ARTICLES

EU-US DATA TRANSFER FROM *SAFE HARBOUR* TO *PRIVACY SHIELD*: BACK TO SQUARE ONE?

FABIEN TERPAN*

TABLE OF CONTENTS: I. Introduction. – II. From *Safe Harbour* to *Privacy Shield*: EU-US data transfer as a feedback loop. – II.1. Action: *Safe Harbour* and the first agreement on EU-US data transfer. – II.2. Effect: *Safe Harbour* invalidated by the CJEU in *Schrems*. – II.3. Feedback: *Safe Harbour* replaced by *Privacy Shield*. – III. *Privacy Shield*: non compliance, full or partial compliance? – III.1. Slightly improved protection of personal data. – III.2. Persistent shortcomings. – IV. Why only partial compliance? – IV.1. Reasons why non-compliance was not an option. – IV.2. Reasons why full compliance was not possible. – V. Conclusion.

ABSTRACT: This *Article* focuses on data transfer from the European Union to the United States, and compares the new EU-US legal framework (*Privacy Shield*) with the former one (*Safe Harbour*), which was invalidated by the CJEU in the case of *Schrems* (judgement of 6 October 2015, case C-362/14). It combines legal analysis with a more political perspective taking into account the wider context in which these decisions were taken. This allows us to see whether the CJEU is able to ensure compliance with EU law, and EU fundamental rights in particular, in a sensitive area of external relations. It also brings some insights to bear on normative change, or the lack thereof, in fields where external relations and EU politics are intertwined. The conceptual model of the feedback loop is used to analyse the evolution from the *Safe Harbour* to the *Privacy Shield* regime. The action (adoption of *Safe Harbour* in 2000) has provoked an effect (the *Schrems* ruling adopted by the Court in response to the demands of data protection activists), which has finally led to feedback (adoption of *Privacy Field* in 2016). A legal analysis of this feedback effect shows that *Privacy Shield* only partially complies with the *Schrems* ruling. This partial compliance can be explained both by normative constraints and actors' preferences.

KEYWORDS: *Safe Harbour* – *Privacy Shield* – data protection – EU-US relations – data transfer – compliance.

* Senior Lecturer in Public Law and European Studies, Sciences po Grenoble, Univ. Grenoble Alpes, Centre for the study of international security and European cooperation (CESICE), Jean Monnet Chair, fabien.terpan@iepg.fr.

I. Introduction

On 2 February 2016, the United States and the European Union agree on a new regime for the transfer of personal data over the Atlantic.[1] The so-called *Privacy Shield* becomes part of the EU legal order thanks to a decision made by the Commission on 12 July 2016.[2]

Two main logics are accommodated: the economic logic aimed at allowing businesses to transfer data and at providing legal certainty to these operations; and the fundamental rights logic whereby EU citizens' personal data must not be unduly processed in the United States, a country where personal data is less protected than in Europe.

Privacy Shield is not the first transatlantic regime to deal with data transfer as it takes over from *Safe Harbour*, which was enacted by a Commission decision dating back to 26 July 2000.[3] The evolution, from *Safe Harbour* to *Privacy Shield*, was triggered by a CJEU ruling of 6 October 2015,[4] which invalidated the old legal regime which dealt with transatlantic data transfer. To a large degree, *Privacy Shield* can be understood as an attempt by EU political institutions to respond to a ruling made by the EU judiciary to better protect EU citizens' personal data *vis-à-vis* a third state.

This *Article* aims to analyse the EU's reaction to the *Schrems* ruling to assess whether the guarantees provided to EU citizens by *Privacy Shield* match the demands of the CJEU in view of *Schrems*. I will argue that this is not really the case, and will examine the reasons why the changes have been so limited.

This research question relates more generally to two different streams of academic literature. First, it contributes to the debate on legal integration and the role of the CJEU in the process of "integration through law".[5] Is the CJEU still a cornerstone of the EU integration process? What are the conditions under which EU law is respected, not only at national level but also at EU level (where secondary legislation must comply with "constitutional" primary law)? Second, it can be seen as a classic case of institutional change,

[1] European Commission Press Release 216/16 of 2 February 2016, *EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield*, europa.eu.

[2] Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Parliament and Council Directive 95/46/EC on the adequacy of the protection provided by the EU-US Privacy Shield.

[3] Decision 2000/520/EC of the Commission of 26 July 2000 pursuant to Parliament and Council Directive 95/46/EC on the adequacy of the protection provided by Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[4] Court of justice, judgement of 6 October 2015, case C-362/14, *Schrems* [GC]. For an overview of mass surveillance and privacy issues in the context of the transatlantic relations: D. Cole, F. Fabbrini, S. Schulhofer (eds), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford: Hart, 2017.

[5] S. Saurugger, F. Terpan, *The Court of Justice of the European Union and the Politics of Law*, Basingstoke: Palgrave, 2017; D.S. Martinsen, *An Ever More Powerful Court? The Political Constraints of Legal Integration in the European Union*, Oxford: Oxford University Press, 2015.

or normative change, where factors of change or inertia are scrutinised.[6] What triggers change? Why does inertia sometimes occur, even when the sophisticated judicial system of the European Union strives towards change? The specificity of the debate on EU-US transfer of data is that it cannot be considered as purely "internal". Although the *Schrems* ruling has to be complied with at European level, it is not merely an EU political issue. On the contrary, external relations and EU politics are intertwined, and external factors, including the position of the United States, need to be addressed. Thus, studying reactions to *Schrems* will also help us to determine how external factors alter both the conditions for institutional change in the EU, and compliance with CJEU rulings.

In order to better encapsulate the evolution from *Safe Harbour* to *Privacy Shield*,[7] and the lack of normative change, I will apply a law and politics approach, based on the assumption that law is embedded in a wider system of social facts and causal mechanisms, and is better understood when situated in a wider political context. I will use the framework of the *feedback loops*, which helps to understand how relationships between actors are shaped and reconfigured. Three steps can be distinguished: an action (adoption of *Safe Harbour*) triggers a reaction (the *Schrems* judgment), which leads to a feedback effect (*Privacy Shield*). Three possible outcomes can result from this feedback effect: a return to the original situation (non-compliance with the requirements of *Schrems*), a radical move towards greater protection of personal data (full compliance with *Schrems*), and, in between the two, a limited evolution (selective compliance with *Schrems*). The evaluation of the feedback effect will be carried out through legal analysis, while its explanation will require a larger perspective based on EU politics and governance.

Section II will present the empirics through the application of the feedback loop model. Section III will then analyse the content of *Privacy Shield* in order to determine the outcome of the feedback effect. Finally, in section IV, the factors that explain this outcome will be investigated.

II. From *Safe Harbour* to *Privacy Shield*: EU-US data transfer as a feedback loop

With the development of digital technologies and the Internet in the 1990s, rules controlling the transfer of personal data between Europe and the US were introduced in the so-called *Safe Harbour* "agreement". Non-governmental organizations (NGOs) as well as national and EU institutions expressed their concern, arguing that EU citizens'

[6] J. Mahoney, K. Thelen (eds), *Explaining Institutional Change: Ambiguity, Agency, and Power*, Cambridge: Cambridge University Press, 2009; A. Héritier, *Explaining Institutional Change in Europe*, Oxford: Oxford University Press, 2007.

[7] M.A. Weiss, K. Archick, *US-EU Data Privacy: From Safe Harbour to Privacy Shield*, Report prepared for Members and Committees of Congress, 19 May 2016, fas.org.

personal data was not sufficiently protected. In the end, the CJEU ruled on the issue, making the adoption of a new regime necessary.

II.1. Action: *Safe Harbour* and the first agreement on EU-US data transfer

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, adopted by the Parliament and the Council on 24 October 1995,[8] states that the transfer of personal data to a third country may take place only if the third country in question ensures an "adequate level of protection" (Art. 25, para. 1). The adequacy of the protection must be ascertained by the Commission. When a State does not ensure an adequate level of protection, transfer remains possible by way of derogation to Art. 25. Art. 26 specifies the conditions of such derogations.

Yet, it would be detrimental to EU-US relations if data transfer were only possible on the basis of derogations negotiated by private operators. This is precisely why the EU and the US introduced *Safe Harbour*. The Commission decision 2000/520/EC,[9] based on Art. 25, para. 1, of Directive 95/46/EC, certifies that the new EU-US data transfer regime offers an adequate level of protection for European citizens whose personal data are transferred to the US.

According to *Safe Harbour*, American companies must comply with a series of principles if they want to legally process personal data that comes from Europe. In particular, they must inform individuals that their data is being collected and specify how it will be used. Individuals must have the option to opt out of their data being collected and transferred to third parties. Transfer of data to third parties may only be carried out by those organizations that follow adequate data protection principles. Reasonable efforts must be made to prevent loss of collected information. Data must be relevant and reliable for the purpose for which it was collected. Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate. Effective means of enforcing these rules are included in *Safe Harbour*. They combine self-regulation by the private sector with public authority control, more specifically the Federal Trade Commission (FTC).

However, according to an annex to Decision 2000/520/EC, issued by the US Department of Commerce, adherence to these principles may be limited "to the extent necessary to meet national security, public interest, or law enforcement requirements". These limitations are themselves "limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization".[10] In other words, when US intelligence requires US companies to cooperate for reasons of national security, protection

[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.

[9] Decision 2000/520/EC, cit.

[10] Annex I to Decision 2000/520/EC, cit.

of EU citizens' personal data becomes a secondary consideration. This limitation, although not the only problem in terms of data protection, has been the main reason why *Safe Harbour* has been targeted by privacy activists.

II.2. Effect: *Safe Harbour* invalidated by the CJEU in *Schrems*

Maximilian Schrems, an Austrian student and privacy activist, asked the Irish Data Protection Commissioner (DPC) to prohibit the transfer of personal data to the United States via Facebook Ireland (Facebook having its head office in Ireland). He considered that Internet users are not protected against the intrusion of US agencies, in particular the National Security Agency (NSA), the latter having unlimited access to the personal data of European citizens, without the need to resort to a judicial decision. The Commissioner rejected this demand, arguing that Facebook had been certified under the *Safe Harbour* agreement.

Maximilian Schrems then filed an application for judicial review to the Irish High Court in response to the inaction of the Irish DPC, invoking both Directive 1995/46/EC and Arts 7 and 8 of the Charter of Fundamental Rights of the European Union (on respect for private life and the protection of personal data respectively). The High Court appealed to the CJEU, asking whether the adequacy decision prevented a national control authority from stopping the transfer of data on the grounds that privacy is not protected enough. The Grand Chamber of the CJEU issued a ruling on 6 October 2015 making it clear that national authorities must maintain the right to exert control, provided they do not declare the adequacy decision invalid. The Court then looked at the legality of the decision and decided that Art. 1 of Decision 2000/520/CE[11] was in breach of Art. 25, para. 6, of Directive 1995/46/CE, in light of the Charter of Fundamental Rights of the European Union. As the decision did not include any evaluation of the US rules, the Commission did not provide evidence that an adequate level of protection had been reached.

In addition, this protection level had to be regularly re-evaluated when confronted with new circumstances. Most certainly, the revelations from Mr Snowden regarding the NSA programme of mass surveillance (PRISM) could be considered a new occurrence justifying a re-evaluation. The Commission should have mentioned the fact that US

[11] *Schrems* [GC], cit., para. 98. On the *Schrems* ruling: S. Carrera, E. Guild, *The End of Safe Harbor: What Future for EU-US Data Transfers?*, in *Maastricht Journal of European and Comparative Law*, 2015, p. 651 *et seq.*; C. De Terwangne, C. Gayrel, *Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems*, in *Cahiers de droit européen*, 2017, p. 35 *et seq.*; R.A. Epstein, *The ECJ's Fanal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices*, in *European Constitutional Law Review*, 2016, p. 330 *et seq.*; J.F.M. Marques, *And [They] Built a Crooked H[arbour] – The Schrems Ruling and What it Means for the Future of Data Transfers Between the EU and US*, in *EU Law Journal*, 2016, p. 54 *et seq.*; X. Tracol, *Invalidator Strikes Back: The Harbour Has Never Been Safe*, in *Computer Law & Security Review*, 2016, p. 345 *et seq.*

agencies had generalized access to the content of digital communications, without any external and independent control, and without any precise criteria limiting the number of cases where access for national security reasons was allowed. In fact, the Commission had by this time started to discuss the issue with US authorities, but this was not enough to change the Court's position/ruling.

The Court's ruling was consistent with previous case law supporting data protection, which was quite cautious in the early 2000s,[12] and more audacious in the post-Lisbon period, after the Charter of Fundamental Rights of the European Union (which included a provision on data protection) had become legally binding.[13]

Although it contributed to the CJEU's "constitutionalisation" of European law,[14] the *Schrems* ruling prompted a renegotiation of the rules contained in *Safe Harbour*.

II.3. Feedback: *Safe Harbour* replaced by *Privacy Shield*

Safe Harbour was replaced by *Privacy Shield* thanks to an agreement between EU and US representatives announced on 2 February 2016. The new regime is supposed to secure the transfer of data in accordance with EU primary and secondary law. On 12 July 2016, the Commission adopted a decision declaring that the United States, and the Department of Commerce in particular, should ensure an adequate level of protection as required by the Directive 95/46/EC.[15] This adequacy decision was based on one declaration and several letters that came from US authorities, which are reproduced in Annexes 1 to 7.

Annex 2 shows a declaration made by the Department of Commerce setting out the principles of *Privacy Shield*. Annexes 3 to 5 contain letters from the Secretary of State, the President of the Federal Trade Commission and the Secretary of Transport, which were sent to the European Commission. Annexes 6 and 7 originate from the Director of National Intelligence and the Assistant Attorney General, and were sent to senior officials at the Department of Commerce, and not to the Commission.

III. *Privacy Shield*: non-compliance, full or partial compliance?

Are personal data better protected thanks to *Privacy Shield*? To what extent does the new regime comply with the requirements in *Schrems*? We distinguish between three possible

[12] See for instance, Court of justice: judgment of 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, *Österreichischer Rundfunk and Others*; judgment of 29 January 2008, case C-275/06, *Promusicae*; judgment of 16 December 2008, case C-73/07, *Satakunnan Markkinapörssi and Satamedia*.

[13] Court of justice: judgment of 8 April 2014, joined cases C-293/12, C-594/12, *Seitlinger and Others*; judgment of 13 May 2014, case C-131/12, *Google Spain*. For a general view, O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford: Oxford University Press, 2015.

[14] S. Saurugger, F. Terpan, *The Court of Justice of the European Union and the Politics of Law*, cit., pp. 158-179; F. Terpan, *Le constitutionnalisme européen: penser la Constitution au-delà de l'État*, in *Mélanges en l'honneur du Professeur Henri Oberdorff*, Paris: Lextenso, 2015, p. 181.

[15] Commission Implementing Decision 2016/1250, cit.

scenarios. Full compliance refers to a situation where the level of protection ensured by the US authorities is similar to the level required by the European Union. Non-compliance is when, apart from a formal change (adoption of a new adequacy decision), the new regime is substantially similar to the old one. In between these two scenarios, we may have partial compliance if *Privacy Shield*, albeit improving the level of protection of European personal data, remains quite far from the requirements laid down by *Schrems*.

III.1. Slightly improved protection of personal data

Legal analysis of the new documents shows that three main improvements have been made to the EU-US transfer of data regime.

First, *Privacy Shield* is based, like *Safe Harbour*, on a system of certification: corporations can transfer data as soon as they are certified by the US Department of Commerce. To be certified, they need to comply with a series of privacy requirements.

While the system remains unchanged, *Privacy Shield* private operators are subject to greater commitments with regard to notifications, limits to data retention, rights of access, publicity of privacy policies etc. The Department of Commerce has the power to investigate and control the implementation of these commitments.

Second, the Department of Justice and the Director of National Intelligence provided written assurance (annexed to the adequacy decision) that security agencies' access to European data will be clearly limited and controlled. The Commission, together with the Department of Commerce, and European as well as US data protection authorities, will provide an annual assessment.

Third, EU citizens benefit from better control mechanisms. They now have the ability to file a claim: *1*) against US companies, which have 45 days to resolve the complaint; *2*) against European data protection authorities, which may refer the complaint to the Department of Commerce. In a more indirect way, European citizens can appeal to the Department of Commerce or an alternative mechanism if the latter does not follow it up. As for complaints about intelligence agencies, an ombudsperson was appointed by the Department of State, presently Mrs Manisha Singh (Under Secretary of State for Economic Growth, Energy, and the Environment).

The ombudsperson, who is responsible for the cases submitted by European data protection authorities, is presented by the European Commission as being independent from the intelligence authorities.[16] In addition to *Privacy Shield*, the Obama administration introduced, on 24 February 2016, a new law – the Judicial Redress Act – under which European citizens can benefit from the same rights guaranteed to US citizens by the US Privacy Act of 1974. The Commission welcomed this development.[17]

[16] *Ibid.*, para. 121.

[17] Commission Press Release of 24 February 2016, *Statement by Commissioner Věra Jourová on the Signature of the Judicial Redress Act by President Obama*.

III.2. Persistent shortcomings

However, despite these improvements, the protection ensured by US authorities still suffers from several major shortcomings.[18] *Privacy Shield*, like *Safe Harbour*, does not take into account the evaluation carried out by the Commission on US data protection rules. The lack of a proper assessment was one of the main motivations for the CJEU to declare the decision 2000/520/EC on *Safe Harbour* illegal. As this major flaw has not been corrected, there is enough evidence to believe that *Privacy Shield* could also be invalidated; the validity of the new regime remains fragile.[19]

Moreover, the legal nature of the documents provided by US authorities is a matter for discussion. The general principles that apply to US companies are established on the basis of a simple declaration from the Department of Commerce, which cannot be seen as a legal commitment. It is also doubtful whether these documents can be seen as international agreements between the EU and the US.

While the letters from the Secretary of State (Annex 3), the President of the Federal Trade Commission (Annex 4), as well as of the Secretary of Transport (Annex 5), might be considered "executive agreements" at best, this cannot be the case with the letters from the Director of National Intelligence (Annex 6) and the Assistant Attorney General, which were not sent to EU institutions.

Privacy Shield also raises concerns on both the commercial and security dimension. At least three types of shortcomings affect the commercial part of *Privacy Shield*. The first one relates to the way data is collected and circulated. No specific rules are applied to automated data collection. And very few guarantees are provided regarding the transfer of data to third countries as well as the role played by sub-contractors. The second category of shortcomings concerns the degree of rights protection. There is no obligation for private organisations to delete personal data when it is no longer required by them. Consumers have no right to oppose the collection of data. Thirdly, the complaints mechanisms remain complex and there are serious reasons to doubt their effectiveness.

Regarding the security dimension, we have already mentioned that the mechanism still relies on letters from US public authorities, more than actual legal commitments. While the Office of the Director of National Intelligence declare that they will refrain from collecting massive and indiscriminate amounts of data, there is no legal means to ensure that they will respect this declaration of intent. Even the independence of the Ombudsperson remains an issue, as she works under the vice-secretary of the US State Department. The fact

[18] The Art. 29 Working Party emphasised the remaining shortcomings on 13 April and 29 July 2016, before and after the adequacy decision. See: G. Vermeulen, *The Paper Shield, on the Degree of Protection of the EU-US Privacy Shield Against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services*, in D.J.B. Svantesson, K. Dariusz (eds), *Transatlantic Data Privacy Relationships as a Challenge for Democracy*, Portland: Intersentia, 2017.

[19] X. Tracol, *EU-US Privacy Shield: The Saga Continues*, in *Computer Law & Security Review*, 2016, p. 1 *et seq.*

that the Commission, in its adequacy decision, has mentioned the independence of the Ombudsperson, is not exactly a guarantee that this independence will be effective.

The emphasis on guarantees and control mechanisms can easily be understood, for both commercial and security reasons. We have witnessed this before; Safe Harbour contained obligations that were not respected either by businesses or public authorities. The Federal Trade Commission opened procedures against no more than ten companies during the 13 years of existence of *Safe Harbour*. Dozens of companies have declared activities within the framework of *Safe Harbour* while they are not actually covered by this regime.[20] Although complaints procedures have improved, the effectiveness of *Privacy Shield* will depend, as was the case with its predecessor, on the willingness of the Federal Trade Commission. As for Public authorities, they have largely and indiscriminately made use of the exception concerning national security. If the same causes produce the same effects, there is enough reason to believe that practices that do not respect private life and data protection will persist.

Thus, *Privacy Shield* appears to have only partially complied with the *Schrems* ruling. While it perhaps did not fully return to square one, as a few improvements have been made, it clearly did not really progress much further, leading to doubts about the legality of the new regime.

IV. Why only partial compliance?

To explain why *Privacy Shield* constitutes a case of only partial compliance, I will proceed in two stages. I will first identify the reasons why non-compliance was not an option, before turning to the reasons why full compliance was not possible either, leading to the middle ground of partial compliance. Two considerations will inform the analysis, pertaining first to the legal and normative context, and second to the preferences of the actors.

IV.1. Reasons why non-compliance was not an option

a) Legal and normative explanations.

In the EU system of governance, it is unlikely that EU institutions ignore or even circumvent a ruling of the CJEU. In the case of *Schrems*, the Court based its decision on Directive 1995/46/EC as well as Arts 7 and 8 of the Charter of Fundamental Rights of the European Union. Non-compliance with *Schrems* would mean revising secondary legislation and, possibly, revising the Charter in order to be sure that the Court would have no legal grounds for invalidating the new adequacy decision. This would imply that the Commission, as well as the Council and the Parliament, would have to be ready to lower

[20] G. Vermeulen, *The Paper Shield*, cit. See also: R.R. Schriver, *You Cheated, You Lied: The Safe Harbour Agreement and Its Enforcement by the Federal Trade Commission*, in *Fordham Law Review*, 2002, p. 277 *et seq.*

the level of data protection in Europe and bring it closer to US rules, which is hardly conceivable. On the contrary, the adoption of the General Data Protection Regulation (GDPR) in May 2016[21] clearly indicates that the Union has set in motion new moves towards greater data protection.

Art. 7 of the Charter of Fundamental Rights of the European Union states that "everyone has the right to respect for his or her private and family life, home and communications". Art. 8 of the same Charter brings with it three kinds of guarantees.

First, it provides a general right for personal data to be protected. Second, it specifies the nature of this right, by stating that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" and that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". And third, Art. 8 includes a mechanism for the control of these rules by an "independent authority". Thanks to these provisions, data protection in the EU has been elevated to the level of a constitutional principle, allowing the CJEU to use it against any act or practice that does not conform to it. A similar evolution has occurred in the Council of Europe, where the European Court of Human Rights has issued decisions quite similar to the CJEU because of *Schrems*. Mass surveillance was condemned in *Zakharov*[22] and *Szabo*,[23] which, just like *Schrems*, show how far European Courts have gone to constitutionalise the protection of personal data and provide effective guarantees to citizens.[24] The emergence of a constitutional principle of data protection, in the EU as well as in the Council of Europe, creates normative constraints that cannot be evaded by political institutions.

b) Actor-centered explanations.

This process of constitutionalisation of data protection at EU level has been supported by different actors, whose mobilization explains why non-compliance was not a feasible option. In particular, the use of litigation by civil society organizations has had a huge impact since 2013, as well as the disclosure of PRISM. Both national courts and NGOs have contributed effectively to the control of *Safe Harbour*. The Irish High Court, which made a reference to the CJEU in the *Schrems* case, had already criticized the NSA and the US programmes of mass surveillance.

[21] 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). Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[22] European Court of Human Rights, judgment of 4 December 2015, no. 47143/06, *Zakharov v. Russia*.

[23] European Court of Human Rights, judgment of 12 January 2016, no. 37138/14, *Szabo v. Hungary*.

[24] J.-F. FOEGLE, *Chronique du droit Post-Snowden: La CJUE et la CEDH sonnent le glas de la surveillance de masse*, in *La Revue des droits de l'homme*, 2016.

As we have already seen, Maximilian Schrems, data protection activist and founder of "Europe vs. Facebook", is the one who triggered the downfall of *Safe Harbour*, by starting the judicial procedure in Ireland. Yet the judicial incentive could have come from other actors engaged in the cause of data protection, if they have chosen to litigate, in addition to their lobbying activities.[25] NGOs have remained active since the *Schrems* ruling. As a matter of fact, some of them have already sought the annulment of the adequacy decision regarding *Privacy Shield*, showing that they are willing to act as a counter-weight to the power of EU and US institutions with regard to data transfer.[26] This is not to say that this is always successful. The action brought by Digital Rights Ireland (DRI) in case T-670/16 has already been declared inadmissible by the General Court of the CJEU, which argued first, that DRI does not have any interest in initiating proceedings, and second, that it does not have legal standing to act in the name of its members and supporters or on behalf of the general public.

EU political institutions have also adapted to the new "post-Snowden" climate. In the European Parliament, voices were raised in favour of the suspension of *Safe Harbour*; and they are still actively lobbying against *Privacy Shield*. Jan Philipp Albrecht, for example, has been one of the most active Members of the European Parliament, criticizing a system that is mostly based on declarations of intent from US authorities.[27] The way that *Privacy Shield* is configured has been negotiated by the Commission with a view to meeting the approval of the Parliament.

Similarly, the Commission has taken into account the concerns expressed by Member States, in particular France and Germany, who reacted strongly to the revelations by Snowden about PRISM and have remained alert during the negotiations over *Privacy Shield*.[28] The Art. 29 working party aims to enable the Commission to exert some kind of national control, and is composed of a representative from the supervisory authorities designated by each EU country, as well as a representative from the authorities established by the EU institutions and bodies, and a representative from the European Commission.

Furthermore, the Commission itself expressed concerns about *Safe Harbour*, even before the Snowden revelations. Two documents in 2002[29] and 2004[30] underlined the

[25] For instance, among others: Cyber Privacy Project (CPP), Digitale Gesellschaft e. V., Electronic Frontier Finland (EFFi), Epicenter.Works (prior: AKVorrat), European Digital Rights, Facebook Class Action, Human Rights Watch, IT-Political Association of Denmark (IT-Pol), Privacy International, Stichting Bits of Freedom (Bof), Transatlantic Consumer Dialogue (TACD), Verein für Konsumenteninformation (VKI), Panoptykon Foundation.

[26] General Court: order of 22 November 2017, case T-670/16, *Digital Rights Ireland v. Commission*; action brought on 9 December 2016, case T-738/16, *La Quadrature du Net and Others v. Commission*.

[27] Cited in N. LOMAS, *Europe and US Seal Privacy Shield Data Transfer Deal to Replace Safe Harbour*, in *Techcrunch.com*, 2 February 2016, techcrunch.com.

[28] K. DORT, J.T. CRISS, *Trends in Cybersecurity Law, the Privacy Shield, and Best Practices for Businesses Operating in the Global Marketplace*, in *The Computer and Internet Lawyer*, 2016, p. 5 *et seq.*

[29] Commission Staff Working Paper SEC(2002) 196 of 13 February 2002 on the application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament

shortcomings of *Safe Harbour*, and more specifically its lack of legal commitments and effectiveness. A few months after the PRISM disclosure, in November 2013, the Commission adopted two communications, the first one entitled "Rebuilding Trust in EU-US Data Flow",[31] the second one "on the functioning of Safe Harbour from the perspective of EU citizens and companies established in the EU".[32]

With regard to the latter, it has been clearly established that Microsoft, Google, Facebook, Apple, Yahoo!, Skype and YouTube, although certified within the framework of *Safe Harbour*, are all involved in PRISM. This programme, thus, goes far beyond what is necessary to protect national security under the exception included in decision 2000/520/EC. In 2014, the Commission negotiated a revision of *Safe Harbour* with the US Department of Commerce (*Safe Harbour 2.0*) aimed at greater transparency and control of data transfer. This renegotiation is consistent with the EU internal evolution towards better protection of personal data, starting with the legislative package presented by the Commission in 2012 and culminating in the adoption of a new regulation (on 27 April 2016, in force since 24 May 2016)[33] and a new directive (on 5 May 2016, in force since 6 May 2018).[34]

This section has shown that compliance was necessary not only due to strong legal and normative constraints, but also because of a consensus that emerged among different actors. In the following section, I will identify the reasons why compliance could not be full but only partial.

IV.2. Reasons why full compliance was not possible

Privacy Shield is the result of a difficult negotiation process with a US partner whose main objective is not to adapt to the requirements of European law as interpreted by the CJEU. Contrary to purely "internal" compliance issues, compliance in this case thus includes an "external" dimension, which hinders the prospects for full compliance. Both legal/normative and actor-centered factors explain why changes have been limited.

a) Legal and normative explanations.

and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.

[30] Commission Staff Working Document SEC(2004) 1323 of 20 October 2004, *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related frequently Asked Questions issued by the US Department of Commerce*.

[31] Communication COM(2013) 846 final of 27 November 2013 from the Commission to the European Parliament and the Council, *Rebuilding Trust in EU-US Data Flow*.

[32] Communication COM(2013) 847 final of 27 November 2013 from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.

[33] Regulation 2016/679/EU, cit.

[34] Directive 2016/680/EU, cit.

At a normative level, full compliance could only be possible if the guarantees given by US authorities to citizens dramatically improved, which has not been the case in recent years. There is still a huge gap between EU and US rules in the field of data protection, a gap that increased with the adoption of GDPR in 2016.[35]

This is precisely why a growing number of proposals for federal privacy legislation in the United States have arisen over recent months. In particular, the draft Consumer Data Protection Act,[36] would require certain organizations to submit annual data protection reports to the FTC and would empower the FTC to impose fines of up to 50.000 dollars per violation or four percent of the total annual gross revenue of an organization for a first time offense. Under the new Bill, the FTC would also be given rulemaking authority to establish new regulations with regard to privacy. But for now, the level of protection in the US remains lower than in Europe.

Furthermore, apart from the "level" of protection, the "nature" of the protection afforded by the US system also differs from EU law, with greater involvement of private organisations in the resolution of disputes.

b) Actor-centred explanations.

There is no serious will to change in the US administration, with regard to data protection. The most recent changes in the United States date back to the Obama period, and the election of Donald Trump seems to have closed the door on any hope of further improvement. The European internal market is attractive for US companies, which may give some leeway to the EU in its negotiations on EU-US data transfer,[37] and confirm the idea of a "Market Power Europe";[38] however, it might not be attractive enough to trigger a radical change in the level of data protection. The US government has not given any guarantees that mass surveillance carried out by the NSA will be stopped or limited in the near future. Thus, there is no real sign from the United States that US rules could be aligned with those of the EU.

From an EU perspective, data protection, important as it may be, must be reconciled with economic objectives. Transatlantic data flows must not be hindered by overprotective rules. This explains why the Commission, before the Irish High Court submitted a preliminary question to the CJEU, had never really considered the demands of Maximilian Schrems and some Members of the European Parliament to suspend *Safe Harbour* because of the Snowden revelations. The Commission feared that such a decision would have a negative impact on business in Europe and transatlantic economic

[35] K. DORT, J.T. CRISS, *Trends in Cybersecurity Law, the Privacy Shield, and Best Practices for Businesses Operating in the Global Marketplace*, cit., p. 2.

[36] US Congress, *H.R.4544 – Consumer Data Protection Act*, introduced in House on 12 April 2017, www.congress.gov.

[37] G. SHAFFER, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards*, in *Yale Journal of International Law*, 2000, p. 82 *et seq.*

[38] C. DAMRO, *Market Power Europe*, in *Journal of European Public Policy*, 2012, p. 682 *et seq.*

relations.[39] This is why *Safe Harbour* was discussed but never really challenged before the Court issued its decision on *Schrems*.

The same reasoning applies to the post-*Schrems* period. The invalidation of Decision 2000/520/EC by the CJEU has made the adoption of a new decision necessary, but the logic of economic interest still plays a central role. The Court's decision has created legal uncertainty for some 5500 US companies that are active in the EU's internal market.

Commissioner Jourová (in charge of justice, consumer and gender equality) as well as Commissioner Günther Oettinger (in charge of the digital economy) and Vice-President Andrus Ansip (in charge of the digital internal market) have made it clear that facilitating transatlantic data transfer is a top priority.[40]

Member States have agreed with the Commission's position. Despite a general feeling of worry and some concern expressed particularly by France and Germany, they all understand the necessity of maintaining a political discourse regarding transatlantic trade.[41]

In early 2018, the new French government defended *Privacy Shield* during the proceedings at the General Court of the CJEU: this ran contrary to the idea of renegotiating the agreement, which was extolled by Emmanuel Macron during his presidential campaign.[42] In seeking to raise the importance of data protection, national governments risk putting transatlantic economic relations in jeopardy. What remains to be seen is whether a more difficult EU-US climate, with Donald Trump threatening Europe with commercial war, will change the position of EU member states.

V. Conclusion

The objective of this *Article* was to shed some light on the transformation of the EU-US data transfer regime, from *Safe Harbour* to *Privacy Shield*. In section I, the theoretical model of the feedback loop was used to distinguish between an action (the adoption and implementation of *Safe Harbour*), an effect (the invalidation of *Safe Harbour* by the CJEU due to *Schrems*) and feedback (the replacement of *Safe Harbour* by *Privacy Shield*).

Legal analysis of the feedback effect, in section II, shows that the judgment in the case of *Schrems* has not been ignored, but has not been fully taken into account either. It can be seen as a case of partial compliance, given that several concerns about *Safe Harbour* have not disappeared with the advent of *Privacy Shield*. One major shortcoming is that the adequacy decision as regards *Privacy Shield*, like its predecessor, does not meet the CJEU requirement that the Commission should make an evaluation of US rules and guar-

[39] Communication COM(2013) 847 final, cit.

[40] G. Vermeulen, *The Paper Shield*, cit., p. 6.

[41] K. Dort, J.T. Criss, *Trends in Cybersecurity Law, the Privacy Shield, and Best Practices for Businesses Operating in the Global Marketplace*, cit., p. 5.

[42] On the French position with regard to *Privacy Shield*: M. Rees, *Le gouvernement défend le Privacy Shield et la conservation généralisée des données*, in *NextInpact*, 28 February 2018, www.nextinpact.com.

antees. As these guarantees continue to be mostly based on declarations of intent, there are sufficient reasons to believe that the legality of the new regime is fragile.

The explanations for this partial compliance must stem from the constraints brought about by legal and normative factors as well as the preferences of actors. Data protection has been highly constitutionalized and is now supported by several actors, NGOs, member states and EU institutions, all of which are concerned about its effectiveness. However, there are strong limitations to this effectiveness as regards external data transfer. Given that US law remains less protective of personal data than EU law, and economic interests being prioritised on both sides of the Atlantic, the changes made in *Privacy Shield* are limited.

The adoption of *Privacy Shield* has initiated a new feedback loop, the trajectory of which remains to be discovered. Digital Rights Ireland and La Quadrature du net brought a case before the General Court of the CJEU,[43] seeking the annulment of the new adequacy decision, on different grounds: the collection of data afforded by US rules is indiscriminate; processing of data is not limited to what is strictly necessary; the lack of an effective mechanism of control; the lack of truly independent control etc.. They are facing serious difficulties, due to the fact that NGOs that defend the public interest do not have legal standing in annulment actions. Yet, the European system of governance opens up other opportunities to litigate and wage a legal battle against *Privacy Shield*. Litigation at member state level, culminating in a preliminary question to the CJEU, may have the same result as the *Schrems* ruling. The pending case of *Facebook Ireland and Schrems* (C-311/18) will give an opportunity for the CJEU to rule on *Privacy Shield*. If the latter is declared illegal, this time the feedback effect will have to be of a different nature, otherwise the feedback loop will lead to normative and institutional deadlock.

[43] *Digital Rights Ireland v. Commission*, cit.; *La Quadrature du Net and Others v. Commission*, cit.