all the people who supported me in this work by their encouragement and who believed in me.