Rebooting US-EU Data Transfers in the Pipeline

The Resurrection of the Acclaimed Privacy Shield

István Sabjanics[*]

Abstract

On 25 March 2022 US President Biden and European Commission President von der Leyen announced that an agreement in principle had been struck by their negotiating representatives. This came two years after the CJEU declared invalid the Commission's Privacy Shield Decision regarding the adequacy of protection provided by the US. The joint announcement was welcomed with much anticipation. Economic and security concerns had been voiced on both sides of the Atlantic, while the desire to protect European privacy principles remain strong. Commission President von der Leyen underlined European hopes for a predictable and trustworthy data flow between the EU and the US, one that safeguards privacy and civil liberties. Not much has surfaced of the new deal. Still, with more than 20 years of experience in transatlantic data flow and two fatal decisions of the CJEU, we must assume that the proposal will yield more compliance with European data protection standards and less loopholes.

Keywords: data protection, Privacy Shield, GDPR, surveillance, Schrems.

1. Introduction

On 25 March 2022, Joe Biden and Ursula von der Leyen announced that their negotiating parties struck an agreement in principle on a refurbished data transfer agreement between the US and the EU.[1] It will be called Privacy Shield, according to the announcement. After more than a year of meticulous negotiations between the European and US delegations a common ground and a feasible proposal was reached. This breakthrough is crucial since the value of continued data flow produces more than USD 1 trillion in cross-border commerce on a yearly basis.[2]

The privacy law of the EU, the General Data Protection Regulation (GDPR) came into effect on 25 May 2018. It was considered a great achievement primarily in the eyes of supporters of privacy rights, but a contradictory decision at least, if not a Pyrrhic victory for those, who felt protective over the previously moderately

* István Sabjanics: senior lecturer, Pázmány Péter Catholic University, Budapest.

1 *See* at https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087.

2 *See* at www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

doi: 10.5553/HYIEL/266627012022010001012

challenged economic and technological development in the field of data processing, and data fusion in particular. In July 2020 the CJEU invalidated Decision 2016/1250 on the adequacy of the protection provided by the previous EU-US Data Protection Shield. The decision of the CJEU put several global communication service providers operating in the EU in peril.

2. Beginnings: The Safe Harbor Agreement (2000-2015)

Personal data of EU citizens or personal data collected in the EU cannot be transferred to a third country unless the European Commission finds that this third country in question provides an 'adequate' level of personal data protection. Yet this adequacy requirement does not have a clear cut definition, for neither the Data Protection Directive, nor the GDPR succeeded in defining it.[3] According to the Commission: under EU law, an adequacy finding requires the existence of data protection rules comparable to the ones in the EU. This concerns both the substantive protections applicable to personal data and the relevant oversight and redress mechanisms available in the third country.[4] So far 14 countries[5] received this appreciation and recognition by the Commission for their data protection systems, including the UK after its recent departure from the EU. The US data protection system has never been recognized as an adequate system comparable to its European counterpart under the Data Protection Directive and the GDPR, which meant certain pre-approved mechanisms were necessary: previously the Privacy Shield and before that, the Safe Harbor. There are other so-called secondary mechanisms[6] that allow for the transfer of personal data. These were also updated and modernized as the GDPR came into force, albeit with certain exceptions.[7]

The 2013 Snowden revelations on surveillance activities carried out by US authorities on a global scale, targeting EU countries[8] and EU citizens in the

3 Regulated previously under Article 25 Data Protection Directive, and today under Article 45 GDPR.

4 Opinion: Exchanging and Protecting Personal Data in a Globalised World. European Economic and Social Committee (Rapporteur: Christian Pirvulescu), at https://webapi2016.eesc.europa.eu/v1/documents/EESC-2017-03365-00-01-AC-TRA-EN.docx/content.

5 These are Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, United Kingdom, and South Korea.

6 These are the *(i)* Standard Contractual Clauses, sometimes referred to as Model Contracts, *(ii)* the Binding Corporate Rules, *(iii)* Passenger Name Records (PNR), and lastly *(iv)* the Terrorist Financing Tracking Program. The last two originating from obligations under international law.

7 Data controllers and processors can continue to rely on earlier forms of the Standard Contractual Clauses for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged. *See* at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

8 The surveillance of elected members of parliaments and members of governments, most notably Angela Merkel, who was Germany's chancellor at the time, resulted in EU-US relations plummeting.

doi: 10.5553/HYIEL/266627012022010001012

process, played a crucial part in losing trust in the prevailing system, one, that was based on the presumption that data transfers over the Atlantic took place in compliance with the Privacy Principles.[9] Vivian Reding, Vice-President of the European Commission at the time, cunningly even said that 'The Safe Harbor agreement may not be so safe after all'.[10] The infamous PRISM program is the flagship of the American global surveillance initiative, which grants access for the National Security Agency (NSA) to the massive amount of data gathered by major US-based tech companies, such as Google, Yahoo, Apple, Microsoft and Facebook.[11] These companies had hundreds of millions of clients in Europe and transfer personal data for processing to the US on a scale which is practically inconceivable.[12]

On 25 June 2013 Maximilian Schrems, an Austrian national, made a complaint to the Data Protection Commissioner of Ireland, complaining that Facebook Ireland Inc. transfers his personal data to the US, where it can be automatically and secretly accessed by American authorities. Schrems also asked the Commissioner to exercise his statutory powers to prohibit Facebook Ireland from transferring his personal data to the US. Schrems, referring to the Snowden revelations earlier that year, contemplated that the law and practice applicable in the US did not ensure an adequate protection of the personal data held in its territory against the surveillance activities carried out by public authorities.[13] The Irish Data Protection Commissioner dismissed the complaint, on the grounds that Schrems did not prove that the NSA actually accessed his data, and regardless of the likelihood of any misconduct, the Commission had previously decided that the US provides an adequate level of protection.[14]

Schrems then appealed to the High Court, which after due consideration found that the electronic surveillance and interception of personal data transferred from the EU to the US serve necessary and indispensable objectives in the public interest, such as national security, counterterrorism, and complying with other international obligations. The High Court also added that the Snowden revelations, published earlier that year, have demonstrated a 'significant over-reach' on the part of US authorities, and in particular the NSA.[15] The High Court stated that Union citizens have no effective right to be heard in regard of the indiscriminate surveillance and interception carried out by US agencies and authorities on a large scale.[16] The High Court held that the mass and

9 These Privacy Principles were notice, choice, onward transfer, security, data integrity, access, and enforcement.

10 *See* at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_710.

11 Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, at www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf.

12 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU, COM/2013/0847, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0847.

13 Judgment of 6 October 2015, *Case C-362/14, Schrems,* ECLI:EU:C:2015:650, para. 28.

14 Id. para. 29.

15 Id. para. 30.

16 Id. para. 31.

undifferentiated access to personal data is clearly contrary to the principle of proportionality, should the case solely be decided on the basis of Irish national law, the fundamental values protected by the Irish Constitution.[17] The High Court stated that Schrems did not question the validity of the Safe Harbor decision, yet in reality this must come under due scrutiny eventually.[18]

Whether the Safe Harbor Decision precludes Member States' data protection authorities from assessing the adequacy decision on the level of protection afforded by the US or not, was one of the questions referred to the CJEU by the High Court. It was assumed unreasonable to allow Member States' institutions to investigate proceedings based on the decision of an EU institution, if meaningful evaluation is *ab ovo* out of the question, since such decisions cannot be found unlawful by Member States' institutions. It would take only one Member State's institution to find the protection provided by the US inadequate for it to automatically defeat the sole purpose of the Safe Harbor Decision. Measures of EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.[19] For this reason it was no surprise that Advocate General Yves Bot advised the CJEU to find the Safe Harbor Decision all together invalid[20] with prevailing practices on international data transfers to be reviewed case-by-case by Member States' data protection authorities. Considering the apprehensive criticism voiced by European governments towards Washington following the Snowden-revelations, the lack of a Safe Harbor Decision meant that in due course the Member States' decision to suspend data flow became more than just a possibility, much rather a probability.

On October 2015 the Grand Chamber of the CJEU found the Safe Harbor Decision invalid based on the following four arguments. *(i)* The CJEU emphasized the importance of privacy and data protection, with reference to the freedom of thought, expression, and information under the EU CFR.[21] *(ii)* The exception for private companies meant that national security, public interest, or law enforcement requirements have primacy over the Safe Harbor Principles.[22] The CJEU further noted that US law did not contain any rule of exception for the surveillance of EU citizens,[23] which created a generalized process lacking any differentiation, limitation or exception, hence it was in clear violation of EU and Irish law regarding the essence of the fundamental right to respect for private

17 Id. para. 33.
18 Id. para. 35.
19 Id. para. 52; *see also* Judgment of 5 October 2004, *Case C-475/01, Commission v Greece*, ECLI:EU:C:2004:585.
20 Opinion of Advocate General Bot Delivered on 23 September 2015 (AG Opinion), *Case C-362/14, Schrems,* ECLI:EU:C:2015:627, paras. 183 and 216.
21 *See* Articles 7-8, and 10-11 EU CFR.
22 *Case C-362/14, Schrems,* para. 28.
23 Id. para. 88.

doi: 10.5553/HYIEL/266627012022010001012

life.[24] *(iii)* The US Federal Trade Commission (FTC) had the enforcement role over the Safe Harbor Principles, excluding the processing of personal data by public authority.[25] The legal safeguards in the system were incomplete in this regard, and in effect, EU citizens were left with no administrative or judicial means of redress,[26] resulting in a clear violation of the right to an effective remedy and to a fair trial under Article 47 EU CFR. *(iv)* Respect for fundamental rights is a condition for the validity of EU acts under the landmark *Kadi* decision.[27] Since the essence of these rights was violated, a more thorough examination of the legal act in question[28] or the assessment against the principle of proportionality was deemed unnecessary by the CJEU.[29]

3. Following Snowden and Schrems I: Privacy Shield (2016-2020)

Even before the Snowden-revelations, there were calls for a revision of the Safe Harbor Agreement as it contained a number of data protection loopholes, as certain European privacy advocates claimed.[30] Following the invalidation of the Safe Harbor decision the future of data flow between the US and the EU was uncertain, which was especially damaging for the economy reliant on data transfer. Discussions between EU and US officials on revising and updating the Safe Harbor Agreement began in late 2013,[31] partially in response to growing European concerns about surveillance programs carried out by US authorities and other subsequent allegations of US intelligence collection operations in Europe.[32] In addition, the Safe Harbor Agreement dated back to the beginning of the Internet, resulting in an unavoidable tension between the prevailing legal provisions and the existing technological advances. European criticism eventually had an effect on the FTC's approach to privacy claims against US companies.[33] Among other problems there were European concerns that some companies failed to completely implement Safe Harbor requirements, due to a lack of mandatory

24 Id. para. 94. *See also* Judgment of 8 April 2014, *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and others,* ECLI:EU:C:2014:238, para. 39.

25 *Case C-362/14, Schrems,* AG Opinion, para. 205, citing FAQ 11 in Annex II to Decision 2000/520 and Annexes III, V and VII. *See also C-362/14, Schrems,* judgment, para. 89.

26 *C-362/14, Schrems,* para. 94.

27 Judgment of 18 July 2013, *Joined Cases C-584/10 P, C-593/10 P, and C-595/10 P, Kadi,* ECLI:EU:C:2013:518, para. 66.

28 *C-362/14, Schrems,* para. 98.

29 Article 52(1) EU CFR.

30 Nikolaj Nielsen, 'Hundreds of U.S. Companies Make False Data Protection Claims', *EUobserver.com*, 8 October 2013, at https://euobserver.com/rule-of-law/121695.

31 The actions set out by the European Commission to restore trust in data flows between the EU and the US, were released on 27 November 2013.

32 European Commission, *First Vice-President Timmermans and Commissioner Jourova's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems)*, Press release, 6 October 2015.

33 Wilson Sonsini Goodrich & Rosati, *FTC announces settlements for allegedly false Safe Harbor compliance claims*, 6 February 2014, at https://sites.law.berkeley.edu/thenetwork/2014/02/06/ftc-announces-settlements-for-allegedly-false-safe-harbor-compliance-claims/.

annual compliance checks, which most probably induced companies to falsely claim they complied with requirements. This concern was deepened by the previous inactivity of the FTC in bringing actions against US companies. This omission was apparent, since only ten companies came under investigation during the first 13 years of the Safe Harbor Agreement.[34]

Criticism arose from European data protection officials and Members of the European Parliament, regarding specific major US based companies, such as Google and Microsoft, for their alleged involvement in the US surveillance program affected most citizens of the EU. This prompted a call for suspending the Safe Harbor Agreement. The proposal for suspension was eventually rejected, for the European Commission gave more weight to possible negative effects for EU business interests and overall, the Transatlantic economy on both sides. The negotiations between EU and US officials starting in November 2013 focused on key topics considered to be most problematic by European data protection officials: *(i)* enhancing transparency, *(ii)* ensuring redress, *(iii)* strengthening enforcement, and *(iv)* limiting the access of US authorities to dataflows under Safe Harbor.[35] All four topics purposely lacked detail, allowing representatives room for negotiation. The US' national security interests and European demands to ensure limited access seemed irreconcilable in practice, both before and after the CJEU judgment and all through the negotiations. On 2 February 2016 Penny Pritzker, the US Secretary of Commerce at the time, two days after the 31 January deadline established by the Article 29 Working Group, made the announcement that negotiations had been completed. The work-title Safe Harbor 2.0 previously in use was finalized as 'Privacy Shield' which also implied the intention of rebranding the outcome. On 29 February 2016, US and EU officials released the full text of the agreement and the supporting documentation. The Privacy Shield framework was substantially longer and encouragingly more detailed than the previous Safe Harbor.[36] The US Government noted that this

> "historic agreement is a major achievement for privacy and for businesses on both sides of the Atlantic. It provides certainty that will help grow the digital economy by ensuring that thousands of European and American businesses and millions of individuals can continue to access services online."[37]

The Privacy Shield principles covered seven distinct categories: *(i)* notice, *(ii)* choice, *(iii)* accountability for onward transfer, *(iv)* security, *(v)* data integrity and

34 Martin A. Weiss & Kristin Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, Congressional Research Service, 19 May 2016, at https://sgp.fas.org/crs/misc/R44257.pdf.

35 *See* European Commission, *European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows*, Press prelease, 27 November 2013, at http://europa.eu/rapid/press-release_IP-13-1166_en.htm; *see also* Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU, 27 November 2013.

36 Department of Commerce, EU-US Privacy Shield, Washington, DC, 29 February 2016.

37 Article 29 Data Protection Working Party, Minutes of the 103rd meeting of the Article 29 Data Protection Working Party.

doi: 10.5553/HYIEL/266627012022010001012

purpose limitation, *(vi)* access and recourse, and *(vii)* enforcement and liability. Essentially, the goal was to mirror, or at least attempt to mirror, the requirements of EU law. It was mandatory for all participants to comply with this new regime. The rules of conduct acted as a bridge between EU and US regulatory systems. The Privacy Shield regulation was in substance a softer version of EU data protection law. From the American perspective it was a reinforced US information privacy law. Provisions around sensitive data, secondary liability, the role of data protection authorities, human resources data, pharmaceutical and medical products, and publicly available data were also included in a supplemental set of principles in laid down in the Privacy Shield.

Addressing the foremost European concerns after the Snowden-revelations, the Privacy Shield accommodated five written commitments in the form of letters from US national security officials, about protection guaranteed under the Privacy Shield with regard to EU citizens' data. These letters from US institutions aimed at clarifying both parties' understanding and commitments from the US side. The letters were principally made up of *(i)* an International Trade Administration Letter[38] and the Arbitral Model, *(ii)* a letter from US Secretary of State John Kerry to Commissioner Jourova[39] and the Ombudsperson Mechanism,[40] *(iii)* a letter from FTC Chair Edith Ramirez to Commissioner Jourova,[41] *(iv)* a letter from the Director of National Intelligence (DNI) to the US Department of Commerce,[42] and *(v)* a letter from US Deputy Assistant Advocate General Bruce Schwartz to the Department of Commerce.[43] These letters are political commitments of the US Government by nature, reassuring the EU that US institutions will take the Privacy Shield's requirements seriously.

In 2018 the Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-US Privacy Shield focused on two areas, to which certain recommendations were made: *(i)* the commercial aspects of the program, and *(ii)* the access by US authorities to data of EU citizens transferred through it.[44] As far as the commercial considerations were concerned, the report mostly focused on (re)-certification, compliance monitoring, enforcement, and complaint handling. In terms of numbers, Privacy Shield proved to be at least as attractive as the previous Safe Harbor Agreement, after its first two years in force, the amount of involvement remained practically unchanged, over 3,800 companies had signed-

38 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0M.
39 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0b.
40 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.
41 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v.
42 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F.
43 *See* at www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0W.
44 Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-US Privacy Shield, COM(2018) 860 final, at https://ec.europa.eu/info/sites/default/files/staff_working_document_-_second_annual_review.pdf.

up and became certified under the program.[45] Additional elements were integrated into the certification procedure by the US Department of Commerce.

During the first annual review meeting it emerged that companies publicly referred to their adherence to the Privacy Shield even before their certification had been finalized by the US Department of Commerce. To avoid legal uncertainty and false claims, the Commission recommended that companies not be allowed to make public representations about their Privacy Shield certification before the US Department of Commerce had finalized the certification and included the company on the Privacy Shield list.[46] The US Government published an additional guidance on the Privacy Shield's website to clarify the procedure.[47] The report listed specific areas suggested by the Commission, that were in need of improvement, such as deeper engagement in awareness raising and cooperation between EU and US authorities. The report finally included a discussion on potential divergences in certain areas of data processing, that will need to be addressed in the future. These included automated individual decision-making and the definition of human resources data. It is obvious that US authorities can access data transferred to the US through the Privacy Shield, since protective orders were incorporated as approved procedures. Nonetheless, public authorities' access is regulated by law, specifically by the Foreign Intelligence Surveillance Act (FISA)[48] and the Stored Communications Act.[49] The US government made additional reassurances that bulk data collection is only an exceptional mechanism that in any case may never happen to personal data transferred under Privacy Shield.[50] The US Inspector General for the Intelligence Community "confirmed that any referral from the Privacy Shield Ombudsperson would receive his serious, timely and effective attention."[51]

On 6 July 2020 the CJEU delivered its decision on what is now referred to as *Schrems II*. Following the *Schrems I* judgment and the subsequent annulment by the referring court of the decision rejecting Schrems's complaint, the Irish supervisory authority asked Schrems to reformulate his complaint in the light of the ruling of the CJEU that Decision 2000/520 was invalid.[52] In his reformulated complaint lodged on 1 December 2015, Schrems claimed, *inter alia*, that US law requires Facebook Inc. to make the personal data transferred to it available to certain US authorities, such as the NSA and the Federal Bureau of Investigation. He submitted that, since that data was used in the context of various monitoring programs in a manner incompatible with Articles 7, 8 and 47 of the Charter, the

45 Id. p. 4.
46 Id. p. 6.
47 US Department of State Privacy Shield Ombudsperson, at www.state.gov/e/privacyshield/ombud/.
48 50 USC 36, para. 1081 *et seq.* Foreign Intelligence Surveillance Act (FISA).
49 18 USC ch. 121, Stored Wire and Electronic Communications and Transactional Records Access.
50 2nd Annual Review of the Functioning of the Privacy Shield, p. 25.
51 Maximin Orsero, *Understanding the data privacy divide between the United States and the European Union*, Lund University, 2019, p. 50.
52 *Judgment in Case C-311/18 Press and Information Data Protection Commissioner v Facebook Ireland and Maximillian Schrems,* CJEU Press release No 91/20, Luxembourg, 16 July 2020, p. 1.

doi: 10.5553/HYIEL/266627012022010001012

SCC Decision[53] cannot justify the transfer of that data to the US. On these grounds, Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.[54]

As Recital of the Privacy Shield Decision establishes, the US Foreign Intelligence Surveillance Court (FISC) does not authorize individual surveillance measures under Section 702 FISA. Instead, it authorizes surveillance programs[55] based on annual certifications prepared by the US Attorney General and the DNI. Since these operations usually lack the focus of an individual target, the certifications to be approved by the FISC contain no information about the individual persons to be targeted, but rather identify categories of foreign intelligence information. This way, the FISC does not assess under a probable cause or any other standard that individuals are properly targeted to acquire foreign intelligence information. However, it covers the purpose of the acquisition to obtain foreign intelligence information.[56] The FISA also claims to provide a number of remedies, available also to non-US citizens, when they challenge unlawful electronic surveillance. Individuals even have the right to challenge the legality of surveillance, and may seek to suppress the information in the event the US government intends to use or disclose any information obtained or delivered through electronic surveillance against the individual in judicial or administrative proceedings in the US.[57] Although the exception of national security purposes is regulated in this way,[58] it is also accepted by the Commission that not all legal bases that US intelligence authorities may use[59] are covered by the avenues of redress open for EU data subjects.

The High Court of Ireland found that Executive Order No. 12333 allows the NSA to access data *in transit* to the US by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before they arrive in the US and become subject there to the FISA. Thus, these activities conducted pursuant to Executive Order No. 12333 were not governed by statute.[60] In addition to this, the NSA's activities based on Executive Order No. 12333 were not subject to judicial oversight and were not justiciable.[61] Therefore, Executive Order No. 12333 did not confer rights which were enforceable against the US authorities in the courts.[62] The High Court of Ireland disputed that Section 702

53 The interpretation and validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016.

54 Judgment of 16 July 2020, *Case C-311/18, Facebook Ireland and Schrems,* ECLI:EU:C:2020:559, para. 44.

55 Like the infamous PRISM and UPSTREAM.

56 Commission Implementing Decision (EU) 2016/1250 (Privacy Shield Decision), Recital (109), at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

57 Id. Recital (112).

58 Id. Recitals (113)-(114).

59 Like the ones covered by Executive Order No. 12333.

60 *Case C-311/18, Facebook Ireland and Schrems,* para. 63.

61 Id. para. 65.

62 Id. para. 182.

of the FISA, Executive Order No. 12333, read in conjunction with Presidential Policy Directive No. 28, correlated to the principle of proportionality found in EU law. With that in mind, it could be doubted that the surveillance programs in question could be regarded as limited to what is strictly necessary.[63]

Judicial redress possibilities for surveillance under FISA offered limited causes of action and claims would be declared inadmissible where the individual cannot show standing which ultimately restricted access to ordinary courts.[64] The High Court of Ireland stated that EU citizens did not have the same remedies as US citizens in respect of the processing of personal data by US authorities. The Fourth Amendment to the US Constitution, which constitutes, in US law, the most important cause of action available to challenge unlawful surveillance, did not apply to EU citizens. There were substantial obstacles in respect of the causes of action open to EU citizens, in particular that of *locus standi*, which it considered to be excessively difficult to satisfy. Lastly, the Privacy Shield Ombudsperson did not qualify as a tribunal according to Article 47 of the Charter, therefore, the level of protection was essentially not equivalent to that guaranteed by the fundamental right enshrined in the Charter.[65]

Be that as it may, the Commission considered that the US ensured an adequate level of protection for personal data transferred from the EU to certain self-certified organizations in the US under the EU-US Privacy Shield Agreement.[66] The Advocate General in his opinion called into question the Commission's previous finding that the US provide an adequate level of protection of personal data transferred from the EU to the US, thus calling into question the validity of the Privacy Shield Decision.[67] The CJEU took the findings of the Commission and the opinion of the Advocate General into consideration,[68] and found that Article 1 of the Privacy Shield Decision was incompatible with Article 45(1) GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and was therefore invalid.[69]

4. Hopes and Concerns Surrounding the Privacy Shield 2.0 Proposal (Announced in February 2022)

On 25 March 2022 US President Biden and European Commission President von der Leyen announced that the US and the EU have struck an agreement in principle on a revamped Privacy Shield data transfer agreement. Representatives of the US and the EU have been negotiating the agreement for almost two years now. Von der Leyen called the agreement a political breakthrough, responding to

63 Id. para. 184.
64 Privacy Shield Decision, Recital (115).
65 *Case C-311/18, Facebook Ireland and Schrems,* para. 65.
66 Privacy Shield Decision, Recital (136).
67 *Case C-311/18, Facebook Ireland and Schrems,* para. 160; Opinion of Advocate General Saugmandsgaard Øe Delivered on 19 December 2019, *Case C-311/18, Facebook Ireland and Schrems,* ECLI:EU:C:2019:1145, paras. 175-177.
68 *Case C-311/18, Facebook Ireland and Schrems,* judgment, paras. 191-193.
69 Id. para. 199.

doi: 10.5553/HYIEL/266627012022010001012

the hopes of Europeans for a predictable and trustworthy data flow between the EU and the US, one that safeguards privacy and civil liberties. Still, some issues are still on the table, such as effective legal redress from a European perspective, which still need resolving.[70]

In summary, we must take stock of certain issues, before we claim victory. *(i)* Firstly, there is an economic ambition that must be addressed. US President Biden stated that the framework would allow the authorization of Transatlantic data flows that facilitate USD 7.1 trillion in economic relations.[71] A relationship that is fruitful on both sides of the Atlantic and a lifeline for several businesses in areas from payroll processing to social media display. Lesser or ineffective regulatory limitation on data processing is obviously a goldmine for companies in the data processing business, but the threat of losing the European market is far too risky for them. Consequently, their willingness to comply with European data protection standards is almost certain. *(ii)* Secondly, public interests, namely national security is an acceptable exception recognized under the Charter and the GDPR. The US is the closest ally of its European partners with formidable intelligence capabilities. Thus, we can safely assume that the European counterparts of the NSA would graciously accept relevant information on counterterrorism. Should the opportunity present itself where illegally obtained data could prevent a terrorist attack, every European government would undoubtedly choose security over privacy. *(iii)* Thirdly, there are some legal issues that came to light in the CJEU's decision invalidating the Privacy Shield Decision of the Commission, to which no satisfying solution has been proposed as of yet. It is a well-known fact that the US's privacy regulation is best described as a patchwork consisting of state and federal level regulation. The lack of binding law, that provides a clear understanding of the principles of data protection, the rights of the data subject, the obligations of the data controller and the data processor unsurprisingly causes loopholes in the legal system. The method of self-certification used in the US under the Privacy Shield protocol provides even more opportunities for those who seek to bypass European data protection standards. The fact that there is a systematic discrimination by forums of possible remedies against those non-US citizens who do not reside within the US, raises some concerns. And *(iv)* lastly, from a European perspective at least, it is a wonder, how a relatively vaguely composed statute can endure a coexisting Executive Order that basically contradicts the essence of the statute in question, and eventually authorizes a public authority to pursue activities without any consideration to the statute or other legally binding documents.

Without wanting to sounding too pessimistic, we must hope for the best with the newly updated Privacy Shield in the pipeline, but trust is a two-way street. In light of the earlier conduct of the US public authorities, it is better to

70 Vincent Manancourt, 'EU, US strike preliminary deal to unlock transatlantic data flows', *Politico*, 25 March 2022, at www.politico.eu/article/eu-us-strike-preliminary-deal-to-unlock-transatlantic-data-flows/amp/.

71 Id.

stay vigilant from the start and maintain a watchful eye on processes in the long run.

Hungarian Yearbook of International Law and European Law 2022 (10) 1
doi: 10.5553/HYIEL/266627012022010001012