HOW SCHREMS II JUDGMENT AFFECTED THE PERSONAL DATA FLOW BETWEEN THE EUROPEAN UNION AND THIRD COUNTRIES?*

Mariam Pilishvili[1]

The environment of the 21st century is more than friendly for innovation. The speed of technological growth is reaching the highest level. Recent advancement has facilitated the easy sharing of personal information. Personal data is fundamental to both our businesses and daily lives, and the utilization of such information for various purposes is now possible on a never-before-seen scale due to technology. When it comes to volume, an astounding variety of devices are currently used to generate and share data on a global scale. Throughout the digital progress, it has become necessary to update personal data protection legislation and adapt it to new challenges. As is the case, the General Data Protection Regulation went into effect on May 25, 2018. In order to consolidate data protection law and increase data subjects' rights with regard to the processing of their personal data, the GDPR replaced the previous data protection directive and became operative in all member states. The speed at which personal information is being retained and made more broadly available by individuals themselves has increased along with the strengthening of data privacy laws. Hence, technology has revolutionized both business and social life and become easier for personal data to be transferred freely inside the European Union as well as to other nations and international organizations. However, whether global data transition maintains a high level of privacy protection is still in question. In this regard, we will analyze the landmark decision of the Court of Justice of the European Union "Schrems II" and outline why the Court invalidated the EU-U.S. Privacy Shield.

Keywords: Personal Data Protection, Privacy, Data Flow, EU-US Privacy Shield, GDPR, Mass Surveillance.

1. Introduction

The global debate on privacy rights and data protection has gained momentum in the aftermath of the Snowden revelations in 2013. Specifically, on May 20, 2012, after Edward Snowden quit his work at a National Security Agency (NSA) site in Hawaii and traveled to Hong Kong, he disclosed thousands of top-secret NSA papers to the journalists. Everything changed drastically, and from the United States of America (U.S.) and Central America to Europe and Asia, the discussion has raged across time zones. Vladimir Putin's protection of Snowden prompted Barack Obama to postpone a trip to Moscow. In response to the US snooping on her, Brazilian President Dilma Rousseff canceled an official visit to Washington. Angela Merkel accused the U.S. of spying on her in Germany, sparking a controversy that led to the White House acknowledging that additional restrictions on the NSA's operations may be required.

* DOI 10.21868/PGnG.2025.1.2.

[1]*Mariam Pilishvili*, PhD student, Marton Géza Doctoral School of Legal Studies, University of Debrecen

The position of the American Internet corporations was quite beyond belief, as they stated that the law required and forced them to cooperate (Macaskill and Dance, 2013). Aside from this, Joe Sullivan, Facebook's chief security officer, stated that they do not grant any government body direct access to Facebook systems. And when Facebook is asked for data or information about particular persons, they carefully review each request to ensure compliance with all applicable regulations and release data only to the extent needed by law. According to Apple spokesman Steve Dowling, they have never heard of the FBI's and NSA's now-public alleged homeland surveillance project (PRISM). Furthermore, every government entity requiring information about Apple customers must obtain a court order since any government agency is restricted from having direct access to Apple Servers (Macaskill and Dance 2013).

To highlight from top to bottom, the first disclosed surveillance program, PRISM, which was led by the U.S. NSA, allowed access to global internet traffic and communications from major U.S. companies operating in Europe, and thus access to the personal data of millions of Europeans (Gellman and Poitras 2013). The Snowden disclosures further demonstrated that the fiber-optic cables between the United States and Europe had their communication data inadvertently intercepted in large quantities. In other words, as transatlantic fiber optic cables also transport internet traffic between the U.S. and Europe, Government Communications Headquarters (GCHQ) has direct access to a significant amount of the world's internet data. The program was called TEMPORA (Shubber 2013).

In terms of the justification and legal grounds, it has to be noted that the Human Rights Act, which states that searches must be necessary and proportional, meaning that there must be a reason for looking at the material, is one law that GCHQ asserted its agents follow. GCHQ claimed that the program has stopped terrorist strikes on British territory and that it doesn't eavesdrop on the data of ordinary citizens instead focusing on "bad guys" like terrorists and criminals (Shubber 2013).

The Civil Liberties, Justice, and Home Affairs Committee was given permission by the European Parliament to launch an investigation into the alleged widespread surveillance of people by the U.S. NSA and many EU nations, as well as the implications for people's fundamental rights, on July 4, 2013. The comprehensive research compiles all the data and offers a number of recommendations, including outlining specific online privacy safeguards, seven steps to secure personal information, and a roadmap for the future. Emphasis was placed on issues such as transfers to third countries with an adequacy decision, transfers based on contractual clauses and other instruments, transfers based on the Mutual Legal Assistance Agreement, transfers based on the Terrorist Finance Tracking Program and Passenger Name Record agreements, and the Framework agreement on data protection in the field of police and judicial cooperation (Umbrella Agreement) (European Parliament 2014).

This was an essential reminder to lawmakers that the amount of pervasiveness of information technology must be matched by appropriate legislative protection. A new regulatory framework for cross-border data transmission between the European Union (EU) and the U.S. was created as a result of the reformative process. It has to be mentioned that there is no worldwide data flow regulation that might be related to the global protection of personal data, and only bilateral agreements are an essential tool for data transit and storage. In this regard, we will analyze one of the known and

controversial frameworks between the EU and the U.S., namely the EU-U.S. Privacy Shield agreement in accordance with the case Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II) (Court of Justice of the European Union 2020).

2. The legal framework of the study

In the case C-311/18 Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, the Court of Justice of the EU (CJEU) issued a preliminary ruling on July 16, 2020, thoroughly invalidating the European Commission's Decision (EU) 2016/1250 relating to the EU-US Privacy Shield. Specifically, the EU data protection authorities were issued a draft ruling by Ireland's Data Protection Commission proposing to prohibit Facebook parent company Meta from sending personal data from the EU to the US In what is referred to as the "Schrems II" judgment, the Court raised questions about the use of Standard Contractual Clauses (SCCs).

Contractual provisions guaranteeing adequate data protection measures may be used as justification for data transfers from the EU to third countries, in accordance with the General Data Protection Regulation (GDPR). This comprises sample contract language or "pre-approved" standard contractual clauses (SCCs) from the European Commission. For data transfers between controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA, the Commission announced modernized standard contractual terms on June 4, 2021 (European Commission 2021).

After that, the CJEU upheld the legality of Standard Contractual Clauses as a way to ensure an adequate level of protection for personal information being transmitted to foreign nations, constantly requiring full and strict compliance to the criteria set forth under the Charter of the Fundamental Rights of the European Union and European data protection legislation. Following the CJEU ruling, the Data Protection Commission opened an "own volition" research under the Data Protection Act of Ireland to determine if Facebook's data transfers to the U.S. were appropriate and lawful.

3. Methodology

In order to gather as much information as feasible, we will use historical, document analysis, and case study approaches during our research. By using historical methodologies, we will emphasize a historical overview of the EU-U.S. Privacy Shield agreement, while the document analysis approach will give us the possibility to carefully look over the texts of the law and articles in order to fully analyze fundamental requirements for invalidating the abovementioned agreement. By employing case study methodologies, we will discuss the main points of the CJEU's ruling in case C-311/18 and outline the influence of Schrems II over privacy protection.

The social backdrop that can be connected to our paper is the need to preserve each person's privacy and personal information to the greatest extent possible. Personal data should be gathered, kept, and processed with growing precision and accuracy, especially by government agencies. It is widely known that globalization and rapidly advancing

technology have created new difficulties for the protection of personal data. Due to this issue, personal data is now being collected and shared on a far larger basis. Hence, the regulations for the protection of the basic freedoms and rights of individuals across the world with regard to the processing of personal data shall be applied uniformly and consistently. The growth of international trade and international collaboration depends on the flow of personal data to and from nations outside the EU and international organizations. However, the degree of protection of personal data should not be compromised when personal data is transferred from the EU to controllers, processors, or other recipients in third countries or to international organizations.

4. Overview of the EU-US Privacy Shield Agreement

On July 12, 2016, the EU-U.S. Privacy Shield adequacy judgment was adopted, allowing the free flow of data to organizations recognized in the U.S. under the Privacy Shield. The EU-US Privacy Shield is a self-certification method developed by the U.S. Department of Commerce and the European Commission to assure that data protection laws are followed while transmitting personal data from the EU to the US in order to improve transatlantic trade. The decision outlines personal data protection to any EU data subject whose personal data has been flown from the region to organizations in the U.S. (Commission Implementing Decision (EU) 2016/1250)). Back in time, the EU-U.S. Privacy Shield had been recognized as providing an appropriate degree of protection in light of the legal framework for personal data protection in the EU. In addition to this, By Decision No. 144/2017 of the European Economic Area (EEA) Joint Committee on July 7, 2017, the Privacy Shield Decision was officially entailed into the EEA Agreement (EEA Joint Committee 2017).

It is very important to take note of the principles outlined in the aforementioned decision, which at first glance seem to imply high-level security in terms of data flows. The EU-US. Privacy Shield identifies seven principles that have to be fulfilled and protected by the organizations while transmitting the data: the notice principle, the data integrity and purpose limitation principle, the choice principle, the security principle, the access principle, the recourse, enforcement and liability principle and the principle of accountability for onward transfer.

The notice principle is a simple requirement, under which organizations are required to notify data subjects of a number of important details pertaining to the processing of their personal data: these include, among others, the purpose of the processing and which types of data have been collected (Commission Implementing Decision (EU) 2016/1250, para 20). Under the principle of data integrity and purpose limitation, personal information shall only be processed if it is necessary, precise, ongoing, and trustworthy for the purpose intended (para 21). One of the essential principles written down in the decision is the choice principle, which grants data subjects the right to object to collection of their data (opt-out). Additionally, organizations must often get the data subject's express, affirmative agreement before handling sensitive data (opt-in) (para 22). The security principle includes the requirement for organizations handling data to take “reasonable and appropriate security measures” while taking into consideration the risks that may stem from the nature of the processing of personal data (para 24). According to the principle of access, the data subjects are given the right –

without the need for justification – to request verification from a company that they are processing their personal data and to have that information communicated to them within a reasonable amount of time (para 25). Under the enforcement and liability principle, organizations are required to provide effective systems for ensuring compliance with other principles (para 26). And finally, based on the principle of accountability for onward transfer, any onward transfer is only permitted if it stipulates specific and limited objectives, is based on a contract, and offers the exact level of security as the principles (para 28).

Consequently, the EU-U.S. Privacy Shield essentially permits the transfer of personal data from entities based in the EEA that have self-certified as providing adequate legal guarantees in respect of such transfers of data and commit to upholding and observing a number of data protection principles enshrined in the EU-U.S. Privacy Shield to entities based in the United States. Alternatively, in light of the aforementioned strong principles, it is initially curious as to why the directive's validity was questioned and what caused the repeal.

5. Findings of the CJEU's decision

The case began with Austrian activist and lawyer Maximilian Schrems' request that the Irish Data Protection Commissioner invalidate the SCC since personal data was used by Facebook to transmit it to American headquarters. It was asserted that American intelligence agencies might access personal data while it was in transit to and while it was being stored in the US. Hence, Schrems believed that his and other people's personal information gathered by Facebook Ireland was through servers in California for additional processing, which strictly violated the General Data Protection Regulation, and more broadly, the law of the European Union. Specifically, due to the fact that the law and the practice of the US did not provide adequate protection of data in its territory and that his and other Europeans' information was available to the NSA. This case was dismissed, among other reasons, due to the determination of the Commission that the United States provided an acceptable level of protection in Decision 2000/520 (para 52). The Irish High Court, where Mr. Schrems had filed an application for judicial review of the dismissed complaint, urged the Court for a preliminary ruling on the scope and legality of Decision 2000/520. The Court invalidated that decision in Schrems in 2015 (para 53). After that, the decision about the annulment of the complaint was rejected and given back to the Commission on the grounds that, through the investigations of the Commissioners, Facebook Ireland confirmed that a significant amount of personal data was transmitted to Facebook Inc. in accordance with the standard data protection clauses listed in the annex to the SCC Decision and asked Mr. Schrems to reformulate his complaint (para 54).

The reformulated complaint stated that Facebook Inc. is required by US law to provide the National Security Agency and the Federal Bureau of Investigation with access to the personal data that has been transmitted to it. He argued that the SCC Decision cannot support the transfer of that data to the United States because the data was utilized in the context of several monitoring programs in a way that violated Articles 7, 8, and 47 of the Charter (para 55). Hence, the reformulated complaint raised questions regarding the validity of the SCC Decision.

The Schrems II case was brought by the Data Protection Commissioner before the High Court of Ireland, (para 57). which then forwarded questions to the CJEU for a preliminary ruling. The European Court of Justice had been assigned, among other things, to determine, whether the Privacy Shield Decision met the requirements of Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, as interpreted in light of the EU Charter. In addition to this, the High Court requested that the CJEU decide whether data transfers made possible by SCCs infringed the rights to privacy and data protection enshrined in the Charter (para 68).

In terms of the standard contractual clauses for the transfer of personal data, the CJEU acknowledged SCCs as legitimate data transfers but gave supervisory authorities oversight duties to make sure the GDPR is carried out in the context of SCCs (para 108). Articles 46(1) and 46(2)(c) of the GDPR, according to the court, necessitate that EU citizens whose data is transferred to a third country receive "*a level of protection essentially equivalent to that guaranteed within the European Union,*" including "*appropriate safeguards, enforceable rights, and effective legal remedies*" (para 105). The court ruled that such protection might be provided by a legitimate European Commission adequacy judgment or by SCCs. The competent supervisory authority, however, must make sure that the SCCs can be followed in the third country or that EU standards for data protection can otherwise be upheld if data is transmitted through SCCs (paras, 94-96).

The Privacy Shield Decision was declared unlawful by the Court on the grounds that the GDPR's necessity and proportionality requirements are inconsistent with the application of US legislation. The CJEU determined that there is no adequate administrative or judicial remedy mechanism available to EU individuals who are data subjects and whose personal data is being processed unlawfully in the US The court explicitly determined that section 702 of the FISA and Executive Order 12,333 do not impose "minimum safeguards" and are not "limited to what is strictly necessary," which led it to the conclusion that US restrictions on data protection violate the principle of proportionality (para 184). Consequently, the Court concluded that the U.S. law violates the basic right to adequate judicial protection as codified in Article 47 of the Charter of the Fundamental Rights of the European Union and is inconsistent with Article 45 of the GDPR as it does not provide individuals the possibility to utilize legal remedies for accessing personal data related to them (paras 199-201).

6. Discussion

In the journal Harvard Law Review, in relation to the Schrems II decision, Michael Aktipis and Ron Katwan outlined the Court’s failure to create a legal framework according to which the European Commission could make and evaluate adequacy decisions. The court's decision that the U.S. does not offer *"adequate level of protection"* for personal information transmitted from the European Union was a major factor in the Privacy Shield's invalidation. Specifically, Section 702 was occasionally ambiguous and frequently inconclusive. In the review, we read that the court's evaluation of the proportionality of U.S. tracking regulations, particularly section 702,

was occasionally superficial and usually ambiguous. Because of this, it is unclear which parts of section 702 go beyond what is essential or don't have the necessary protections. Therefore, the court's incomplete approach offers little direction as to the legitimacy of recent and upcoming sufficiency rulings (Aktipis and Katwan 2021).

From the viewpoint of European lawyers, the Court's ruling was distinguished with astonishing clarity. Ironically, despite the fact that the issue concerns Facebook Ireland's transfer of data to Facebook, Inc. servers in the U.S., it will be businesses in the European "old economy" who will have to deal with serious repercussions in the wake of this landmark decision rather than Facebook. They have also stated that the consent of the data subjects will frequently be hard to gain in the course of routine data processing in the business environment. It is at the same time practically hard to prohibit data to be moved outside the EU. As a result, many data processing activities that were permitted before Schrems II are now prohibited (Ziegenhorn and von Heckel 2015).

From my viewpoint, the CJEU, according to the ruling, definitely increased the fundamental rights' substantive content. The decision also implicitly supported the need for comparable data protection rules in the United States, and as such, it could be read as a plea for a legislative framework, perhaps on a global scale.

7. Conclusion

We can draw the conclusion that the Schrems decision accepted the legitimacy of the concerns that have long been expressed at the EU level. Specifically, concerns about the Privacy Shield's ability to adequately protect personal data when it is transferred to processing facilities outside of the EEA.

Given the Schrems ruling, it is possible that this Commission decision could be overturned soon using a very similar line of reasoning to that used by the CJEU in Schrems: the level of data protection may be in jeopardy not only in cases of transfers to the US. but also, in circumstances when the data is moved to third countries under the EU standard contractual terms due to the individual national laws and their implementation in those countries. To this purpose, it is evident that the EU's regulatory framework for data processing is moving in the direction of re-territorialization.

References

Aktipis, M.S. & Katwan, R.B. (2021). Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU). *International Legal Materials* 60(1): 1571.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176). *Official Journal of the European Union*, L 207/1. https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj/eng [accessed April 9, 2023].

Court of Justice of the European Union (2020). Judgment in the case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case Schrems II) https://curia.europa.eu/juris/liste.jsf?num=C-311/18 [accessed April 9, 2023].

EEA Joint Committee (2017). Decision of the EEA Joint Committee amending Annex XI (Electronic communication, audiovisual services, and information society) to the EEA Agreement [2019/751], No 144/2017. Official Journal of the European Union, L 128/44. https://eur-lex.europa.eu/eli/dec/2019/751/oj/eng [accessed April 9, 2023].

European Commission (2021). *Standard Contractual Clauses (SCC)*. https://commission.europa.eu [accessed April 9, 2023].

European Parliament (2014). *REPORT on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, Report 2013/2188(INI). https://www.europarl.eu [accessed April 9, 2023].

Gellman, B. & Poitras, L. (2013). U.S., British Intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*, June 6, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [accessed April 9, 2023].

MacAskill, E. & Dance, G. (2013). NSA Files: Decoded – What the revelations mean for you. Produced by F. Cage and G. Chen. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [accessed April 9, 2023].

Shubber, K. (2013). A simple guide to GCHQ's internet surveillance programme Tempora. *WIRED*, July 4, 2013. https://www.wired.com/story/gchq-tempora-101/ [accessed April 9, 2023].

Ziegenhorn, G. & von Heckel, K. (2015). The Schrems Judgement: New Challenges for European and international companies. *VerfBlog*, 12 October 2015. https://verfassungsblog.de/the-schrems-judgement-new-challenges-for-european-and-international-companies-2/ [accessed April 9, 2023].