Marquette Intellectual Property & Innovation Law Review

Volume 27 | Issue 1 Article 6

Winter 2023

International Tax Agreements as the Final Push for US Adoption of Adequate Protection in Connection with the GDPR

Olivia Hansen

INTERNATIONAL TAX AGREEMENTS AS THE FINAL PUSH FOR US ADOPTION OF ADEQUATE PROTECTION IN CONNECTION WITH THE GDPR

OLIVIA HANSEN

I. INTRODUCTION

With the world becoming increasingly interconnected, there have been growing concerns of how to protect private information while allowing for the flow of data, that is used to fulfill lawful purposes, to an efficient degree. Privacy regulations are coming to fruition all over the world, yet conflicts between different countries and businesses on how to abide by these policies, as well as maintain their own focuses, is leading to issues. Those conflicts and concerns are becoming progressively clearer as privacy relations between the United States ("US") and the European Union ("EU") become more tense. With recent decisions such as *Schrems II*, bilateral tax agreements are at risk of falling apart, with tax enforcement and privacy law cooperation standing in the crossfire.

As noted in Forbes, consumer data started being collected in the 1980s but became more prevalent in the 1990s due to the rise of consumer internet; however, much of the data being collected was done without any regulation.[1] The consumer voices calling for regulation started slow but ramped up as consumers became aware of what their information was used for and how much information was truly being collected and stored.[2] The rise of consumer voices calling for regulation, due to the mistrust in information being collected coupled with government action, as well as industry actors, leads to the change and growth in data collection regulation.[3]

The EU drafted one of the most prominent and conservative privacy regulations, known as the General Data Protection Regulation ("GDPR").[4] The GDPR is a collection of data protection laws that sets forth a way to collect,

1. Swish Goswami, *The Rising Concern Around Consumer Data and Privacy*, FORBES (Dec. 14, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=206a674d487e.html.

2. *Id.*

3. Hossein Rahnama & Alex "Sandy" Pentland, *The New Rules of Data Privacy*, HARVARD BUSINESS REVIEW (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy.html.

4. *See generally* Commission Regulation 2016/679 of April 27, 2016, O.J. (L119) (EU) [hereinafter EU Reg. 2016].

store, and share personal information with others.[5] The GDPR went into effect in May 2018, replacing the former EU Data Protection Directive.[6] Furthermore, the GDPR describes the rights of the people who reside in the EU in connection with their information.[7] These rights are articulated as: Right to be Informed (Article 12)[8], Right of Access (Article 15)[9], Right to be Forgotten (Article 17)[10], and Right to Object (Article 21).[11] The GDPR has widespread implications on many countries, government agencies, entities, and individuals as the current policies are some of the strictest forms of enforced data protection.[12] Due to the breadth of affected parties, the GDPR infiltrates many areas including tax law.[13]

Tax law works at a variety of diverse levels, including state, federal, national, and international.[14] Entities and individuals may be tax liable in more than one country for a variety of reasons, including job location, citizenship, residential status, place of incorporation, and subsidiaries.[15] International tax law ensures that the income of the taxpayer is taxed once, rather than multiple times by each jurisdiction.[16] Countries enter into international tax agreements to set forth which country will tax specific income and which country will have laws in place to limit the ability of taxpayers to minimize and evade their tax burden.[17] Tax authorities use these tax agreements to collect information about the taxpayers to collect the right amount of taxes, ensuring that taxpayers are, in fact, paying taxes, and to investigate any issues with taxation.[18]

This Comment seeks to show that the relationship between the GDPR and the US government is at a tipping point, and the international tax agreements

5. *See generally id*.

6. *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.html (last visited Mar. 28, 2022) [hereinafter *History of the GDPR*].

7. EU Reg. 2016, *supra* note 4, at 1.

8. *Id*. at 39-40.

9. *Id*. at 43.

10. *Id.* at 43-44.

11. *Id.* at 45-46.

12. Kristin Archick and Rachel F. Fefer, *EU Data Protection Rules and U.S. Implications*, U.S. CONG. RES. SERV. (July 17, 2020), https://sgp.fas.org/crs/row/IF10896.pdf.

13. EU Reg, 2016, *supra* note 4, at 6.

14. *Tax Treaties*, INTERNATIONAL REVENUE SYSTEM, HTTPS://WWW.IRS.GOV/INDIVIDUALS/INTERNATIONAL-TAXPAYERS/TAX-TREATIES (last visted January 30, 2023).

15. *International Tax Rule*, TAX FOUNDATION, https://taxfoundation.org/tax-basics/international-taxrules/#:~:text=International%20tax%20rules%20define%20which,multiple%20times%20by%20multiple%20jurisdictions.html (last visited Mar. 28, 2022).

16. *Id.*

17. *Id.*

18. *Id.*

and the sharing of taxpayer information may be the final push to change US privacy policies. In order to show this, Section II will explain the current state of the US Privacy Regulations in relation to the GDPR by reviewing past legal issues, namely the two *Schrems* cases. Section III will examine US tax agreements with EU member states to highlight the sharing of information and policies in place, namely, the international income tax treaty between the US and France. Section IV will look at the potential conflict between the privacy regulations and the international income tax treaties with the US and EU member states. Finally, Section V will show the possible next step to allow for the continued exchange of information with the US, namely, with taxes, while still maintaining the rights prescribed under the GDPR to EU residents.

II. CURRENT STATE

The tension between the US and the EU's GDPR is often centered around the question of whether US laws ensure adequate protection for the data of individuals that is being collected and transferred.[19] The GDPR outlines when the transfer of data is allowed and what criteria must be established in order to maintain a lawful and protected transfer.[20] However, before the GDPR went into effect, the EU Data Protection Directive dictated the relationship, which held very similar goals.[21] Due to these criteria and legislation, outside countries had to show that they were able to provide adequate protection of personal data, while meeting mandatory criteria, in order to have data transferred out of the EU and into their country.[22] Though there is no clear definition set forth by the EU regarding what adequate protection is, the EU expects non-member countries to respect the rights, and take the necessary steps to protect these rights of the EU residents, when obtaining and transferring their data.[23]

In 2000, the US and EU negotiated the Safe Harbor Framework, which stated that US companies and organizations met the requirements of the EU Data Protection Directive and could legally transfer personal data out of EU member countries into the US.[24] Following the commencement of the Safe Harbor Framework, the European Commission adopted a decision aligned with this Framework, allowing for the transfer of data between EU member states

19. Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 ECLA:EU:2015:650, (Sept. 23, 2015).

20. EU Reg. 2016, *supra* note 4, at 60-62.

21. *History of the GDPR*, *supra* note 6.

22. EU Reg. 2016, *supra* note 4, at 60-62.

23. Case C-362/14, *supra* note 19.

24. Martin A. Weiss & Kristin Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, U.S. CONG. RES. SERV., p. 5, (May 19, 2016), https://sgp.fas.org/crs/misc/R44257.pdf.

and the US to go forward.[25] Many different actors relied on this Safe Harbor Agreement, and, so long as the organizations filed a certification with the US Department of Commerce to show that they still maintained the criteria set forth by the EU, they were allowed to collect and transfer data.[26] However, in 2015, this agreement came to an end as the Court of Justice of the European Union ("CJEU") issued a judicial decision in *Maximillian Schrems v. Data Protection Commissioner*.[27] This decision stated that the Safe Harbor Framework was void and could no longer be relied upon.[28]

In *Schrems*, Maximillian Schrems, an Austrian resident, used Facebook, Inc. ("Facebook"), a social media network, and raised a complaint that his private personal information was being transferred to servers belonging to Facebook, located in the US.[29] In the complaint, Schrems wished to exercise his rights, under EU laws, to prohibit his information being transferred because there were not adequate protections in place and thus, the Safe Harbor Framework failed to protect him.[30] This claim followed the Edward Snowden declarations regarding National Security Agency ("NSA") and other intelligence services in the US.[31] The CJEU analyzed the decision that allowed the Safe Harbor Framework to go into effect, alongside Schrems' complaint, concluding that the arrangement must end.[32] The CJEU ruled that data protection authorities are allowed to verify the adequacy of information transfer under the Safe Harbor Framework to ensure that adequate protection is in place.[33] During the investigation of the adequacy of information transfer, the CJEU determined that the US, in fact, lacked adequate protection to ensure the rights of EU residents and thus, the agreement was not valid.[34] One concern of the CJEU was that once the information has been transferred to the US, there

25. *Data Protection Commissioner v Facebook and Max Schrems (Standard Contractual Clauses)*, EPIC.ORG, **Error! Hyperlink reference not valid.**https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/#:~:text=The%20case%20(%E2%80%9CSchrems%20I%E2%80%9D,the%20EU%20and%20the%20US.html (last visited Mar. 28, 2022).

26. Anna Myers, *FTC Enforcement of the U.S.-EU Safe Harbor Framework*, IAPP., p. 2, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf.

27. *See generally* Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 ECLA:EU:2015:650, (Sept. 23, 2015).

28. *Id.* at ¶ 107.

29. *Id.* at ¶¶ 26-27.

30. *Id.* at ¶ 28.

31. *Id.*

32. *Id.* at ¶ 107.

33. *Id.* at ¶¶ 82-83.

34. *Id.* at ¶ 83.

were no rules or legislation that had been adopted in order to "limit any interference with the fundamental rights of the persons whose data is transferred" and that information "is capable of being accessed by the NSA and other federal agencies[.]"[35] The CJEU deemed that the lack of legislation and protection from federal agencies compiling private information fell below the adequate protection standard, and thus the Framework was invalidated which halted the legal transfer of EU residents' data.[36]

Following the decision in what is now known as *Schrems I*, the US and EU were forced to negotiate a new agreement that would allow for the transfer of data, while upholding the criteria needed under the EU Data Protection Directive and the CJEU's decision.[37] In 2016, the EU and US adopted a new piece of legislation, known as the EU-US Privacy Shield Framework.[38] The Privacy Shield, subsequently backed by a CJEU directive, stated that the US did have adequate protection measures in place, which allowed for the continuation of data transfers from the EU to the US.[39] Under the Privacy Shield, personal data could be transferred from the EU to US organizations if the organization was included in the publicly available Privacy Shield List, which was maintained by the Department of Commerce.[40] However, in 2020, the Privacy Shield Framework came into question as the CJEU delivered an opinion in the case, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*, ("*Schrems II*").[41] *Schrems II* questioned, if the US did not have adequate protection in place, (1) whether the contractual clauses established by the European Commission cover the delinquencies of the protections,[42] (2) whether those contractual clauses themselves were valid,[43] and (3) whether the transfers were legal under the GDPR, as it had now gone into effect.[44]

In an amended complaint filed by Schrems, he stated that the clauses in the agreement with Facebook are not consistent with the clauses established by the

35. *Id.* at ¶ 31.

36. *Id.* at ¶ 83.

37. *US-EU Safe Harbor Framework*, THOMSON REUTERS, https://ca.practicallaw.thomsonreuters.com/2-501-8616?transitionType=Default&contextData=(sc.Default)&first Page=true.html (last visited Mar. 28, 2022).

38. *Id.*

39. *Id.*

40. *Id.*

41. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶ 1 (Dec. 19, 2019).

42. *Id.* at ¶ 74.

43. *Id.* at ¶ 79.

44. *Id.* at ¶ 177.

European Commission, nor do they justify a transfer of his personal data.[45] Schrems' complaint again focuses on the fact that once the information is obtained and transferred to the US, there are no safeguards from US surveillance agencies obtaining the information, which violates the rights awarded to him within the EU.[46] In what became known as *Schrems II*, the CJEU noted that a transfer of data may take place where there is adequate level of protection; however, if there is no decision on adequate protection, there must be appropriate safeguards in place to protect the transfer, such as contractual clauses.[47]

During the CJEU's decision in *Schrems II*, the CJEU noted that US law does not offer remedies to EU residents where their personal data is transferred and processed in ways inconsistent with EU laws, and as such, the safeguards provided in the Standard Contractual Clauses ("SCC") do not bridge that gap.[48] Thus, the US lacks the ability to ensure adequate protection of EU residents and fails to maintain the fundamental rights and freedoms that the GDPR seeks to protect.[49] As the US failed to provide adequate protection, the CJEU determined, under *Schrems II*, the Privacy Shield Decision was invalid and could not be relied upon for the transfer of data out of EU member states.[50] Furthermore, the CJEU's decision highlighted the concern with using SCCs.[51] Although SCCs were not invalidated, the CJEU stated that if a country transfers and processes the private information of an EU resident based on SCCs, there must be a level of protection similar to the level provided by the GDPR.[52] In other words, the CJEU states that if the US seeks to use SCCs to obtain information, they must show that they are abiding by the rights of the GDPR—no matter the legal basis for the transfer of data.[53]

Since the ruling in *Schrems II*, there has been uncertainty of where the relationship and the standard for processing and transferring of personal data from the EU to the US stands and what the next move will be in order to comply with the GDPR and the standards set forth by the CJEU in their decisions.[54] Despite the invalidation of the Privacy Shield Framework, there is still allowance of transfers based on standard contractual clauses, so long as the US

45. *Id.* at ¶ 55.
46. *Id.*
47. *Id.* at ¶ 91.
48. *Id.* at ¶¶ 188-189.
49. *Id.*
50. *Id.* at ¶¶ 199-201.
51. *See generally id*.
52. *Id.* at ¶ 121.
53. *Id.*
54. *Id.*

abides by and upholds the rights afforded to EU residents under the GDPR.[55] However, there have been no changes in US policy to show that organizations and agencies are required to abide by the GDPR or offer the same protections as the GDPR.[56] Due to this inactivity, the current state of the relationship between the US and GDPR remains tense and uncertain. Without changes in US policy to guarantee the rights of EU residents to the degree of the GDPR, there is a likelihood of a possible "*Schrems III*" arising.

III. TAX AGREEMENTS AND EXCHANGE OF INFORMATION

International tax law seeks to create an efficient manner to ensure that taxpayers are not subject to double taxation in multiple jurisdictions by outlining which state will collect specific tax revenue and to ensure that taxpayers are not attempting to limit their tax burden by using different jurisdictions.[57] Though each state has different tax laws, the Organization for Economic Development ("OECD") helps to create a model that streamlines and strengthens the international tax law system.[58]

The OECD is a group of thirty-eight member countries, including the US and many EU member states, that work to develop economic and social policies which seek to shape the global economy by supporting free-market economic ideals.[59] For the issue of double taxation, the OECD created a Double Taxation Convention Model ("DTC") that is used as the basis for bilateral tax treaties for many countries.[60] The DTC outlines which taxpayers are covered and what taxes are addressed;[61] furthermore, in Article 26, it outlines the exchange of information in order to carry out the purpose of the DTC.[62] Specifically, Article 26 states that "competent authorities of the Contracting States shall exchange such information as is foreseeably relevant for carrying out the provisions of this convention," and that information must be treated as secret and in accordance with information obtained under domestic law.[63] The contracting

55. *Id.*

56. *Id.* at ¶ 156.

57. *International Tax Rule*, *supra* note 15.

58. *How we work*, OECD, https://www.oecd.org/about/how-we-work/ (last visited Feb. 1, 2023)

59. *Who we are*, OECD, https://www.oecd.org/about/.html (last visited Mar. 28, 2022).

60. *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD, https://www.oecd.org/tax/treaties/model-tax-convention-on-income-and-on-capital-condensed-version-20745419.html (last visited Mar. 28, 2022).

61. *Model Tax Convention on Income and on Capital Condensed Version*, OECD (Nov. 21, 2017), https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page3.html.

62. *Id.*

63. *Id.*

state gathers the requested information for the other party, even if the gathering state does not need the information for their own tax purposes, and therefore, the contracting state will not deny the request simply because the information is held by a bank or other financial institution.[64]

The US has more than fifty international bilateral tax treaties with different countries, of which twenty-six are with EU member states.[65] These tax treaties resemble the OECD DTC in coverage and enforcement and therefore, resemble one another; so I will only provide an in-depth analysis for one of the numerous agreements. The US and France entered the "Convention Between the Government of the United States of America and the Government of the French Republic for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital" ("Convention") on August 31, 1994, and the treaty went into effect on January 1, 1996.[66] Like the OECD's DTC, the Convention outlines the taxes covered, the taxpayers affected by the Convention, the income exempt from taxes, preventive clauses to stop tax treaties being used to avoid taxation, and the necessary sharing of information to maintain this Convention.[67] Article 27 of the 1996 Convention, titled "Exchange of Information," states that:

> The competent authorities of the Contracting States shall exchange such information as *is pertinent* for carrying out the provisions of this Convention and of the domestic laws of the Contracting States concerning taxes covered by this Convention insofar as the taxation thereunder is not contrary to this Convention . . . 3. The exchange of information shall be on request with reference to particular cases, or spontaneous, or on a routine basis . . . 4. (a) If information is requested by a Contracting State in accordance with this Article, the other Contracting State shall obtain the information to which the request relates in the same manner and to the same extent as if its own taxation

64. *Id.*

65. *See generally United States Income Treaties-A to Z*, IRS, https://www.irs.gov/businesses/international-businesses/united-states-income-tax-treaties-a-to-z.html (last visited Mar. 28, 2022).

66. *Convention Between the Government of the United States of America and the Government of the French*
Republic for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital, IRS (Jan. 1, 1996), https://www.irs.gov/pub/irs-trty/france.pdf [hereinafter *The Convention between the US and France*].

67. *Id.*

> were involved, notwithstanding the fact that the other State may not, at that time, need such information for purposes of its own tax.[68]

However, in 2009, the US and French governments issued a technical explanation that amended the Convention, which was the most recent amendment.[69] In this explanation, Article 27 is addressed and amended as such: the first paragraph uses the phrase "may be relevant" instead of "information as is pertinent," which allows for the Internal Revenue Service ("IRS") to examine "any books, papers, records, or other data which *may be relevant* or material";[70] the amended second paragraph explains that any information received by a Contracting State under the Convention is to be treated as secret and "disclosed only to persons or authorities, including courts and administrative bodies, involved in the assessment or collection of, the administration and enforcement in respect of, the determination of appeals in relation to the taxes."[71]

With this Convention and technical explanation, US and French tax authorities, and other competent authorities, are required to share information on taxpayers which the other state believes "may be relevant" to a tax investigation or any other provision outlined in their Convention.[72] "May be" is further defined by a US Supreme Court case to mean that the IRS is allowed "to obtain 'items of even *potential* relevance to an ongoing investigation."[73] Thus, the Convention has a broad definition and allowance for the exchange of information between the Contracting States with few limitations or directions on the protection of this information. Though there is a legal basis and genuine interest in the exchange of information to streamline the international tax law and to create an efficiency in preventing double taxation, this breadth and lack of protection could raise issues with the GDPR and EU resident's rights to a private life.

68. *Id.* (emphasis added).

69. *Department of the Treasury Technical Explanation of the Protocol Signed at Paris on January 13, 2009 Amending the Convention Between the Government of the United States of America and the Government of the French Republic for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital*, TREASURY (Jan. 13, 2009), https://www.treasury.gov/resource-center/tax-policy/treaties/Documents/tefranceprot09.pdf [hereinafter *Amending the Convention*].

70. *Id.*

71. *Id.*

72. *Id.*

73. United States v. Arthur Young & Co., 465 U.S. 805, 104 S. Ct. 1495, 79 L.Ed.2d 826, 834 (1984).

IV. POSSIBLE CONFLICT BETWEEN THE GDPR AND TAX CONVENTIONS

Following the issuance of the *Schrems II* decision and the growing uncertainty between the EU GDPR and the US privacy regulations, many relations could be questioned or cause concern. Despite the long history and stability of bilateral international tax agreements, the *Schrems II* decision could upheave the agreements, and governments, businesses, and individual actors should be prepared for changes. Under the *Schrems II* decision, the CJEU states that it is less important what the legal basis of transferring information is if there are no safeguards in place.[74] So, despite the legality of exchanging information for tax purposes under the bilateral international tax conventions, such as the one between the US and France, the US still needs to uphold the rights afforded by the GDPR to EU residents.[75] Namely, there are two concerns with Conventions and GDPR relations, which could bring claims and further issues to the strained relationship about data privacy.

First, though there is the language within the Convention that states that only authorized parties can see the information gathered, there is no guarantee that this is the case.[76] Looking at both *Schrems*' opinions, the CJEU had concerns that despite the Safe Harbor Framework and the Privacy-Shield Framework, there was no guaranteed protection for the data once it entered the US.[77] This is because the US did not create any legislation or policies to guarantee the EU residents rights or to provide any form of restitution if the rights had been violated.[78] US law allowed intelligence agencies to obtain and store information about EU residents.[79] The CJEU stated that there are not sufficient policies in place to protect against misuse of information once it enters the US, which applies to tax information obtained through Conventions as well.[80] Despite Article 27 of the Convention, which states that no other parties beyond those involved in the collecting and assessing of tax information are to see the confidential data, there are no preventive measures or legislation stopping NSA or other intelligence agencies from obtaining and storing the information obtained by tax authorities.[81]

74. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶ 199 (Dec. 19, 2019).

75. *Id.* at ¶¶ 187-188.

76. *The Convention between the US and France*, *supra* note 66.

77. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶¶ 64-65 (Dec. 19, 2019).

78. *Id.*

79. *Id.*

80. *Id.*

81. *The Convention between the US and France*, *supra* note 66.

The second concern is the language of what information may be requested and transferred under the Convention.[82] The breadth of the phrase "may be relevant" that was specifically added so that the IRS could examine any data that *may be relevant*, despite it not being needed for the other parties' tax purposes, could lead to issues under the GDPR.[83] The GDPR grants EU residents the right to a private life; but the ability of the US to request and obtain any information about a taxpayer by routine checks, particular cases, or spontaneous requests that could be relevant for tax purposes, allows the US authorities large access to information that could impede on the right to a private life.[84] This right to a private life is especially hindered by the abovementioned point that EU residents would not have a way to object to intelligence agencies obtaining the possible vast amount of information or a way to obtain restitution if the right is violated.[85] By using this language, the US authorities have access to so much information, which directly contradicts the purpose of the GDPR in protecting the EU residents' right to privacy when it comes to the transfer and collecting of personal information.

The lack of safeguards in place when the tax information is received by the US, and the breadth of the type of information these competent authorities can obtain, under US/EU member state international tax treaties, brings into question their validity under the guidelines of the GDPR and the decisions of the CJEU.

V. POSSIBLE NEXT STEPS

There have been various methods and proposals to allow for the continued acquisition and transfer of the data of EU residents by the US. As seen by the issuance of *Schrems I*, which invalidated the Safe Harbor Framework, it did not take long for the US and EU to negotiate a new arrangement, the Privacy Shield, in order to continue the relationship.[86] However, *Schrems II* invalidated the agreement, showing yet again that the CJEU does not believe that the US has adequate protections in place to uphold the rights under the GDPR, and now a new solution is needed.[87] The possibility of international bilateral tax treaties' validity being questioned, in terms of information sharing under the GDPR, may be the final straw for the CJEU to allow for the transferring of data; the

82. *Amending the Convention*, *supra* note 69.

83. *Id.* (emphasis added).

84. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶ 170 (Dec. 19, 2019).

85. *Id.*

86. Weiss, *supra* note 24, at 9.

87. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶¶ 199-201 (Dec. 19, 2019).

US may have to make large changes in order to proceed. Two possible steps to consider are additional SCCs added to the tax agreements, or a change in US legislation that would prevent other agencies or actors from collecting the information in violation of GDPR standards.

The tax agreements between the US and EU member states currently contain contractual clauses, which state that the information obtained shall remain confidential and not be shared beyond the agencies and authorities that are involved in the assessment or collection of the information.[88] These tax agreements could be amended further to provide additional language that follows the CJEU directives, with language protecting information and rights to a similar degree of the GDPR. However, the use of SCCs is not favored by the CJEU, due to the continued lack of legislation which would prevent the US from obtaining and misusing the data.[89] So, despite the ability to use SCCs, I believe that it would just be a temporary fix, which would not allow for a long-term solution for the continued relationship and sharing of data in international tax agreements.

Rather, I think that the US will be required to make legislation and policy changes if they seek to continue the sharing of taxpayers' information and maintain a productive relationship with the EU and its member states. As seen in *Schrems I* and *II* decisions, the CJEU is holding, despite bilateral agreements, contractual clauses, and attempted regulation to show that organizations are in line with GDPR criteria, there is still doubt that the US has adequate protection for EU residents' rights to privacy and concerns of the lack of legal restrictions that prevent misuse of the information once it is obtained.[90] As the CJEU continues to tighten the reigns on what is allowed under the GDPR and what agreements will survive, the US needs to enact legislation if they wish to maintain the relationship and the ability to collect and transfer data about EU residents. Enacting legislation which prevents the misuse of EU residents' information once it is in the US and allows for restitution to residents if there is misuse, or rights provided by the GDPR are violated, will appease the CJEU and show that the US does, in fact, have adequate protection in place.

The US needs to enact or amend legislation that has enforcement mechanisms rather than just promises to protect the data with no backing. Since the CJEU has yet to define what "adequate protection" is, there may be a variety of approaches to reach this level. However, a feasible option of legislation, which would abide by the GDPR and allow for the continued sharing of tax

88. *The Convention between the US and France*, *supra* note 66.

89. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145, ¶ 72 (Dec. 19, 2019).

90. *Id.* at ¶¶ 199-201.

information under the Convention, is an amendment to the Judicial Redress Act.

The Judicial Redress Act of 2015 was a piece of US legislation ratified by both the House and the Senate and signed into law by President Obama.[91] The Judicial Redress Act ("Act"):

> extends certain rights . . . under the Privacy Act of 1974, 5 U.S.C. § 552a, to citizens of certain foreign countries or regional economic organizations. Specifically, the Judicial Redress Act enables a "covered person" to bring suit in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an "individual" (*i.e.*, a U.S. citizen or permanent resident alien) may bring and obtain with respect to the: 1) intentional or willful unlawful disclosure of a covered record under 5 U.S.C. § 552a(g)(1)(D); and 2) improper refusal to grant access to or amendment of a covered record under 5 U.S.C. § 552a(g)(1)(A) & (B). Under the Judicial Redress Act, the access/amendment action may only be brought against a "designated Federal agency or component."[92]

In other words, the Act would extend privacy protection to foreign citizens, including EU residents, that US citizens currently enjoy.[93] However, an amendment stated that this Act would only be effective as to "not materially impede the national security interests of the United States" and, thus, intelligence agencies are still capable of obtaining and transferring the information.[94] Furthermore, the Act "relates specifically to information transferred in a law enforcement context."[95] The Act was originally praised by the EU and US as a step forward in providing adequate protection as needed by the GDPR; however, it was not enough, which can be seen as it was in place when *Schrems II* was decided.[96] A possible next step would be to amend the Act to extend the protections for foreign citizens, especially those that are residents of the EU, so that the Act plays a role in non-law enforcement contexts of collecting data and ensuring that intelligence agencies do not have free reign over the collection of anyone's data. By amending the Act to provide further protection and grant a wider ability for EU residents to bring suit when their

91. *Judicial Redress Act of 2015 & U.S.-EU Data Protection and Privacy Agreement*, OFFICE OF PRIVACY AND CIVIL LIBERTIES: U.S. DEPARTMENT OF JUSTICE (Dec. 28, 2022), https://www.justice.gov/opcl/judicial-redress-act-2015.html.

92. *Id.*

93. *Id.*

94. Weiss, *supra* note 24, at 13.

95. *Id.*

96. *Id.*

privacy rights have been violated, the CJEU may deem that the US does in fact have adequate protection, because the actors will be bound and thus the transfer of information in international tax treaties will be allowed to proceed. Furthermore, the amendment will have to stretch in order to apply to agencies, such as the IRS collection process which reviews and requests the information of EU citizens, and apply to EU government agencies collecting the information in connection to the bilateral tax agreements that are currently active.

Beyond extending the Act to foreign citizens, specifically EU citizens, and binding active government agencies, there are concerns within *Schrems II* stating that there are not enough restrictions on the US government, arguing "national security" reasons for going against the GDPR and continuing to share information of EU citizens. In order to appease the CJEU on this ground, it is likely that the US would have to amend the Foreign Intelligence Surveillance Act. The lack of limits placed upon intelligence agencies in the US is a concern noted by the CJEU in the *Schrems*' decisions. Until the USt is willing to compromise, there is little work to be done with the CJEU and their stand point.

VI. CONCLUSION

As the world becomes more digital and interconnected, the strained relationship between the US's privacy regulations and the EU's GDPR is at the forefront. Following the CJEU's decisions in the *Schrems*' cases, which invalidated both the Safe Harbor Framework and the Privacy Shield, the question of the US's ability to provide adequate protections for EU residents while maintaining efforts of collecting and transferring personal information is again unclear and draws attention to other agreements allowing for the sharing and transferring of data.

The proposed possible next step is likely not the only step that could be taken, but it highlights the changes that need to occur. In other words, legislation needs to bind the US government protecting the rights of the EU residents, as set forth in the GDPR. The proposed step, however, will require bipartisan support, which may be difficult to achieve to the level required by the CJEU and the GDPR. But, I believe that the fear of invalidating the long-standing international bilateral tax agreements, and the need for international tax cooperation, may be just enough to push the US to finally adopt legislative changes and provide adequate protections for the GDPR in the transfer of personal data.