"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

João Marques*

ABSTRACT: Safe Harbour (Henceforth, SH) has been the main enabler of EU-US personal data transfers since Decision 2000/520/EC came into force. Initially, Safe Harbour was seen as an innovative solution to a difficult problem. However, the problems the agreement was created to solve were never remedied. Thus, it did not come as a surprise that the Court of Justice of the European Union (hereinafter, CJEU), in Case C-362/14 (the Schrems ruling), deemed the agreement invalid. In the story "And he built a crooked house", the infamous 'crooked house', designed by Robert A. Heinlein's character Quintus Teal, mirrors SH's flawed design. It also exemplifies the fact that great innovations can fail if not thought through carefully. Although the Schrems ruling's scope does not go beyond Decision 2000/520/EC, it will force European Data Protection Agencies to look deeper into alternative data transfer mechanisms and possibly, consider transfers to jurisdictions other than the US. Furthermore, this decision highlights the fact that if any progress on this front is going to be made going forward regarding personal data transfers, any solution(s) would have to be made at a global level. This paper will provide an overview of the implications of the CJEU ruling on data transfers between the EU and the US going forward.

KEYWORDS: Decision 2000/520 - Safe Harbour - Maximillian Schrems v. Data Protection Commissioner - data transfers - adequate protection.

* Lawyer and currently serving as Commissioner at "Comissão Nacional de Proteção de Dados" (National Data Protection Commission).

1. Introduction

The CJEU ruling on Case C-362/14 (the *Schrems* ruling),[1] which resulted in the invalidation of Decision 2000/520, means that personal data will no longer be able to be transferred from the EU to the US, without regulatory approval from Data Protection agencies in each EU Member State. In the Court's view, there is no guarantee that under SH, *the principle of adequate protection* is strictly adhered to and that the personal data of European citizens' is, potentially, not given equal treatment on both sides of the Atlantic.

Fueled by the revelations of former National Security Agency (Henceforth, NSA) employee Edward Snowden and the subsequent worries over how effective data protection is in the US, Austrian citizen Maximillian Schrems filed a complaint with the Irish Data Protection Authority (hereinafter, DPA), claiming that Facebook was transferring the personal data of its users to a country (i.e. the US) that did not meet the standard level of protection, promulgated in Article 25 (1) of Directive 95/46/EC. Given the findings on the surveillance activities carried out by US public authorities, the Irish Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be submitted since any question of the adequacy of data protection in the US had to be determined in accordance with Decision 2000/520. In that decision, the Commission had found that the US ensured an adequate level of protection.[2] Subsequently, Mr. Schrems challenged the Irish DPA's decision before the Irish Court who, later, referred the issue to the CJEU, under the Preliminary Reference Procedure.[3] The ruling puts all flows of data between the EU and the US at stake, and has forced both blocks' to find a new, alternative framework for data transfers.

As this paper delves into the intricacies of this ruling, the authors will try to explain how changes to US data protection law is, arguably the only way to guarantee that both, a new SH and other data transfer mechanisms, remain viable, safe and law abiding avenues to conduct such transfers across both sides of the Atlantic.

This paper will also explore the growing notion that only a global solution to data transfers can allay people's apprehensions about their fundamental right to privacy being encroached upon by unscrupulous individuals, companies or governments. SH is, indeed, the tip of the iceberg as data transfers from the EU to other parts of the world will, soon, be in the spotlight. Now that the CJEU has evaluated the shortcomings of the US legal framework, it is only a matter of time before the issue of adequate protection is raised again regarding transfers to other jurisdictions.

2. The Tesseract House and the Tesseract Harbour

Quintus Teal is a name that might not have said much in the European Commission (henceforth, EC) and the US Department of Commerce (henceforth, DOC) in the late nineties and the beginning of the first decade of the 21st century. However, the ideology behind his work surely must have been at the heart of the Commission's Decision 2000/520/EC and the SH principles and the Frequently Asked Questions (hereinafter, FOA) put forward by their American counterpart in

[1] Judgment *Maximillian Schrems* v. *Data Protection Commissioner*, Case C-362/14, October 2015.
[2] Para. 29 of the Ruling.
[3] Article 267 TFEU.

the year 2000.[4]

Quintus, the lead character from the story *"And he built a crooked house"* by Robert A. Heinlein,[5] claims for himself the endeavour of designing and building the true house of the future, the present and the past. Putting a name for himself as an architectural, "visionary" if you like or as Robert A. Heinlein describes him, *"the original Hermit of Hollywood,"*[6] he starts by asking his friend Homer Bailey: *"What is a house?"*[7]

In a passionate discussion, arising from the said question, Quintus asks crudely: *"What's Frank Lloyd Wright got that I haven't got?,"*[8] only to be dismissed by Homer Bailey's even cruder answer: *"Commissions."*[9] It is perfectly clear that Bailey´s answer had nothing to do with the EC or with the Federal Trade Commission (hereinafter FTC),[10] looking deeper into the *"crooked house"* designed and built by the two institutions, admittedly embedded in the same good will as Quintus' quintessential, albeit, defective masterpiece, we can't help but notice the similarities displayed in both, the concept and in the results it has produced.

Although Quintus hits back at Homer with a rhetorically valid point when he says *"why should we be held down by frozen concepts of our ancestors,"*[11] as he grasps to make his friend fully understand his own concept of a breathing, living house, responding to the surrounding environment and its inhabitants – we unfortunately know that the end result does fail to demonstrate his point. The ingenious "tesseract house" became both his life's work and his bypass to perpetual unemployment.

The four dimensional house of Quintus proved too vague and uncertain for the daily life. As with its spectacular *capolavoro* fallout, where the owners of the house and the architect himself ended up stranded inside a labyrinth in which entering any door was a life threatening experience, as they did not know where it would lead them next, the SH agreement was invalidated by the CJEU because of the uncertainty over whether the fundamental right of the European constituents, to privacy of data,[12] was being adequately safeguarded.

A SH 2.0 has been suggested[13] by the Commission as a response to the Court's arguments, but doubts remain over how effective a self-regulatory based mechanism will be in restoring confidence in transatlantic personal data transfer when the fundamental rights issue at stake doesn't seem to be at the epicentre of the solution.

---

[4] The Decision is available at http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520 and https://www.federalregister.gov/articles/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission contains the Principles and Frequently Asked Questions issued by the Department of Commerce.

[5] Robert A. Heinlein, *"And he built a crooked house"*, 2013, Ibook edition, published together with other four short stories in the ebook *"All you zombies" - Five Classic Stories by Robert A. Heinlein.*

[6] *Idem,* 9-61.

[7] *Idem,* 9-61.

[8] *Idem,* 9-61.

[9] *Idem,* 9-61.

[10] The Federal Trade Commission (hereinafter FTC) is responsible for the oversight of the SH scheme in the US. See http://www.law.cornell.edu/uscode/text/15/45, section 5 of the FTC Act.

[11] Robert Heinlein, *op. cit.* 9-61.

[12] Article 8 of the Charter.

[13] See Commission's Communication to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment *Schrems* by the Court of Justice in, Case C-362/14, – COM (2015) 566 final, available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

3. The *Schrems* ruling

In the case referred to the CJEU from Northern Ireland, Maximillian Schrems challenged the Irish Data Protection Commissioner's decision not to pursue the latter's claims against Facebook Ireland Ltd. Schrems argued that by transferring the personal data of its (i.e Facebook's) users to the US, and keeping it on servers there in light of the recent findings on the mass surveillance done by the NSA, inter alia, Facebook was responsible for data transfers to a country that *"…did not ensure adequate protection…"*[14] of personal data.

The Irish Data Commissioner, for its part, decided that *"…his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection."*[15]

Following the Commissioner's decision, Schrems presented the case to Ireland's High Court, which acknowledged some of the threats raised by Schrems, namely the fact that *"Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an ex parte and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of… indiscriminate surveillance…"*[16] The Court, however, considered that the implementation of EU law, as referred to in Article 51 of the Charter, was in question, as Decision 2000/520's validity had to be assessed. This prompted the Irish High Court to refer the case to the CJEU, together with two questions, for a preliminary ruling. The questions are enunciated below:[17]

> *(1) Whether in the course of determining a complaint which has been made to an independent office holder, who has been vested by statute with the functions of administering and enforcing data protection legislation, that personal data is being transferred to another third country, (in this case, the US) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?*
>
> *(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?*

In its ruling the Court began by pointing out what the Commission had already voiced[18] through its Communications – *COM(2013)* 846 *final*[19] and *COM(2013) 847*

[14] Alexandra Maria Rodrigues Araújo, "The Right to Data Protection and the Commissions' Adequacy Decision", in *UNIO – EU Law Journal*. Vol. 1, No. 1, July 2015, p. 77-93, for an extensive overview on the Commission's Adequacy Decision.
[15] *Id.,* para. 29.
[16] *Ibid.,* para. 31.
[17] *Ibid.,* para. 36.
[18] *Ibid.,* para. 11 to 25.
[19] Available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

final,[20] both of which derived from the Snowden revelations.

The Irish Court addressed some of the findings the Commission's report and acknowledged the fact that SH was a voluntary and sparsely regulated agreement that, potentially, left the data of EU citizens vulnerable to unauthorized access by US officials, thereby undermining the basis upon which the data was originally collected and the purposes for which it was transferred. Secondly, the Commission observed that SH also acts as a conduit for the transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes.

Notwithstanding, the Commission concluded in point 3.2 that, *given the weaknesses found, the current implementation of SH could not be maintained, but at the same time, acknowledged that* its revocation would adversely affect the interests of Member Companies in the EU and the US. Finally, the Commission added that it would engage the US authorities to discuss the shortcomings identified.

Taking into consideration *Communication COM(2013) 847 final*, the Court highlighted the fact that the Commission had already stressed that *"[a]ny gap in transparency or in enforcement on the US' side results in responsibility being shifted to European data protection authorities and to the companies which use the schemem,"* adding that *"It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles."*

Point 7 of Communication COM(2013) 847 final states that *"all companies involved in the PRISM programme,[21] and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified'* and that *"[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collect personal data initially processed in the [European Union]."* In that regard, the Commission noted in point 7.1 of that communication that *"a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]"* and that *"[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]."*

Another troublesome aspect of the findings was the double standard that EU citizens face against US citizens given that "safeguards that are provided under US law are mostly reserved for US citizens or legal residents"[22] and that, "[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes."[23]

Finally, the Court underlined point 8 of *Communication COM(2013) 847 final*, where the Commission states that: *"the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious*

[20] Available at http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[21] For a comprehensive explanation about the PRISM Programme, see Lee, Timothy B., 2013, "Here's everything we know about PRISM to date", *Washington Post,* June 12. Available at https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[22] COM(2013) 847 final, Point 7.2, 17.

[23] *Idem.*

questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]."

It is clear that the main questions posed by the Irish High Court didn't pertain to SH's validity in itself. In fact, the main issue at stake in the *Schrems* ruling was whether after the Commission's Decision 2000/520, a supervisory authority was or wasn't able to act on a person's complaint regarding the concrete existence of an adequate level of protection in a given case, when the country to where the data is transferred has previously been considered by the EC, to have an adequate level of protection, pursuant to Article 25(6) of Directive 95/46. This is the standard by which the Commission finds that a third country ensures an *adequate level of protection* of personal data. The Court highlights that Directive 95/46 *"must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter,"*[24] and cites its own jurisprudence to not only to emphasize the need to approach this matter as a question of fundamental rights, but also to clarify that the national supervisory authorities act according to strict independence requirements, as derived from the directive but also, from article 8 of the Charter and article 16 (2) of the Treaty.[25]

It goes on to note that the independence criteria is of utmost importance, as this is needed to ensure the national supervisory authorities effectively and reliably, monitor compliance with the provisions concerning protection of individuals' fundamental rights, which must be interpreted in light of that aim. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46; an essential component of the protection of individuals with regard to the processing of personal data.

In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other, the interests requiring free movement of personal data.

The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive list in Article 28(3) of Directive 95/46, are needed for them to perform their duties effectively, as stated in Recital 63 in the Preamble to the directive. These authorities, in effect, possess investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

It is, immediately apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State. Hence, they do not have competence on the basis of Article 28, to influence how personal data is processed in an external jurisdiction.

However, the process of data transfers from a Member State to a third country still constitutes, in itself, processing of personal data within the meaning of Article

[24] Para. 38 of the Ruling.

[25] "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

2(b) of Directive 95/46. That provision defines 'processing of personal data' as; *"any operation or set of operations which is performed upon personal data, whether or not by automatic means"* and mentions, by way of example, *"disclosure by transmission, dissemination or otherwise making available."*

Article 2(b) of Directive 95/46. That provision defines 'processing of personal data' as; "any operation or set of operations which is performed upon personal data, whether or not by automatic means" and mentions, by way of example, "disclosure by transmission, dissemination or otherwise making available."

Recital 60 in the Preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the Directive. In that regard, Chapter IV of the Directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data.

As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules, such as, *inter alia*, the protection of individuals' fundamental rights in the processing of their personal data. Hence, each of them is vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.[26]

The way the Court emphasizes the powers and independence of national supervisory authorities serves to reinforce the point that those entities must exercise the powers vested onto them and that, by Decision 2000/520 limiting that independence, that decision is invalid. It also suggests that to assure an adequate level of protection for EU citizens, any given third country must enforce a similar supervisory mechanism. Although the Court never explicitly mentions such a condition, it is, arguably, impossible to admit future transfers of data to third countries, where the overseeing authorities are not guaranteed this level of independence, as the question of fundamental right(s) at risk is never fully answered if that criterion is not met. We will get back to this when we analyse the current legal framework in the US.

It becomes clear that *"Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46."* In fact, admitting that a supervisory authority is bound not to act on any claim lodged by a natural person on these matters is contradictory to the system put forward by the EU legislator, as the court so eloquently affirms, following its interpretation of Articles 25 and 28 of the Directive: *"…If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights."* The CJEU goes further to notice that the EU is a union based on the rule of law. The Commission's decisions cannot, therefore, escape independent review."[27]

[26] Para. 41 to 47 of the Ruling.
[27] Paragraphs 56 to 60 of the Ruling.

The Court goes on to state that despite a person's right to lodge complaints with their respective supervisory authorities on the lawfulness of data transfers to third countries and the latter's duty to examine it, if the said claims is considered unfounded, there must be a legal mechanism put in force to enable the claimant to dispute the findings of those authorities in a court of justice, so that subsequently it can refer the question, if the judge(s) so chooses, to the CJEU. Nevertheless, when a national supervisory authority comes to the conclusion that the claimant's arguments are solid enough to argue the invalidity of the legal instrument that enables the data transfer, it must; *"in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46...be able to engage in legal proceedings."*[28]

These procedures all derive from the fact that, although a national authority is competent to receive and examine a complaint of a person that may challenge the validity of an EU legal instrument, only the CJEU is able; *"…to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid"*[29] *, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly…."*[30]

After finding that any national EU supervisory authority should act on a complaint of a natural person concerned with the existence of a level of adequate protection in a third country to which their personal data is being transferred to, the court takes on the much more perilous task of assessing the grounds on which Safe Harbour has been built upon.

Referring to Article 25 (6) of the directive, the Court is unequivocal about how the level of adequate protection must be ascertained. Admitting that there is no definition of adequate protection laid down by the directive, it notes that; *"… provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals."*

Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country."[31]

To some extent, the Court lays down what is to be considered an adequate level of protection. It held that such a concept *"must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter."* This is not a definition, in itself, of the concrete terms on which such a legal concept can be fulfilled but, it does stress a theoretical construction that allows for further certitude. We earlier mentioned the plausible need for a third country, willing to receive data from the EU, to implement an independent supervisory authority or an equivalent public body with similar responsibilities and powers to oversee compliance requisites by companies and the public sector alike and, enforce whatever measures are deemed

[28] Paragraphs 63 to 65 of the Ruling.
[29] Articles 264 and 267 of TFEU regulate the effects of the declaration of invalidity.
[30] Para. 61 of the Ruling.
[31] Paragraphs 71 and 72 of the Ruling.

necessary to uphold the fundamental rights at stake.

The said legal order is, as the Court admits, a changing reality that must be continuously monitored by the Commission so that its adequacy level stays updated ("factually and legally").[32] Moreover, "the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict."

Regarding the SH scheme, the Court denotes various shortcomings. From the outset, the Court finds that a self-certification system, as is the case of SH, does not necessarily fall over the scope of Article 25 (6) of the directive but it still requires further assurances: *"the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice."*[33] On the other hand, the CJEU critically highlights the fact that only companies of the private sector are eligible for (and abide by) the SH scheme and not the public sector.[34] More troublesome is the fact that the SH scheme doesn't provide for adequate measures that make it possible for the US to uphold the adequate level of protection envisioned by Directive 95/46.[35]

Equally disturbing to the Court's understanding is paragraph 4 of Annex I to the Decision 2000/520 by which the principles of SH are dismissed under certain conditions, *"the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'."*[36]

This is, unequivocally, the problematic issue that dilutes the potency of Court's ruling. The bypass to the SH principles means not only that its effectiveness is called into question, but the mere likelihood of an adequate level of protection being respected is bleak, to say the least. Giving the US authorities and the SH adherents the ability to circumvent their obligations under such nebulous conditions has the potential to undermine any initiatives that could be introduced to ensure fundamental rights are better protected during the process of inter-jurisdictional data transfers.

Besides, in Decision 2000/520 there is no evidence whatsoever of *"the existence of effective legal protection against interference of that kind."* The different approach of both sides of the Atlantic is well documented by the fact that SH only acknowledges the need for dispute resolutions under this scheme for commercial purposes and cannot be summoned to resolve the main issue at stake, i.e., the *"legality of interference with fundamental rights that results from measures originating from the State."*[37]

The Court quotes the *Commission's Communication COM(2013) 846 final*, notably stressing the fact that *"…the Commission found that the United States authorities were able*

[32] Para. 76 of the Ruling.
[33] Para. 81 of the Ruling.
[34] Para. 82 of the Ruling.
[35] Para. 83 of the Ruling.
[36] Para. 84 of the Ruling.
[37] Para. 89 of the Ruling.

to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security…." Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.[38] There were no *"…clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data."*[39]

Both the purpose limitation and the necessity principles were at stake, posing constant and unforeseen threats to the Charter's (Article 8) and the directive's (Chapter 2) basic grounds over which data processing is legally admitted.

A further point was made against the fact that *"…any differentiation, limitation or exception [was] being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail"*[40] *"in complete contradiction not only with the directive but also with the case law of the Court."*[41] Such a generalised violation of a person's right to respect for private life together with the lack of remedies provided to the ones affected by such violation could not be tolerated by the Court.

Given the Commission's non-compliance with the need to factually present the case with specific, "identified and identifiable" legal arguments for the backing of any adequate level of protection ruling, the Court found *"…that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is, therefore invalid."*[42]

In what concerns Article 3[43] of Decision 2000/520, the Court was much more

[38] Para. 90 of the Ruling.

[39] Para. 91 of the Ruling.

[40] Para. 93 of the Ruling.

[41] Judgment *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, by which the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC were declared invalid.

[42] Par. 98 of the Ruling.

[43] Article 3 (1) read as follows:

Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance

succinct, stating that the conditions posed onto supervisory authorities were to *"… be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the Directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals."*[44]

As with Article 1, Article 3 was also ruled invalid together with all the remaining articles of Decision 2000/520.

4. A new "Crooked Harbour"?

Since the beginning, SH has been the practical response to a theoretical problem. As the economic importance of data, and personal data in particular, rose at the verge of the 21st century, the legal frameworks that tried to respond to the challenges posed by the increasing new industry of data gathering and data processing had to play catch-up in a very dynamic atmosphere. In this regard, it is well known that both EU and the US have been at the forefront of this integral part of the new technological revolution.[45]

As the writers said in the beginning of this paper, the SH scheme appeared to be a good willed product designed to render the impossible possible, a legal tool that would allow two different legal frameworks to operate harmoniously. The fact of the matter is that even at early stages of the implementation of SH, numerous doubts emerged over its applicability and conformity with EU law.

The Article 29 Working Party (henceforth, WP) was one of the most notorious agents to voice out those doubts. On its Opinion 4/2000,[46] concerning the level of protection provided by the "SH Principles", the WP took note of some of the shortcomings that the Court underlined:

> • *"Since adherence to SH is based on self-certification, without any kind of ex-ante verification, the supervisory powers of a public body are essential for the credibility of the arrangement."*[47]
> • The WP reiterates its view that adherence to the principles should only

with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

[44] Para. 102 of the Ruling.

[45] This new industrial revolution is one of a sheer magnitude as Victoria Espinel, President and CEO of the Business Software Alliance, demonstrated on her opening statements during the joint hearing of the Subcommittee on Commerce, Manufacturing, and Trade with the Subcommittee on Communications and Technology, Committee on Energy and Commerce, gathered to "Examin[e] the Eu Safe Harbor Decision and Impacts for Transatlantic Data Flows." Ms. Espinel started by pointing out that "While the 19th century was powered by steam and coal and the 20th century by electricity, cars, and computers, the 21st century runs on data.", she then referred to the actual numbers that sustained her claims stressing that "More than 90 percent of the data that exists in the world today was created in the last 2 years alone, and that is a rate of change that will continue to increase exponentially. The volume of business data worldwide is doubling every 15 months…" The preliminary transcript of the hearing is available at http://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-Transcript-20151103.pdf.

[46] Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf.

[47] Page 3 of the Opinion.

be limited to the extent necessary to comply with conflicting obligations and that, for reasons of transparency and legal certainty, the Commission should be notified by the DOC of any statute or government regulations that would affect adherence to the principles. Explicit authorisations, such as a reason for exceptions could be accepted only in so far as the overriding legitimate interests underlying such authorisations do not substantially differ from exemptions or derogations applied in comparable contexts by EU Member States in accordance with their laws implementing the Directive.[48]

- The "bridge" between the two layers is very uncertain. According to FAQ 11, the Alternative Dispute Resolution (henceforth ADR) bodies should notify the FTC of cases of failure to comply with the principles, but there is, currently, no obligation for them to do so. Although the individuals concerned can complain directly to the FTC, there is no guarantee that the FTC will examine their case (its powers are discretionary). Additionally, individuals would not have the right to be heard before the FTC, to enforce the ADR bodies' decisions before it, nor to challenge such decisions (or the lack of decisions). As a result, the individuals concerned by an alleged violation of the principles would not be assured of the right to stand before an independent decision making body.[49]

The awareness of these and other issues that hindered SH from the outset have been at the centre of current negotiations between the EU and the US. The *Schrems* case was, no doubt, a very tough blow to the current talks and certainly had a big impact on, not only the subjects addressed, but also the timing of the negotiations.

As the Court clearly stated on paragraph 81 of the ruling, there is nothing standing in the way of a (renewed) system of self-certification as a legal mean to transfer data between the EU and the US, but there are currently so many loopholes to be filled that a critical analysis of such a solution cannot bypass the severe difficulties that come into play.

Initiatives such as the *"Privacy Bridges - EU and US privacy experts in search of transatlantic privacy solutions"*[50] presented on the last international data protection conference[51], are obviously welcomed. The ten *"bridges"* put forward have their own merits and it cannot be overly stressed that both sides of the Atlantic must come together and work on subjects such as clearer user control or applying best practices for de-identification of personal data or for security breach notifications.

But the fact of the matter is that we tend to agree with Marc Rotenberg's[52] view, expressed when addressing the US House of Representatives last October; *"The Safe Harbour Framework is an industry-developed self-regulatory approach to privacy protection that simply does not work. Coordinated by the Department of Commerce, the Safe Harbour program allows US companies to self-certify privacy policies in lieu of complying with legal requirements for*

[48] Page 5 of the Opinion.
[49] Page 7 of the Opinion.
[50] Available at https://www.privacyconference2015.org/wp-content/uploads/2015/10/Privacy-Bridges-Paper-release-version.pdf.
[51] The annual International Data Protection Conference took place in Amsterdam, from the 23rd to the 29th of October 2015, gathering data protection authorities together with data processors, data controllers and NGO's.
[52] President of the Electronic Privacy Information Center "EPIC".

the processing of data of Europeans."[53]

The ocean that still separates the EU and US spawns out of different conceptual approaches and not out of a lack of goodwill. The commercial bias and the consumer trust concern entailed into the US privacy policies builds a theoretical and practical trench that clearly divides the two continents. This is not to say that the US doesn't look at privacy as a fundamental right, for as Peter Swire[54] demonstrated in his most recent white paper, the US respect for the right to privacy has been a genuine topic of the US legislators: *"Following the resignation of President Nixon in 1974, Congress passed the Privacy Act of 1974, creating new protection against misuse of personal information by federal agencies. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), a path-breaking legal structure to address the problem of secret surveillance in an open society."*[55]

However, the balanced and meaningful changes that have occurred especially since the Snowden revelations[56] don't hide the significant differences that persist. Swire himself clarifies that his white paper doesn't concentrate on specifics of the different legal frameworks as he focuses on the *"adequate level of protection"* criteria: *"One aspect of this essential equivalence determination for Safe Harbour 2.0 will concern specific provisions of law, such as data subject access rights or the right to have an investigation by an independent data protection authority in the data subject's country. I leave that sort of essential equivalence analysis to other authors."*[57]

What effectively resonates from up-close viewing is the divergent path that both allies have trailed during the last three decades. Kenneth A. Bamberger and Deirdre K. Mulligan clinically highlighted this in their recent book *"Privacy on the ground"*[58] where the authors frame the US model on handling privacy policies as an issue of *"social license"* rather than legality.[59]

The authors demonstrate, through various interviews carried out with major privacy players on both sides of the Atlantic, that there are virtues and dangers to both approaches. Even if they may not conclude it in such a blunt way, the virtues of the US model come down to a much more integrated take on privacy by companies, something that has made them more aware of the incremental importance that this matter must receive in any big organization. US businesses have instituted stricter internal privacy policies than in some of their European counterparts.[60] Adversely, where legal compliance becomes the "alpha and omega" of privacy commitments within a company, few steps are given towards integrating privacy as an essential and integral part of management, leaving its intricacies almost exclusively up to

[53] Written testimony presented to the joint hearing of the Subcommittee on Commerce, Manufacturing, and Trade with the Subcommittee on Communications and Technology, Committee on Energy and Commerce, gathered to "Examin[e] the Eu Safe Harbor Decision and Impacts for Transatlantic Data Flows", available at http://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-Wstate-RotenbergM-20151103.pdf.

[54] Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business.

[55] Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013", 2015, available at https://fpf.org/wp-content/uploads/2015/12/Schrems-White-Paper-12-18-2015.pdf.

[56] Detailed in full by Peter Swire in Chapter 3 of the aforementioned White Paper.

[57] Page 9 *ob. cit.*

[58] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground*, 2015, MIT Press, Ebook edition.

[59] *Id.,* page 17.

[60] Germany follows the US closely on this matter, a fact surely related to its history of tortuous national secret intelligent agencies.

compliance divisions and legal counsellors.

A point can be raised about how the Europeans are getting closer to this perspective. With the new General Data Protection Regulation (hereinafter, GDPR)[61] it becomes mandatory to appoint Data Protection Officers (DPO's) in certain cases.[62] Although already in practice in some EU countries,[63] the potential dissemination of DPOs is a welcome step towards raising awareness of data protection issues within the organizations.

Although as important as DPO's may be, a unanimous agreement remains on the importance of independent data protection authorities[64] and their supervisory role. Deemed an essential aspect of the EU's data protection legal framework, the existence of independent DPOs remains one of the fundamental disagreements with the US. As it stands, the principle of adequate protection, as interpreted by the CJEU, cannot be met; the lack of an independent overview is a critical fault of the American data protection legislation and will not be mended easily given the reluctance of public officials to create such a body.

Nevertheless, in the paper's view, leaving the privacy framework almost entirely up to the companies' management to decide, produces an uneven playing field for businesses and generates complete uncertainty to the public. Without a comprehensive legal basis, fundamental rights may be left almost entirely up to the market's subjective approach, a scenario that cannot provide any rule of law enthusiast with plausible reassurance. Sensible legislation and effective enforcement are paramount, *"While respondents generally downplayed the role of compliance with legal rules in shaping corporate approaches to privacy, every single respondent interviewed mentioned two important regulatory developments they believed central to shaping the current "consumer expectations" approach to privacy: the behaviour of the FTC, and the enactment of state data breach notification statutes."*[65]

This perfunctory regard on the differences between the EU and US concepts doesn't leave the European faults at bay. It is true that the current legal environment in Europe amasses for much of the difficulties many businesses and even public entities face. Directives aren't meant to create a single undistinguished common legislation but account only for the harmonization of the EU Member States' laws.

The new GDPR are expected to come into play precisely to overlap these different legal systems and produce a privacy union. Novelties such as the One Stop Shop[66] or the Consistency Mechanism[67] or the end of prior notifications may come in handy for the personal data professionals, but it is essential that they don't come

[61] For the latest available version see https://iapp.org/media/pdf/resource_center/2015_12_15-GDPR_final_outcome_trilogue_consolidated_text.pdf.

[62] Article 35 of the GDPR:

"1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and data relating to criminal convictions and offences referred to in Article 9a.

[63] Germany, France and Hungary are just three examples of this.

[64] Chapter VI of the GDPR.

[65] *Ibid.,* page 68.

[66] Article 54 of the GDPR.

[67] Article 57, id.

at the expense of fundamental rights. Therefore we welcome the fact that Article 17 of the GDPR clarifies the scope of the right to erasure (or, as referred to by the CJEU, the "right to be forgotten")[68] and provides for a common approach to the enforcement issues faced by the DPOs, although the wording of the article seems to circumscribe the scope of the right, as originally envisaged by Court.[69] In the aftermath of the *Costeja* case, the WP of Article 29 issued its guidelines[70] on the implementation of the CJEU's ruling, laying a tentative common approach to a very complex situation. In fact, even with such guidelines, the DPO failed to produce a harmonized response to complaints based on the *Costeja* ruling.

Therefore, the EU must apply coherent decisions when applying the law (Directive or GDPR), always bearing in mind Article 7 and 8 of the Charter and avoiding unfavourable situations, such as the one resulting from the recent reaction to Google's New Privacy Policy and what it meant for the future of the purpose limitation principle.[71]

One thing is for certain, the new framework for data transfer prescribed by the GDPR doesn't seem to downsize the requirements to ascertain a country's adequate level of protection. In fact, it seems quite the contrary. As it stands, Article 41 presents a series of new conditions, namely *"…the Commission shall, in particular, take account of the following elements:*

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of this legislation, data protection rules professional rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, jurisprudential precedents, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Member States; and

---

[68] *Costeja* and AEPD *vs. Google Spain and Google Inc.*, Case C-131/12, May 2014.

[69] Para. 4 of the Ruling: "(...)without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."

[70] Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[71] Judith Rauhofer, "Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?", in *European Data Protection Law Review,* Vol. 1, 2015, p. 5-15.

c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

This only comes to support the claim that Safe Harbour 2.0 is not the way forward and that substantial upgrades are needed in US law, as the conditions aforementioned appear to be cumulative and not alternative. A simple tweak to the current (invalid) Decision will therefore be destined to fail, not only the CJEU's, but also the new GDPR criteria for judging the adequate level of protection.

Even if the recent Umbrella Agreement[72] makes amends for some of the lost time and, notwithstanding, the importance of the Judicial Redress Act (still to be passed by the US Senate), we stand by Marc Rotenberg when he posits that *"The Judicial Redress Act*[73] *does not provide adequate protection to permit data transfers and it does not address the many provisions in the Privacy Act that need to be updated."*

The application of the Privacy Act for non-US Persons is the cornerstone of the EU-US Umbrella Agreement. But the current proposed changes to the Privacy Act will not solve the problem as the right of judicial redress is far too attenuated. The much better approach would be to simply revise the definition of *"individual"* to mean *"natural person."*[74]

Alternatives such as Binding Corporate Rules (BCR's) or standard contractual clauses that remain in place for the meantime,[75] are not the solution for most of the intricate problems the *Schrems* case highlighted concerning SH. BCRs compliance alone can; *"…cost more than $1 million and take 18 months to fully implement, from development to approval, and they are limited to governing how personal data is used within a corporation…"* Another alternative, such as model contract clauses, might require a re-examination of tens of thousands of transfers. Model contract clauses are neither comprehensive nor flexible: They are largely impractical for when data is received directly from hundreds of customers.[76]

It should be reiterated that, even if this is currently a problem between the EU and the US, given the leading position both parties enjoy in what concerns personal data protection in the world, the reach of this matter is far greater than the sum of the two protagonists. The world looks with great attention to the EU and the US, copying most of the solutions put forward by the two front-runners.

Personal data is a global subject and will rapidly need a global solution. The recent appointment by the UN of the Special Rapporteur for Privacy is a clear signal of the continuous worldwide concern with privacy. Initiatives such as UN's Global Pulse, focused on the adequate use of Big Data in Humanitarian contexts shed

[72] Available at http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
[73] Available at https://www.congress.gov/bill/114th-congress/house-bill/1428/text.
[74] Page 15 of his written statement, cited in note 41.
[75] The Statement of The Article 29 Working Party of 16 October 2015 defers to the end of January 2016 a final common stance on what actions to take in the future given the ECJ's ruling, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.
[76] As claimed in his written statement presented to the joint hearing of the Subcommittee on Commerce, Manufacturing, and Trade with the Subcommittee on Communications and Technology, Committee on Energy and Commerce, gathered to "Examin[e] the Eu Safe Harbor Decision and Impacts for Transatlantic Data Flows" by John Murphy Senior Vice President for International Policy U.S. Chamber of Commerce, available at http://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-Wstate-MurphyJ-20151103.pdf.

light to the path of privacy in the international community and deserve a common, sensible but rigorous approach by the UN Member States.

5. Conclusion

The SH Decision is no more and the current negotiations between the EU and the US, although respectable, come at a very late stage and are bound to be hindered by the practical reality of living. As always, it is our opinion that the political environment continues to heavily influence will influence the outcome of the meetings. Furthermore, the ever growing terrorism threat, which remains a prominent issue in geo-political discourse, will most likely further protract the process of creating a major breakthrough on the legal aspects of the negotiation.

As it stands, the current legal framework for the transfer of data across the Atlantic is hanging by a thread while the EC, the Member States and its citizens and the companies, *inter alia*, await for the final decision from Article 29 WP regarding the remaining alternative mechanisms (e.g. BCR's). The ruling was very clear on what can or cannot be considered as a compliant with the principle of adequate protection in any third country, making a case for the "portability" of fundamental rights of EU citizens across the world. More than a direct attack to cultural relativism, the ruling of the Court provides the grounds for DPOs to act whenever necessary, reinforcing the independence that all supervisory bodies need to be vested with. After *Schrems*, one would not have to be incredibly adventurous in order to pass a preliminary judgment on the conformity of those mechanisms with the CJEU ruling. In reality, it's not a question of how these alternative means can assure an adequate level of protection in the US as much as it is a question of whether or not the US will implement significant changes to its own legal framework in order to respond to a foreign judicial decision. If we rely solely on the history of EU-US relations, than the chances of formulating a workable solution to this issue are dire to say the least.

However, the fundamental issue at stake does not end on US soil. The adequate protection principle transcends EU-US relations and applies to relevant jurisdictions in the world. For so long as a global solution to this contentious issue remains elusive, personal data transfers will continue to be embroiled in a wave of uncertainty and controversy.

Although unforeseeable in the near future, this will, likely, become the only way to guarantee that the rising global demand for data transfer occurs in a safe and legally binding environment where judicial redress is assured, credible oversight is instituted, enforcement actions are provided in due time and essential data protection principles are abided by.

In the meantime, personal data transfers will have to rely on short-term palliative solutions, such as bilateral commitments of uncertain legal credibility that are, constantly endangered by judicial disputes or technical time-consuming and costly undertakings of immense magnitude, such as moving all data servers collecting and processing EU citizens' personal data into EU territory.

Paraphrasing Robert A. Heinlein in the opening remarks of *"And he built a crooked house,"*[77] as he was referring to Hollywood, *"It's [Data Transfer]. It's not our fault – we didn't ask for it, [Data Transfer] just grew."*

[77] Robert Heinlein, *op. cit.* 9-61.