**15**

# The Future of the EU-US Privacy Shield

*Elaine Fahey*
*Fabien Terpan*

*https://orcid.org/0000-0003-2603-5300*
*https://orcid.org/0000-0002-5008-9029*

**Abstract:** The invalidation of the Privacy Shield has shown how serious the CJEU was with regards to the protection of EU citizens' data. It may not have created a legal vacuum, the GDPR offering different alternative possibilities including standard contractual clauses and binding corporate rules. But it certainly has opened a phase of uncertainties and legal complexity which is not favourable to a smooth and continuous flow of data across the Atlantic. In this chapter we use soft law, defined as an act comprising a soft dimension with regard to either the obligation or the enforcement mechanism. We argued that the adequacy Decision of the Commission -a hard law act- suffers from a major weakness derived from the softness of the guarantees provided by the US government. Changes proposed resulting in the hardening of EU-US arrangements through a new Framework and with a Review Court, may dramatically evolve the partnership. Apart from the hardening of EU-US arrangements, the strengthening of US domestic rules on data protection could also contribute to the securing of transatlantic data flows through hard law legalisation line with the CJEU vision.

**Keywords:** EU-US, Soft law, Data Privacy, Privacy Shield, Transatlantic Privacy Framework, CJEU

## Introduction

Many landmarks in the history of EU-US relations date to the Transatlantic Declaration of 1990, expanded through the New Transatlantic Agenda (NTA) in 1995 (Pollack 2005, p. 900) have been in soft law instruments. Traditionally, political science accounts have contended that EU-US relations are law-light institution-light (Pollack 2005, p. 916; Fahey 2014, p. 370). To a degree, despite immense amounts of engagement, activities and cooperation, there are limited legal outcomes as a matter of international law for several decades of cooperation, before and after the NTA. There are 8 data transfer agreements, not all international agreements, some hybrid regimes, comprising an array of legal bases (Christakis and Terpan 2021). There are also many conclusions that EU-US relations have been plagued by overly complex or inadequate governance, institutions, legal agreements or enforcement (Petersmann 2015; Pollack and Shaffer 2009). Soft law and its complex enforceability, construction and classification is a thorny one. EU-US relations has contributed to many of these challenges through an evolving variety of increasingly complex, novel or simply hybrid transatlantic instruments (Shaffer 2002).

Data transfer between the European Union (EU) and the United States (US) is an important issue given the extent of transatlantic business relationship. However, the degree of data protection and privacy afforded by the EU and the US is quite different, with EU law being far more protective than US law. This does not mean that data transfer is impossible, but at least from a European perspective, it means that a solution needs to be found in order to make data transfer compatible with EU law. From a US perspective, this can be seen as an EU requirement of approximation to European law, which is, of course, highly problematic for both legal and political reasons.

The European Commission and the US administration negotiated two different arrangements aimed to protect the fundamental rights of EU citizens whose personal data is transferred to the United States for commercial purposes, and thus facilitating data flows across the Atlantic. The main purpose of these

arrangements was to allow the free transfer of data to US companies provided that the latter had received a proper certification. Both arrangements were enshrined in EU law by an 'adequacy decision' adopted by the European Commission on the basis of the EU legislation on data protection, a form of complex hybrid governance.[1]

The first arrangement, called Safe Harbour, was endorsed by the European Commission in a Decision of 26 July 2000.[2] In the Case of *Schrems v. European Data Commissioner* (C-362/14)[3] (hereafter Schrems I), the Court of Justice of the European Union (CJEU) issued a preliminary ruling declaring the adequacy decision invalid. This decision forced the EU and the US to negotiate urgently a new framework capable of securing transfer of data from Europe to the US, the so-called Privacy Shield, which came into force in July 2016, based on a Commission new adequacy decision of 12 July 2016.[4] The new framework was supposed to address the issues raised by the Court of justice. This was immediately followed by judicial actions against the Privacy Shield, in the form of actions for annulment brought before the General Court of the CJEU (T-670/16 and T-738/16) and preliminary references.[5] This judicial phase culminated in a recent CJEU judgment (C-311/18)[6] (hereafter Schrems II) invalidating it.

In a previous article we argued that the invalidation of the EU-US arrangements by the CJEU can be explained by a lack of institutionalization, the latter being defined as 'the process by which an organisation becomes increasingly subject to rules, procedures and stable practices' (Fahey and Terpan 2021). Our main argument was that because institutionalisation through EU-US arrangements is weak or informal, negative judicialisation (invalidation of the Safe Harbour and the Privacy Shield) is more likely, with courts and tribunals of the most protective legal order –in the end the CJEU- are prone to make their own rules prevail.

In the present article, we go one step further by focusing on the very nature of the rules established between the EU and the US, in order to discuss the degree of normativity that is required to make the arrangement stable and protected from another invalidation by the CJEU. Based on previous research on soft and hard law (Terpan 2015; See also: Saurugger and Terpan 2021), we argue that norms can be situated on a continuum, from non-legal norms to proper hard law, with in-between an array of different kinds of soft norms. While this idea of a continuum goes against a clear-cut classification in the three categories -non-legal norms, soft law and hard law- it remains useful to situate those norms on the continuum in order to explain, at least partially, their efficiency, or lack thereof.

The identification of soft law is based on two main criteria, obligation and enforcement. Obligation relates either to the act intself -the *instrumentum*- or to the content of the act -the *negotium*. A legally binding act such as a Treaty is considered hard, whereas a non-legally binding act such as a memorandum of understanding or a common declaration between two parties is at most soft law. When looking within the act, two kinds of provisions can be distinguished, those who contain proper commitments and those who are written in a way that soften their content. The second criteria, enforcement, makes the evaluation even more complex. Indeed, the soft-hard continuum also depends on the way the obligation -soft or hard- is enforced. Enforcement, here, is defined in a broad manner, going from soft forms (monitoring, peer review) to harder ones (judicial control).

In the context of this article, we assume that the stability of the EU-US data transfer arrangement is dependent on its legal characteristics. The stronger the commitments and the enforcement mechanism, the lower the probability that the arrangement is invalidated. Drawing on this, we discuss whether a hardening of the common rules and mechanisms could help to frame and stabilize the transfer of data between the European Union and the United States. For this, we will come back to the Safe Harbour and the Privacy Shield, in a first section, to get a clear view of why these arrangements were deemed inadequate. A second section will explain the situation created by the ruling in Schrems II while a third one will explore the possible evolutions of the data transfer regime, considering the on-going discussions between EU and US authorities, and the perspective of stronger commitments and mechanisms. Finally, a fourth section will study the current debate over US state and federal privacy law, as it could affect the EU-US relationship.

## 1. Why previous regimes were not seen as "essentially equivalent" to EU data protection law: the Safe Harbour and Privacy Shield agreements fragilities

The Safe Harbour was an EU-US arrangement setting up a series of principles and rules endorsed by US authorities. On the basis of the GDPR, it was considered "essentially equivalent" to EU data protection law by the European Commission in its adequacy decision of 26 July 2000. The essence of the Safe Harbour was to require US companies to treat the data of EU citizens as if the data were physically in Europe, operating through a voluntary self-certification system with public enforcement conducted by the US Federal Trade Commission.

The Safe Harbour Agreement was understood at the time of its adoption to amount to a new form of mutual recognition or new form of global engagement through complex governance (Shaffer 2002) and capable of being understood in a variety of ways. Shaffer famously summed up the Agreement as being understood to be anything from the EU's exercise of coercive market power in an extraterritorial fashion in an attempt to leverage up privacy standards within the United States, a capitulation by EC bureaucrats to U.S. trading concerns through a weak agreement filled with loopholes or a compromise through new institutional development pursuant to which free transatlantic information flows could be preserved while satisfying legitimate European concerns (Shaffer 2002).

The Safe Harbour Agreement was poorly institutionalised, and suffered legal weaknesses that led to its inevitable invalidation by the CJEU (negative judicialization). This can be further explained by the (soft law) nature and structure of the relationship (Kuner 2017). The only binding and enforceable element in the Safe Harbour was the adequacy decision made by the European Commission on 26 July 2000.[7] Apart from this, the Safe Harbour was made of a series of soft law documents whereby US authorities gave assurances to the EU and to which the adequacy decision referred. Negative judicialisation has then triggered the adoption of the Privacy Shield, which was presented as a strengthened and more institutionalised version of the Safe Harbour but which was in reality mostly weakly institutionalised masked by new terminology, some enhanced governance but little else.

### 1.1. The Privacy Shield: still a soft law arrangement

The soft dimension of the Privacy Shield is obvious when looking at the content of the arrangement.

First, the Privacy Shield replicates the structure of the Safe Harbour, with one legally binding decision of the Commission referring to a series of informal letters addressed by US authorities to the European Union. No real legal guarantees are provided in these letters. The Privacy Shield is not an external agreement based on Article 218 TFEU including mutual commitments. Thus, the first criterion of soft law (lack of obligation) is clearly met in all documents pertaining to the Privacy Shield, with the exception of the Commission's adequacy decision.

Secondly, a strengthened monitoring of the framework has been established by the 2016 adequacy decision of the Commission, with annual joint reviews by EU and US authorities to monitor the correct application of the arrangement discussed next, and a public report to be submitted by the Commission to the European Parliament and the Council. The first review took place in Washington, DC on 18 and 19 September 2017, the second on 18 and 19 October 2018 in Brussels and the third in Washington on 12 and 13 September 2019. This review process was established in order to address the issue raised by the Court in Schrems I about the weaknesses of the assessment made by the EU Commission. Indeed, under the Safe Harbour, the Commission did not directly and continuously assess the adequacy of US rules but mostly relied on self-assessment by US authorities. In contrast to this, the annual reviews under the Privacy Shield have led to the adoption of three reports, published by the Commission in 2017, 2018, and 2019[8]: the Commission was not fully dependent on declarations made by US authorities when itself evaluating the framework. However, although the review process is an improvement, this does not change the fact that the adequacy in itself mainly depends on evolutions in US law and practices. The Commission cannot go beyond recommendations to US authorities and is dependent on the latter's willingness to respond to these demands.

Thirdly, the guarantees provided by US law were supposed to be stronger on both commercial and surveillance aspects of the Privacy Shield; in fact, the hardening of soft law was rather limited, or even fake.

The ostensibly 'light-touch' enforcement practices of the Federal Trade Commission indicated only limited formalisation of the guarantees. Commercial providers were not subject to meaningful infrastructures.[9] As to surveillance, the embryonic role of the now permanent Ombudsman and newly constituted PCLOB indicated further layers of oversight and accountability being put in place- slowly but surely, and in embryonic form. However, the Ombudsman mechanism did not provide for the necessary limitations and safeguards with regard to the interferences authorised by the U.S. legislation[10] and did not ensure effective judicial protection against such interferences. There was no real improvement in terms of effective administrative and judicial redress for the data subjects whose personal data are being transferred.

In the end, both the monitoring of the Privacy Shield and the guarantees offered by US authorities can be seen as a very soft enforcement mechanism (our second criteria), confirming the soft law nature of the arrangement. The only hard law component -the adequacy decision- is thus weakened by the softness of the arrangement and of the US guarantees, a situation which inevitably led to negative judicialization.

### 1.2. The Privacy Shield is subject to negative judicialisation

The CJEU, in the Case of *Schrems* II, held that the Commission's finding that US law was of an adequate level of protection essentially equivalent to EU law under the GDPR read in light of the Charter, was called into question by section 702 FISA and E.O. 12333 because they authorised surveillance programmes such as PRISM and UPSTREAM. FISA did not indicate limitations on powers and E.O. did not confer enforceable rights on EU citizens against the US authorities. This violated the principle of proportionality because surveillance programmes could not be regarded as limited to what was strictly necessary. Moreover, Ombudsman could not remedy deficiencies which the Commission had found (e.g. lack of a redress mechanism) as to the transfers impugning findings as to adequacy with respect to essential equivalence as guaranteed by Article 47 of the Charter.

The decision was not just exclusively about US surveillance laws but was also about the fragile nature of the Privacy Shield architecture. The lack of a robust institutional framework here overall was of salience to the CJEU as well as from the lack of truly legal guarantees provided by US authorities.

Since the European Charter of Fundamental Rights has become binding and the GDPR entered into force, the CJEU acquired solid legal grounds to exert a judicial control over the Privacy Shield. Therefore, it was unlikely that a a limited hardening of the EU-US framework could prevent negative judicialisation. This was confirmed by the CJEU landmark ruling in the Case of *Schrems* II.

## 2. Post-*Schrems* II: a period of high uncertainties

### 2.1. No legal vacuum but a legal mess

The Court's ruling in *Schrems* II has opened a new period of uncertainties (Christakis 2020a). Once again, the EU-US relationship has been destabilized, with important consequences for business transatlantic relations. 5300 companies, which used to rely on the Privacy Shield, need to find other ways to transfer data from Europe to the US, while the flow of data underpins 900 billion euros in cross-border commerce every year. The issues raised by *Schrems* II are even more significant that no grace period has been allowed for Privacy Shield transfers, contrary to what had been decided after *Schrems* II (EDPB 2020a). At the very least EU Data Protection Authorities could slow-roll enforcement, giving companies time to figure out how to respond, as they did when Safe Harbor was invalidated (Daskal 2020). But companies cannot rely on the existing framework until a new arrangement is adopted.

As the CJEU made clear in *Schrems* II, the invalidation did not create a legal vacuum and the absence of an adequacy decision is clearly foreseen by article 49 GDPR[11] However, this article is supposed to cover a limited number of specific situations. A transfer is possible under article 49 under specific conditions such as:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
-

Obviously, article 49 is not supposed to replace a general arrangement between the EU and a third state, which the EDPB had made it clear (2018). The remaining options are to be found in article 46 and 47 of the GDPR.

In the absence of an adequacy decision 'a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available' (Art. 46-1 GDPR). These appropriate safeguards, according to Art. 46-2 GDPR, may be provided for by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
-

Among the list of safeguards, two main options are more likely to be used: standard contractual clauses and binding corporate rules (see also article 47 GDPR).[12] In our views both options pose serious challenges.

### 2.2 Standard Contractual Clauses and Binding Corporate Rules

Data transfers from the EU to other countries, including the US, can be based on contractual clauses ensuring appropriate data protection safeguards. This includes model contract clauses, the so-called standard contractual clauses (SCCs), that have been "pre-approved" by the European Commission. The last version of the SCCs has been approved by the Commission on 4 June 2021 (European Commission 2021a).

The Court in S*chrems* II has clearly indicated that the SCCs remain valid provided that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the EU Charter. This responsibility falls primarily to the exporter, who need to 'verify whether the law of the third country of destination ensures adequate protection under EU law' (Para 134) and 'whether the level of protection required by EU law is respected in the third country concerned' (Para 142). The Court adds that the adequacy assessment by private companies is placed under the control of DPAs, who have the power to terminate the transfer (Para 146), a power that does not seem so easy to exert. If DPAs disagree on the adequacy of foreign law to EU law, then it is the EDPB, and not the

Commission, who is charged of solving the problem (Para 147). This confirms a tendency towards agencification that can be observed in other areas of EU law. To provide guidance on how to assess the adequacy of foreign law, the EDPD has issued a "Recommendation on the European Essential Guarantees for surveillance measures" (2020c), which should not make data transfer easier given the extent of what is required (Christakis 2020b; 2020c; 2020d). Overall, all this process is obviously time consuming and supposes that different actors, private companies and public agencies, should make a difficult assessment of foreign law.

Whatever we think about the workability of this complex system of adequacy assessment, the problem is that the CJEU, in S*chrems* II, has just said that the US level of protection is not essentially equivalent to EU law. How could SCCs be considered as "essentially equivalent" in a context where the Privacy Shield was invalidated and US law has not been genuinely transformed? Two main answers are possible. If all types of data are potentially subject to the US surveillance programmes under US Foreign Intelligence Surveillance Act Section 702, Executive Order 12333 and Presidential Policy Directive 28, then transferring data on the basis of SCCs is not legal. If, on the contrary, those programmes are limited to communication service providers and do not concern the data transferred by other types of companies, then SCCs would be an option for the latter but not for the former.

In *Schrems* II, the CJEU mentions the possibility for the controller or processor to provide 'additional safeguards' to those offered by the SCC (Para 134). This has given rise to much skepticism? Even the EDPB at first did not seem to know what exactly these measures could be,[13] before finally adopting a recommendation aimed at clarifying the notion (2020b).

Discussing the possible legal or technical nature of these measures, Christakis argues that 'If one considers, for instance, that one of the main concerns of the Court was that the US system of surveillance does not offer effective judicial remedies to EU citizens, it is hard to imagine how any "additional safeguards" introduced by the data controller could change this' (2020a).

Given the uncertainties of the SCCs, would the Binding Corporate Rules (BCR) (Bender and Ponemon 2006; Proust and Emmanuelle 2011; Moerel 2012) be the optimal solution to legally transfer data from Europe to the US? Article 47(1) GDPR says that 'The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they: are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; expressly confer enforceable rights on data subjects with regard to the processing of their personal data'. A list of what the BCRs should at least specify is laid down in Article 47(2).

BCRs brings legal certainty as it is approved a priori by the competent supervisory authority. However, companies might not have the necessary means to engage in the costly and time-consuming establishment of BCRs. And, in the end, BCRs are facing the same problem as SCCs: they could prove useless in a context where the US law still does not meet the European standards.

The *Schrems* II ruling may not have created a legal vacuum, but it certainly has led to a legal mess, with an even weaker legal framework than before, as the system of certification provided by the Privacy Shield is no longer applicable, and a still high risk of negative judicialization. Negative judicialization could become even more fragmented, due the diversity of data transfer mechanisms and the uncertainties that was created. Based on its detailed assessment of *Schrems* II, the EDPB has been trying to provide further clarification for stakeholders and guidance on the use of instruments for the transfer of personal data to third countries pursuant to the judgment. But the capacity of the EDPB to bring more coherence and certainty to the system is questionable and its contribution in terms of adequacy assessment could probably be challenged before the CJEU under Article 263 TFEU. This is why the negotiation of third arrangement -Privacy Shield 2.0- has finally been put on agenda by EU and US authorities.

**3. Towards Privacy Shield 2.0: What could the Privacy Shield 2.0 include, and will it be enough?**

Political changeover in the US has brought to power a new administration, more concerned with strengthening the transatlantic relationship than the previous one, and more engaged with data arrangements at international level.

The current US Trade Representative has made it clear that trade agreements are from a previous century and not in line with the Biden administration philosophy that soft law framework agreements constitute the future of international economic law. For instance, the Indo Pacific Economic Partnership (IPEF) of which the US is party to amongst others in the Indo Pacific region has many outline objectives on data flows and data localization and the digital economy across borders using soft law as its main framing device.

The agreement perceived by many to be the most contemporary and cutting-edge digital governance trade agreement is also a soft law non-binding partnership, the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, Singapore 2020.[14] It is not formulated as a trade agreement but rather intended to address the broader issues of the digital economy through a soft law agreement. Its breadth and flexibility are significant in so far as it purported to traverse a range of contemporary challenges issues, such as those in the areas of artificial intelligence (AI) and digital inclusion.

DEPA's 'soft' approach to rulemaking and norm-setting is alleged to have been effective in an Asian context, ie Asia-Pacific Economic Cooperation (APEC) forum (including on digital governance) and worthy of replication. To enable shaping rules and norms in this critical area has in this context appears more significant and efficient to lengthy trade agreement negotiations (Goodman 2021). Yet such a framework contrasts considerably with the very different type of debate taking place across the Atlantic in the context of the post-Privacy Shield negotiations, reaching an agreement on the transatlantic privacy framework which includes a binding transatlantic court, to deal with the complex question of high standards and international data flows.

We know that the CJEU did not take a principled position against surveillance, but rather required safeguards and remedies, which leaves room for negotiation. What we do not know, however, is the exact mechanism and practice which could, for sure, avoid a new invalidation.

A Transatlantic Trade and Technology Council, as proposed by the EU in late 2020 and already in place by Autumn 2021, could provide an important bedrock from which important data privacy agreements evolve (European Commission 2021b; Bown and Malmström 2021). The EU-US Joint Agenda for Global Change included a Transatlantic Trade and Technology Council, putatively developing a loose institutionalisation of key global challenges currently not well covered by, for example, the WTO, including data transfers. It is difficult to determine precisely what level of institutionalisation is needed bilaterally, never mind bilaterally. The Council is a soft governance entity, derived from a non-binding agreement. It is a formula that the EU increasingly uses eg with India, where a new EU-India Trade and Technology Council was similarly established as a soft law arrangement in the absence of an international law agreement framework pursuant to Article 218 TFEU (European Commission 2022b). Thus although relating more broadly to digital governance, it is a notable trend in the era of digitisation.

In March 2022, Ursula Von der Leyen and Joe Biden has announced that the EU and the US had reached an agreement in principle for a new Trans-Atlantic Data Privacy Framework on the basis of which data will be able to flow freely and safely between the EU and participating U.S. companies. It is a remarkable development which seems to elevate the plan of institutions in the protection of rights of citizens and businesses.

This agreement will contain "a new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security" (European Commission 2022a). In this context, "US intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards" (European Commission 2022a). The agreement also includes "a new two-tier redress system to investigate and resolve complaints of Europeans on

access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court" (European Commission 2022a). The White House has made it clear in a Briefing released on 25 March 2022 that "the United States has made unprecedented commitments to: Strengthen the privacy and civil liberties safeguards governing U.S. signals intelligence activities; Establish a new redress mechanism with independent and binding authority; and Enhance its existing rigorous and layered oversight of signals intelligence activities" (2022). The White House also stresses out that, under the New Framework, signals intelligence collection may be undertaken "only where necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties" (2022). EU individuals may seek redress from a new multi-layer redress mechanism "that includes an independent Data Protection Review Court that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed" (The White House 2022). Regarding commercial aspects, the mechanism will continue to rely on the requirement for companies to self-certify their adherence to the Principles through the U.S. Department of Commerce, but there will be strong obligations for companies processing data transferred from the EU. In addition, the agreement should foresee Specific monitoring and review mechanisms.

It might not be easy to precisely evaluate the nature of the proposed and published mechanisms, but the new set of rules are clearly presented as being more binding and accompanied with stronger enforcement, resulting in a hardening of the EU-US data protection framework. We know for sure that soft arrangements, based on merely declaratory and loose commitments, entail a strong risk of negative judicialization in all areas where judicial scrutiny is possible. We also know that US cannot fully align with EU law. But But the idea was to include U.S. commitments in an Executive Order that will form the basis of a draft adequacy decision by the Commission to put in place the new Trans-Atlantic Data Privacy Framework. Accordingly, on 7 October 2022, President Biden signed Executive Order 'enhancing safeguards for United States signals intelligence activities', which along with Regulations issued by the Attorney General implemented into US law the agreement in principle announced in March 2022 (US Government, 2022). It purported to issue new binding safeguards to address all issues raised by the CJEU, in particular allegedly binding safeguards, a first instance Civil Liberties Protection Officer and Data Protection Review Court, as a means to procure an adequacy decision. It should be welcome by the European Commission, who was at pains to indicate that standard contractual clauses still were possible for businesses to use, although the breadth and depth of the hardening of soft law here remains problematic (European Commission 2022).

At the time of writing, doctrinal analyses try to figure out how the new US measures could meet the requirements of *Schrems* II. Christakis, Propp and Swire, in particular, have discussed the sensitive issue of the Redress mechanism (2022a; 2022b). But it will only be possible to more accurately assess the Privacy Shield 2.0 and its adequacy to European standards once it has been transformed into legal documents, before the CJEU is eventually called upon to do so. A significant legalisation of soft law governance may yet occur and align further with the CJEU vision.

**4. Could the transatlantic privacy relationship be facilitated by US domestic changes?**

Apart from a strengthened EU-US framework, the relationship between the EU and the US could be facilitated by an evolution of US data protection laws. Several US states have recently adopted the GDPR de facto if not de jure, demonstrating the force of EU rules and values, which may generate further instititutionalisation pressures outside of the EU (Frankenreiter 2021; Fahey 2022).

Currently, three states in the US have three different comprehensive consumer privacy laws: California (CCPA and its amendment, CPRA), Virginia (VCDPA), and Colorado (ColoPA). Since 2019, a bipartisan data privacy agreement in the US has been faltering between Democrats and Republicans on two key issues. Firstly, whether a federal bill should preempt state privacy laws, and (2) whether it should create a private right to action allowing individuals, not just the government, to sue companies

for violations. Members of the U.S. Congress appear to be likely to realise the finalisation of comprehensive federal privacy legislation in 2022. On July 20, 2022, the House Committee on Commerce & Energy (House Committee) published an amended version of the American Data Privacy and Protection Act (ADPPA) (H.R. 8152) (Kern 2022; Kerry 2022; Linn 2017). The ADPAA will reshape web use and overhaul data laws beyond the U.S in how business and organization can handle customer and user information. It is one of the most significant regulations overseeing data-collection practices in the United States. It is first Act of its ilk and is projected to provide thorough, comprehensive data privacy measures in the US. One of the most distinctive features of the new bill is its focus upon data minimization. This principle holds that the data controller shall limit the collection of personal information to only what is relevant and necessary to achieve the ascertained purpose.

A notable caveat is that the list of permitted purposes spelled out in the bill includes targeted advertising, which is the economic driver of most surveillance to begin with. If the bill in its current form becomes law, it would be insufficient in preventing target advertising which is contrary to what data privacy advocates have been advocating. However, it imposes much tougher restrictions on targeted advertising than any legislation in the U.S. and perhaps the world and would prohibit targeting ads to minors and targeting ads based on 'sensitive data' eg medical information, precise geolocation, and private communications—as well as 'information identifying an individual's online activities over time and across third-party websites or online services.' To the extent that the new bill would still allow targeted advertising, it would require companies to give users the right to opt out. It would confer upon the Federal Trade Commission (FTC) powers to create a standard for a universal opt-out that businesses would have to comply with, meaning users could decline all targeted advertising in one click. In addition to the ADPAA's take on data-minimization, the new bill contains provisions that data privacy experts have long called for, including transparency standards, anti-discrimination rules, increased oversight for data brokers, and new cybersecurity requirements.

Since the House Committee has introduced the ADPPA bill, it is said to be notable that the tech industry has not expressed significant dissent as to the bill possibly indicative of the bill's weaknesses. The bill gives the FTC new authority to issue rules and enforce them, but it doesn't direct any new resources to the agency raising concerns as to an enforcement deficit. The ADPPA appears to align well with consensus emerging on many fronts- bipartisanship and among advocacy organizations, a consensus that bodes well for the bill if and / or when the full House votes on it.

**Conclusions**

The invalidation of the Privacy Shield has shown how serious the CJEU was with regards to the protection of EU citizens' data. It may not have created a legal vacuum, the GDPR offering different alternative possibilities including standard contractual clauses and binding corporate rules. But it certainly has opened a phase of uncertainties and legal complexity which is not favourable to a smooth and continuous flow of data across the Atlantic.

In this chapter we used the notion of soft law, defined as an act comprising a soft dimension with regard to either the obligation or the enforcement mechanism. We argued that the Adequacy Decision of the Commission -a hard law act- suffers from a major weakness derived from the softness of the guarantees provided by the US government.

Could these guarantees be sufficiently strengthened / hardened to avoid any possible invalidation by the CJEU in the future? The EU-US relationship has further developed since the election of Joe Biden as president, including in the area of data privacy. A Transatlantic Trade and Technology Council has been created and an agreement in principle has been found in March 2022 for a new Trans-Atlantic Data Privacy Framework. It is too soon to precisely evaluate the new set of rules included in the Framework, but the trend is clearly towards more binding rules and stronger enforcement, which can be seen as a move towards hard law.

Besides, apart from the hardening of EU-US arrangements, the strengthening of US domestic rules on data protection could also contribute to the securing of transatlantic data flows. While several US states have brought their own legislation closer to GDPR standards, it remains to be seen whether such an evolution could occur at federal level. The deepening and widening of legal cooperation beyond soft law thus appears to be a salient metric of the transatlantic partnership- for now at least, given that it constitutes one of the world's most complex global governance, economic and legal structures.

**References**


Aaronson, S. 2021. The One Trade Agreement Biden Should Sign Up For Now [online]. 8 March. *Barron's.* https://www.barrons.com/articles/the-one-trade-agreement-biden-should-sign-up-for-now-51614607309 [Accessed 30 September 2022].

Bender, D. and Ponemon, L. 2006. Binding Corporate Rules for Cross-border Data Transfer. *Rutgers Journal of Law & Urban Policy*, 3(2), 154-171.

Bown, C. P. and Malmström, C. 2021. What is the Transatlantic Trade and Technology Council [online]. 24 September. *PIIE*. https://www.piie.com/blogs/trade-and-investment-policy-watch/what-us-eu-trade-and-technology-council-five-things-you-need [Accessed 30 September 2022].

Burri, M. 2021. Towards a New Treaty on Digital Trade. *Journal of World Trade*, 55(1), 77–100.

Christakis, T. 2020a After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe [online]. 21 July. *European Law Blog*. https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ [Accessed 30 September 2022].

Christakis, T. 2020b. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1) [online]. 13 November. *European Law Blog*. https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ [Accessed 30 September 2022].

Christakis, T. 2020c. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2) [online]. 16 November. *European Law Blog*. https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ [Accessed 30 September 2022].

Christakis, T. 2020d. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3) [online]. 17 November. *European Law Blog*. https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ [Accessed 30 September 2022].

Christakis, T. and Terpan, F. 2021. EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options. *International Data Privacy Law*, 11(2), 81-106.

Christakis, T. Propp, K. and Swire, P. 2022a. EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution [online]. 31 January. *European Law Blog*. https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/ [Accessed 30 September 2022].

Christakis, T. Propp, K. and Swire, P. 2022b. EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers [online]. 16 February. *European Law Blog*. https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers/ [Accessed 30 September 2022].

Daskal, J. 2020. What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers [online]. 17 July. *Just Security*. https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/ [Accessed 30 September 2022].

European Commission. 2021a. *European Commission adopts new tools for safe exchanges of personal data* [online]. Press release, 4 June. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847 [Accessed 30 September 2022].

European Commission. 2021b. EU-US Trade and Technology Council Inaugural Joint Statement (Pittsburg Statement) [online]. Press Release. 29 September. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951 [Accessed 30 September 2022].

European Commission. 2022a. *Trans-Atlantic Data Privacy Framework*. March. https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 [Accessed 30 September 2022].

European Commission. 2022b. EU-India: Joint press release on launching the Trade and Technology Council [online]. Press Release. 25 April. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2643 [Accessed 30 September 2022].

European Data Protection Board (EDPB). 2018. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 adopted on 25 May 2018.*

European Data Protection Board (EDPB). 2020a. European Data Protection Board publishes FAQ document on CJEU judgment C-311/18 (Schrems II) [online], https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en [Accessed 30 September 2022].

European Data Protection Board (EDPB). 2020b. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en [Accessed 30 September 2022]

European Data Protection Board (EDPB). 2020c. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en [Accessed 30 September 2022].

Fahey, E. 2014. On The Use of Law in Transatlantic Relations: Legal Dialogues Between the EU and US. *European Law Journal*, 20(3), 368-384.

Fahey, E., and Terpan, F. 2021. Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield. *Indiana Journal of Global Legal Studies*, 28, 205-244.

Frankenreiter, J. 2021. The Missing 'California Effect' in Data Privacy Law. Washington University in St. Louis Legal Studies Research Paper No. 21-07-01.

Goodman, M. 2021. DEPA and the Path Back to TPP [online]. 15 July. *CSIS*. https://www.csis.org/analysis/depa-and-path-back-tpp [Accessed 30 September 2022].

Kern, R. 2022. Bipartisan draft bill breaks stalemate on federal data privacy negotiations. 3 June. *Politico.* https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092 [Accessed 30 September 2022].

Kerry, C. 2022. The FTC Ups the Ante for Federal Privacy Legislation. 26 August. *Lawfare Blog.* https://www.lawfareblog.com/ftc-ups-ante-federal-privacy-legislation. [Accessed 30 September 2022].

Kuner, C. 2017. Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18(4), 881-918.

Kuner, C. 2020. The Schrems II judgment of the Court of Justice and the future of data transfer regulation [online]. 17 July. *European Law Blog*. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ [Accessed 30 September 2022].

Linn, E. 2017. A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement. *Vanderbilt Law Review*, 50, 1311-1358.

Moerel, L. 2012. *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers.* Oxford: Oxford University Press.

Petersmann, E.-U. 2015. 'Transformative Transatlantic Free Trade Agreements without Rights and Remedies of Citizens?. *Journal of International Economic Law*, 18, 579-607.

Pollack, M. 2005. The New Transatlantic Agenda at Ten: Reflections in an experiment in International Governance. *Journal of Common Market Studies*, 43, 899-919.

Pollack, M. and Shaffer, G. 2009. *When Cooperation Fails: The International Law and Politics of Genetically Modified Foods*. Oxford: Oxford University Press.

Proust, O. and Emmanuelle, E. 2011. Les Binding Corporate Rules: une solution globale pour les transferts internationaux. *Lamy droit de l'immatériel*, 74, 97-102.

Saurugger, S. and Terpan, F. 2021. Normative Transformations in the European Union: on Soft and Hard Law. *West European Politics*, 44 (1), 1-20.

Shaffer, G. 2002. Managing U.S.-EU Trade Relations Through Mutual Recognition and Safe Harbor Agreements: 'New' and 'Global' Approaches to Transatlantic Economic Governance?. *Columbia Journal of European Law*, 9, 29-77.

Terpan, F. 2015. Soft Law in the European Union - The Changing Nature of EU Law. *European Law Journal*, 21(1), 68-96.

The White House. 2022. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. 25 March. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ [Accessed 30 September 2022].

[1] The adequacy decisions on the Safe Harbour and the Privacy Shield were based on Art. 25 of the 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; Article 25 of the Directive provided that Member States would prohibit all data transfers to a third country if the Commission did not find that they ensured an adequate level of protection.

[2] Commission Decision of July 26, 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, 2000/520/EC, O.J.(L 215) 7.
[3] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.
[4] Commission Implementing Decision (EU) 2016/1250 of July 12, 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 O.J. (L 207) 1.
[5] Case T-670/16 - Digital Rights Ireland v. Commission; Case T-738/16 La Quadrature du Net and Others v. Commission.
[6] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145.
[7] Commission Decision of July 26, 2000, *op. cit.*
[8] European Commission. *Report From the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield*. SWD (2017) 344 final; European Commission. *Report From the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU–U.S. Privacy Shield.* SWD(2018) 497 final; European Commission. *Report From the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU–U.S. Privacy Shield*. SWD (2019) 390 final; See also European Commission. *EU-US data transfers* [online]. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en. [Accessed 30 September 2022]. These reports are based on the discussions held during the annual review but are also informed by a study commissioned by the Commission, which takes into consideration publicly available material, such as: court decisions; implementing rules and procedures of relevant U.S. authorities; annual reports from independent recourse mechanisms; transparency reports issued by Privacy Shield-certified companies through their respective trade associations; reports and studies from NGOs active in the field of fundamental rights and in particular digital rights and privacy; press articles and other media reports. In addition to the collection of written input, and prior to the annual reviews, the Commission had meetings with industry and business associations and with non-governmental organisations.
[9] As far as the commercial dimension was concerned, they included stricter obligations on certified companies receiving personal data from the EU, regarding limitations on how long a company may retain personal data (data retention principle) or the conditions under which data can be shared with third parties outside the framework (accountability for onward transfers principle). Citizens rights are intended to be better protected through information rights, enforceable at national level. DPAs acquired much more significance, whereas US enforcement rested largely with the FTC and appears to strike an imbalance overall through divergent and disparate institutionalisation and enforcement. The DoC provided more regular and rigorous monitoring and EU citizens had enlarged possibilities to obtain redress.
[10] Annex VI to the Privacy Shield Decision contained a letter from the Office of the Director of National Intelligence to the United States Department of Commerce (DoC) and to the International Trade Administration from 21 June 2016, in which it is stated that PPD 28 allowed for '"bulk" collection of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target to focus the collection. Similarly, other NSA's activities and surveillance programmes can be based on Executive Order 12333 (E.O. 12333).
[11] It noted in para. 15: 'Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.' See also para. 202.
[12] Kuner argues though that codes of conduct and certification 'seem worthy of investigation as potentially a new way forward'. See Kuner 2020.
[13] 'The EDPB to is looking further into what these additional measures could consist of', said Andrea Jelinek, Chair of the EDPB, in her Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July 2020.
[14] For details and the text of the DEPA, see: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/ [Accessed 30 September 2022]. See also Burri 2021; Aaronson 2021.