Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case 311/18) - how did we get there and what the future holds?

Hmelina, Ivan

University of Zagreb

Faculty of Law

Jean Monnet Chair of European Public Law

Ivan Hmelina

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case C-311/18) – how did we get there and what the future holds?

Master Thesis

Mentor: doc. dr. sc. Melita Carević

Zagreb, September 2022

Izjava o izvornosti

Ja, Ivan Hmelina, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima do onih navedenih u radu.

Ivan Hmelina, v.r.

_____

Ivan Hmelina

Abstract

This master thesis analyzes what preceded the long-awaited judgment of the Court of Justice of the European Union (CJEU) in case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (more commonly known as the Schrems II), and what can be expected after such a decision. Specifically, the entire history of how the abovementioned judgment was reached is thoroughly described, beginning with the differences between the data protection legislation of the European Union and the United States. The creation of the Safe Harbour, the first agreement governing transatlantic data transfers, and the CJEU's Schrems I ruling, which invalidated the aforementioned framework, are then detailed. This master thesis also tackles the creation of the Privacy Shield, which was the Safe Harbour's successor, and an analysis of the Schrems II judgment. Additionally, it demonstrates what might be expected in the post-Schrems II era, particularly with regard to the new framework for data transfer between the European Union and the United States that shall come into effect in 2023.

Keywords: data protection, transfer of personal data, GDPR, Safe Harbour, Privacy Shield, Schrems I, Schrems II, Trans-Atlantic Data Privacy Framework.

Sažetak

Ovaj diplomski rad analizira pravni okvir koji je prethodio dugo očekivanoj presudi Suda Europske unije u predmetu C-311/18 *Data Protection Commissioner protiv Facebook Ireland Limited i Maximillian Schrems* (koji je poznatiji pod nazivom Schrems II) te što možemo očekivati nakon takve odluke. Konkretno, iscrpno su analizirani svi događaji koji su doveli do spomenute presude – počevši od razlika u zakonodavstvu o zaštiti podataka između Europske unije i Sjedinjenih Američkih Država; stvaranje Sigurne luke, prvog sporazuma koji uređuje transatlantski prijenos osobnih podataka, i s tim u vezi, obrada presude Suda Europske unije Schrems I koja je poništila navedeni sporazum; stvaranje Štita privatnosti koji je bio nasljednik Sigurne luke, te na kraju dubinska analiza presude Schrems II. Uz to, ovaj diplomski rad pružio je uvid u ono što se može očekivati u eri nakon presude Schrems II, posebice u vezi s novim sporazumom o prijenosu osobnih podataka između Europske unije i Sjedinjenih Američkih Država koji će stupiti na snagu 2023. godine.

Ključne riječi: zaštita podataka, prijenos osobnih podataka, GDPR, Sigurna luka, Štit privatnosti, Schrems I, Schrems II, Trans-Atlantic Data Privacy Framework.

Table of Contents

1. Introduction 1

2. The legal framework between the European Union and the United States prior to *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18) 2

2.1. Brief history of modern data protection legislation in the European Union and the United States 2

2.1.1. The European Union's path 2

2.1.2. The United States' path 6

2.2. The Safe Harbour 9

2.2.1. Critiques of the Safe Harbour 11

2.3. *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14) 13

2.3.1. Context of the case 13

2.3.2. Judgement 14

2.3.3. Implications of the judgment 16

2.4. The Privacy Shield 18

2.4.1. Critiques of the Privacy Shield 20

3. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18) 21

3.1. Context of the case 21

3.2. The opinion of the Advocate General 23

3.3. Judgement 24

4. What next? The aftermath of *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18) 27

4.1. The European Data Protection Board's recommendations 28

4.2. The New Standard Contractual Clauses 29

4.3. The new Trans-Atlantic Data Privacy Framework 31

5. Conclusion 32
6. Bibliography 34

1. Introduction

I would like to start this master thesis by posing a question to everyone who will read it – what is privacy? Most people are likely to give a similar, yet different answer. In general, the right to privacy refers to "*the freedom from interference or intrusion and the right to be left alone*".[1] In addition, information privacy is "*the right to some degree of control over the gathering and use of your personal data*".[2]

In 2017, the Economist published a widely referenced article titled "*The world's most valuable resource is no longer oil, but data*".[3] They were not wrong. According to one survey, by 2025, the data universe will consist of 175 zettabytes.[4] In case, like most people, including myself, you do not know how much that is – one zettabyte is 1 trillion gigabytes.[5] If you were to download 175 zettabytes of data on your computer, it would take you 1.8 billion years.[6]

Despite the aforementioned, numbers being numbers, they do not provide much without context. If we look at those figures from a different perspective and take into account that such an enormous pile of data includes not only our own personal information but also that of our family, friends, and colleagues, things become slightly different. In light of this, in this master thesis I will provide an overview of how such data is being protected in cases of an international transfer, namely between the European Union and the United States. In particular, the first part of this master thesis describes the differences of the data protection legislation in the European Union and the United Stated and what preceded the highly anticipated judgment in *Schrems II*. The second part of the thesis analyses the *Schrems II* judgment and its consequences.

---

[1] International Association of Privacy Professionals, 'What does privacy mean?' <https://iapp.org/about/what-is-privacy/> accessed 1 September 2022.
[2] Ibid.
[3] The Economist, 'The world's most valuable resource is no longer oil, but data' [2017] <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 1 September 2022.
[4] Kara Nortman, 'Data is the world's most valuable (and vulnerable) resource' [2021] <https://techcrunch.com/2021/03/04/data-is-the-worlds-most-valuable-and-vulnerable-resource/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACQWNuoOTAw0ffXbog0DNsjo5hYR_WInzdC2S4Ld27pcVybLIBzK7vXKGD5mbE8Zty6c-vdpLbILT82HVp05lPgWCcCu_8D-fILBAigjkJxNSRHWswPdto6Ln99s7jRf9-webjD05KrwvQ6kpDzsKtuxncf144z9FSkz6Mc5CPwi> accessed 1 September 2022.
[5] Ibid.
[6] Ibid.

The last part focuses on the new agreement for transatlantic data transfer which shall come into effect in 2023 and future developments.

2. The legal framework between the European Union and the United States prior to *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18)

2.1. Brief history of modern data protection legislation in the European Union and the United States

2.1.1. The European Union's path

Data protection is highly enrooted in the European Union's (hereinafter referred to as: the "**EU**") legal legacy. It all started with Article 8 of the European Convention on Human Rights[7] (hereinafter referred to as: "**ECHR**"), which states:

"*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Even though ECHR was not adopted by the European Commission, based on this article, the EU has endeavored to protect such right through various legislation.[8] The next significant breakthrough was in the 1970s when the Council of Europe[9] concluded that the aforementioned Article 8 of ECHR had several shortcomings (most notably the ambiguity surrounding what was covered by "private life") due to technological advancement.[10] The end result was the adoption of the Convention for the Protection

[7] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended [1950].
[8] Ben Wolford, 'What is GDPR, the EU's new data protection law?' <https://gdpr.eu/what-is-gdpr/> accessed 21 June 2022.
[9] The Council of Europe is an international organization that promotes human rights, democracy, and the rule of law in Europe. It was founded in 1949 and it consists of 46 members (27 of which are members of the EU).
[10] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' [2014] Collected Courses of the European University Institute's Academy of European Law, 4.

of Individuals with Regard to Automatic Processing of Personal Data[11] (hereinafter referred to as: the "**Convention 108**") which was the first legally binding international instrument in the data protection field. It is important to note that all 27 EU Member States are the signatories of the mentioned convention. The idea of privacy as a "take-back control" by individuals over the processing of their personal data was established by the Convention 108, as were some key concepts and definitions of data protection such as personal data, automatic processing, data controller, and data subject rights.[12]

The adoption of the Convention 108 coincided with the first initiatives at the national or state level, starting with the German state of Hesse. In 1970 it enacted the Data Protection Act, which many consider to be the world's first data protection act.[13] Sweden followed in 1973 by passing its *Datalagen* (in English: the Data Act), the first national data protection law which criminalized data theft and gave data subjects freedom to access their records.[14] By the end of the 1970s, many EU Member States (e.g. both France[15] and Germany[16] in 1978) had incorporated data protection laws as fundamental rights into their legislation. In the beginning, the reasoning behind such laws was to safeguard the citizens' privacy *vis-à-vis* public administration.[17] However, that role changed in the 1990s, when the use of internet and information processing technologies grew widespread among both businesses and individuals and so did the threat to data privacy.[18] The EU was fully aware of such ongoing technology

[11] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981].
[12] Stephen Ragan, Petruta Pirvan, 'What is Convention 108?' <https://www.wrangu.com/what-is-convention-108/> accessed 22 June 2022.
[13] Olga Stepanova, Patricia Jechel, 'The Privacy, Data Protection and Cybersecurity Law Review: Germany' [2021] <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,(BDSG)%20entered%20into%20force> accessed 22 June 2022.
[14] 'DATA PRIVACY ACT: A BRIEF HISTORY OF MODERN DATA PRIVACY LAWS' [2018] <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy laws#:~:text=The%201970s%20%E2%80%93%20The%20First%20Modern%20Data%20Privacy%20Laws&text=In%201973%2C%20Sweden%20created%20the,freedom%20to%20access%20their%20records> accessed 22 June 2022.
[15] 'Data Protection in France' <https://gdprhub.eu/Data_Protection_in_France> accessed 22 June 2022.
[16] 'Data Protection in Germany' <https://gdprhub.eu/index.php?title=Data_Protection_in_Germany> accessed 22 June 2022.
[17] 'Sources of Data Protection Law' <https://www.clarin.eu/content/sources-data-protection-law> accessed 22 June 2022.
[18] Ibid.

progression and its answer was the adoption of the Directive 95/46/EC[19] (hereinafter referred to as: the "**Data Protection Directive**").

With the Data Protection Directive, the EU institutions addressed the problem of mosaic data protection laws widespread throughout the whole EU because, even though the Convention 108 was effective in placing data protection on the agenda and laid out some of its key concepts, it fell short of establishing sufficient consistency among its members.[20] In any case, the Data Protection Directive broadened the rights protected by the Convention 108, and even added new ones like e.g. establishment of national supervisory authorities,[21] which has certainly been a significant step toward harmonization.

In addition to the Data Protection Directive, another important act that regulates data protection is Directive 2002/58/EC,[22] which relates to publicly available electronic communications services and public communications networks and deals with a wide array of issues including security and confidentiality of communications, treatment of traffic data, usage of cookies, etc.[23]

In the EU, data protection is not only protected by the abovementioned secondary legislation, but is also contained in primary law. As a source of primary law, fundamental rights stemming from the ECHR have long been recognized and applied by the European Court of Justice (hereinafter also referred to as: the "**CJEU**") as general principles of the EU law.[24] Nonetheless, the European Council concluded in 1999 that it was time to draft an EU equivalent charter and in 2000 the Charter of Fundamental Rights of the European Union[25] (hereinafter also referred to as: the "**EU Charter**") was proclaimed, initially as a non-binding legal source.[26] Only when the Lisbon Treaty[27] entered into force in 2009 did the EU Charter become a legally binding

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
[20] n 10, p 9.
[21] n 19, art 28.
[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.
[23] n 10, p 14.
[24] Ibid., p 16.
[25] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
[26] n 10, p 16.
[27] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/1.

instrument.[28] One of the EU Charter's novel features was an explicit recognition of the right to the protection of personal data in Article 8(1) which reads "*Everyone has the right to the protection of personal data concerning him or her*". By all means, the EU Charter along with the Lisbon Treaty had a tremendous impact on the EU data protection law.

A few years passed by and in 2012 the European Commission proposed[29] a thorough overhaul and attempt to modernize the existing EU legal framework regarding data protection. Three factors influenced the reasoning behind such a proposal.[30] Firstly, rapid technological advancements have created new challenges for data protection and the scale of data sharing and collection has increased more than ever.[31] Thus, the Data Protection Directive was becoming increasingly outdated and since it was adopted when the internet was in its infancy, it could not cope with the challenges posed by the modern world. Another reason is that the Data Protection Directive is exactly that – a directive, and while it is legally binding, it left to the national authorities the choice of form and methods on how it shall be implemented.[32] As a result, 28 different versions of the basically same principles were created.[33] The third reason is related to the EU Charter and the Lisbon Treaty which, as we have seen, placed a high value on the protection of fundamental rights, particularly the right to data protection.[34] After four years of negotiation, on 27 April 2016, the final text of the General Data Protection Regulation[35] (hereinafter referred to as: the "**GDPR**") was adopted. After additional two years given for accommodation, GDPR become fully enforceable on 25 May 2018, and the Data Protection Directive was replaced.

The twofold aim of the GDPR is: (i) enhancing data protection rights of individuals, and (ii) improving business opportunities by enabling the free flow of

[28] Consolidated version of the Treaty on European Union [2007] OJ C 362/390, art 6(1).
[29] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012] COM/2012/011 final - 2012/0011 (COD).
[30] n 10, p 26.
[31] n 29, p 1.
[32] n 28, art 288 (3).
[33] n 10, p 26-27.
[34] Ibid.
[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

personal data in the digital single market.[36] Furthermore, since the GDPR is a regulation, it is binding in its entirety and directly applicable in all EU Member States and it is aimed at uniting the EU under a single set of rules.[37] There are many novelties in the GDPR, but some things should definitely be highlighted, such as the codification of the "right to be forgotten";[38] new legal basis for processing (legitimate interest);[39] data protection impact assessment;[40] and monstrous fines which, for especially severe violations, can be up to 20 million euros or in the case of an undertaking, up to 4% of the total global turnover of the preceding fiscal year, whichever is higher.[41] One thing is certain – the GDPR is by far the most robust set of legislation worldwide when it comes to data protection yet.

2.1.2. The United States' path

On the contrary, the legal approach in the United States (hereinafter referred to as: the "**U.S.**") was rather different. It all started in 1890 with the famous article "*The Right to Privacy*",[42] whom some consider to be "*the most influential law review article of all*",[43] in which authors gave a new right to the common law – the "right to be let alone".[44] In said article, authors Warren and Brandeis vented their displeasure with the nineteenth-century technological innovations, specifically the use of instant photography and audio recording.[45] These new threats required some kind of remedy, but the problem was that existing common law did not provide much legal protection for privacy.[46] Daniel J. Solove put it nicely: "*Defamation law - the torts of libel and slander - protected against false information, not true private information*".[47] In regards

[36] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 11 June 2015, 2012/0011 (COD) 1.
[37] n 28, art 288 (1).
[38] n 35, art 17.
[39] Ibid., art 6 (1(f)).
[40] Ibid., art 35-36.
[41] Ibid., art 83 (5).
[42] Samuel D. Warren, Louis D. Brandeis, 'The Right to Privacy' [1890] 4 Harvard Law Review 193.
[43] Harry Kalven Jr., 'Privacy in Tort Law—Were Warren and Brandeis Wrong?' [1966] 31 Law and Contemporary Problems 326, 327.
[44] n 42, p 194.
[45] Irwin R. Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' [1990] 39 Catholic University Law Review 703, 703.
[46] Daniel J. Solove, 'A Brief History of Information Privacy Law' [2006] PROSKAUER ON PRIVACY 1,12.
[47] Ibid.

to that, Warren and Brandeis discussed several remedies, the most important of which was "*an action of tort for damages in all cases*".[48]

One of the pivotal cases to address Warren and Brandeis's proposals from the aforementioned article was the 1902 case of *Roberson v. Rochester Folding Box Co*.[49] In the said case, the New York Court of Appeals heard the case of a woman (Roberson) whose privacy was allegedly violated when the defendants used her portrait to advertise flour without her consent.[50] The court rejected Roberson's claims because "*there is no precedent for such an action to be found in the decisions of this court*".[51] The *Roberson* decision sparked a significant debate and in response to the widespread public outrage over this decision, New York passed two statutes that are still in force today.[52] These statutes made it both a tort and a misdemeanor for any person, firm or corporation to use the name, portrait or picture of any living person for commercial purposes, without having first obtained the written consent of such person.[53]

In 1960, William Prosser, a well-known legal scholar at the time, examined roughly 300 privacy cases that were spawned by Warren and Brandeis's article in his life work "*Privacy*".[54, 55] In said article Prosser divided the invasion of a person's privacy into the following torts:

1. Intrusion upon seclusion or solitude, or into private affairs;
2. Public disclosure of embarrassing private facts;
3. Publicity which places a person in a false light in the public eye; and
4. Appropriation of one's name or likeness.[56]

These torts allowed someone, whose privacy was violated, four ways to sue the perpetrator for damages. In addition to that, most of them are recognized by the vast majority of the U.S. states and are still used today.[57]

---

[48] n 41, p 219.
[49] 171 NY 538, 64 NE 442 [1902].
[50] n 45, p 715.
[51] n 49, par 544.
[52] n 45, p 717.
[53] NY Civ Rights L § 50 [2014].
[54] William L. Prosser, 'Privacy' [1960] 48 California Law Review 383.
[55] n 46, p14.
[56] n 54, p 389.
[57] n 46, p 14.

One could not talk about data privacy in the U.S. without addressing the 1965 ruling of *Griswold v. Connecticut*,[58] in which the U.S. Supreme Court protected married couples' freedom to purchase and use contraception.[59] Even though the Constitution of the U.S. does not specifically guarantee or entrench a right to privacy, in the said case justice William O. Douglas reasoned that such a right is featured in the "*penumbras*" of the many of the ten amendments to the Bill of Rights.[60] Following *Griswold*, the U.S. Supreme Court decided a number of cases in the 1960s and 1970s, including *Katz v. United States*,[61] *Roe v. Wade*,[62] and *Eisenstadt v. Baird*,[63] which further set the groundwork for the recognition of a right to privacy as a constitutional right.

The privacy legislation changed dramatically in 1974. The first was the passage of the federal law called FERPA,[64] or Family Educational Rights and Privacy Act, which protected the accessibility of student records. With FERPA, no school, university, or other institution that receives funds from the U.S. Department of Education is permitted to release such information without the explicit consent of the student.[65] In the same year, the Privacy Act[66] was enacted which established a code of fair information practices that governed the collection, use, and dissemination of information about the U.S. citizens that is maintained in systems of records by federal agencies.[67] Despite making significant progress toward controlling government information systems on the federal level, the act itself has a number of shortcomings, the biggest of which is that the private sector, as well as state and local governments, are exempt from it.[68] Up until the year 2000, many laws were passed that had a significant impact on different

[58] 381 US 479 [1965].
[59] 'Overview of Privacy and Privacy Legislation' <https://projects.iq.harvard.edu/privacyproject/overview-privacy-legislation#:~:text=Warren%20and%20Brandeis%20defend%20privacy,be%20protected%20by%20contract%20law> accessed 25 June 2022.
[60] n 46, p 23.
[61] 389 US 347 [1967].
[62] 410 US 113 [1973].
[63] 405 US 438 [1972].
[64] 20 USC § 1232g 34 CFR Part 99 [1974].
[65] n 59.
[66] 5 USC § 552a [1974].
[67] 'PRIVACY ACT OF 1974' [2021] <https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies> accessed 26 June 2022.
[68] n 46, p 26.

areas of data privacy law, such as the Health Insurance Portability and Accountability Act,[69] Fair Credit Reporting Act,[70] Gramm-Leach-Bliley Act,[71] and many more.

Fast-forwarding to 2018, the most exciting event to happen in the meantime was the adoption of the GDPR in the EU. From the U.S. standpoint, the GDPR had a tremendous impact on the U.S. companies, non-profits, universities, and any other entity which processes the personal data of any EU citizen. Additionally, the GDPR unquestionably had an impact on the beginning of the implementation of more profound, almost *GDPResque* laws starting with the 2020 California Consumer Privacy Act,[72] followed by the Virginia's Consumer Data Protection Act and the Colorado's Privacy Act which shall come into effect on 1 January 2023.[73]

Overall, in accordance with many U.S. officials and business representatives, the U.S.'s path to the protection of data privacy is more nimble than what they see as the EU's "one size fits all" approach.[74] As we have seen, there is a jumble of hundreds of laws that have been passed in the U.S. on both the federal and state levels, and even though some U.S. advocates see that as a "patchwork" approach, the gap between the EU and the U.S. is narrowing.[75]

2.2. The Safe Harbour

When it comes to international data transfer, we must refer back to the Data Protection Directive, which had, as was previously said, not only expanded the rights and aspects related to data protection, but also laid out some new requirements that must be followed when transferring data pertaining to the EU citizens in third countries. The directive enforced the principle that personal data may be transferred to such countries only if they ensure an "adequate level of protection".[76] Naturally, such a

[69] Pub L No 104-191 § 264 [1996].
[70] 15 USC §§ 1681 [1970].
[71] 15 USC § 6801 [1999].
[72] Cal Civ Code § 1798.100 [2020].
[73] Eva J. Pulliam and others, 'Are You Ready for 2023? New Privacy Laws To Take Effect Next Year' [2022] 12 National Law Review 1, 1.
[74] Martin A. Weiss, Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' [2016] <https://sgp.fas.org/crs/misc/R44257.pdf> accessed 26 June 2022.
[75] Kyle Levenberg, F. Paul Pittman, 'Data Protection Laws and Regulations USA 2021-2022' <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq> accessed 26 June 2022.
[76] n 19, art 25 (1).

statement raises one inquiry – how shall third countries prove that they had provided an adequate level of protection? The answer to such a question lies in Article 25(2) of the Data Protection Directive, which reads:

"*The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.*"

So, in order for third countries to be recognized as adequate, they must comply with a number of items relating to both hard and soft law.

The EU and the U.S. recognized that such novelty threatened to disrupt or even prevent the transfer of personal data between them.[77] After all, the flow of data across the Atlantic is a form of international trade and is of crucial importance for both the EU and the U.S. economies.[78] After many discussions, the parties decided on a framework that would enable the U.S. businesses to meet the abovementioned adequate level of protection.[79] In 2000, the U.S. Department of Commerce issued a document called Safe Harbour Principles[80] whose aim was "*to diminish uncertainty and provide a more predictable framework for such data transfers … to foster, promote, and develop international commerce*" (hereinafter referred to as: the "**Safe Harbour**"). Subsequently, the European Commission acknowledged the Safe Harbour in its Decision of 26 July 2000[81] (hereinafter referred to as: the "**Safe Harbour Decision**").

[77] n 74, p 5.
[78] Ibid., p 4.
[79] Ibid., p 5.
[80] SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE ON JULY 21, 2000 [2000].
[81] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

Under the Safe Harbour, the U.S. companies were allowed to do an annual self-certification process whether they adhere to the seven basic principles which are as follows:[82]

1. **Notice** - Organizations must notify individuals about the purposes for which they collect and use information about them, how such data will be used and how to contact the data holder for any queries;
2. **Choice** - Organizations must offer individuals the opportunity to choose (opt out) out of the collection of their personal data and its forwarding to third parties;
3. **Onward Transfer** - The transfer of any data can only happen with a third party that meets the required data protection principles;
4. **Security** - Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction;
5. **Data Integrity** - A reasonable effort must be made to keep the data safe from loss/theft;
6. **Access** - Individuals must be able to access information held about them and correct or delete it;
7. **Enforcement** - There must be mechanisms for assuring compliance with the Safe Harbour, recourse for individuals to whom the data relate affected by non-compliance with it, and consequences for the organization when it is not followed.

The certification process itself was open solely to the U.S. companies that the U.S. Federal Trade Commission and the U.S. Department of Transportation deemed suitable, and more significantly, the procedure was not monitored at all by the U.S. Government.[83] Unsurprisingly, such a loose and informal process received a lot of criticism.[84]

2.2.1. Critiques of the Safe Harbour

[82] n 80.
[83] Tihomir Katulić, Goran Vojković, 'From Safe Harbour to European Data Protection Reform' [2016] MIPRO 2016/ISS 1694, 1695.
[84] Ibid.

An analysis conducted by Galexia,[85] a private consulting company with expertise in privacy and electronic commerce, was published by the European Commission in 2008. The Galexia report revealed the true level of security of the EU citizens' personal data when gathered and used by the U.S. companies, particularly when that data was obtained through new information society services.[86] It is important to note that the Galexia report was not the EU's first attempt to review the Safe Harbour, but it was definitely the most thorough one. The said framework was reviewed in 2002[87] and 2004[88] and even those reports expressed substantial doubts about the effectiveness of the Safe Harbour as a privacy protection mechanism.[89]

The Galexia report's highlights include, among others, the following findings:

- Foremost, even though there were more than 1,500 companies on the Safe Harbour list, only 1,109 of them were still actively participating in the Safe Harbour program at the time of conducting the report. Also, many of the listed companies had not renewed their certification and there were a lot of duplicate entries.
- The bare minimum requirements of the Safe Harbour were only met by 348 companies. Many of them either did not have a public privacy policy or did not even include principles set by the Safe Harbour in their policy.
- 206 companies falsely represented themselves as the Safe Harbor members on their public websites. Many of these untrue claims have persisted for a few years.
- The abovementioned Principle 7 is one of the most important compliance requirements for companies to adhere to the Safe Harbour. In order to comply with it, companies must choose an impartial dispute resolution provider, who is typically included in the self-certification entry and/or the public privacy policy. The issue was that many companies opted for American Arbitration Association or Judicial

[85] Galexia Pty Ltd. 'The US Safe Harbor - Fact or Fiction?' [2008] <https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf> accessed 21 July 2022.
[86] n 83, p 1695.
[87] The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce SEC [2002] 196.
[88] The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce SEC [2004] 1323.
[89] n 85.

Arbitration Meditation, which were too expensive for regular consumers, costing up to $1,200 an hour.[90]

To conclude, despite the fact that the Safe Harbour was seen by many in the EU as a mechanism to broadly and effectively secure the personal information of the EU citizens, it was actually a highly restrictive framework with a lot of limitations.

2.3. *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14)[91]

2.3.1. Context of the case[92]

Mr. Schrems has been a user of the popular social networking service Facebook since 2008. To use Facebook in the EU, at the time of registration one must enter into a contract with Facebook Ireland, a division of Facebook Inc., which is headquartered in the U.S. It is standard practice for Facebook Ireland to send users' personal data to its mother company Facebook Inc., where they undergo processing.

In 2013, Mr. Schrems filed a complaint with the Irish Data Protection Commissioner (hereinafter: the "**Irish DPC**") in which he asked the latter to utilize his statutory powers by prohibiting Facebook Ireland from sending Mr. Schrems' personal data to the U.S. In his complaint, Mr. Schrems claimed that the U.S. did no longer ensure an aforementioned adequate level of protection of the personal data against the surveillance activities that were engaged in the U.S. by the government authorities. In this context, Mr. Schrems made reference to Edward Snowden's revelations about the operations of the U.S. intelligence agencies, namely the National Security Agency (hereinafter: the "**NSA**"). The Irish DPC rejected the complaint as unfounded. It reasoned that there was no proof that the NSA had acquired Mr. Schrems' personal data and more importantly, that under the Safe Harbour Decision, the U.S. in fact did ensure an adequate level of protection.

Mr. Schrems took the case to the Irish High Court which, after taking into account the evidence presented by the parties, found that "*electronic surveillance and interception of personal data transferred from the EU to the U.S. serve necessary and indispensable objectives in the public interest*". It did, however, add that Edward

[90] Ibid.
[91] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.
[92] Ibid., paras 26-36.

Snowden's revelations had revealed "*serious overreach*" on the part of the NSA and other federal agencies. Also, the Irish High Court concluded that, if the main proceedings were to be decided solely on the basis of Irish law, it would then have to be determined that the Irish DPC should have continued to look into the issues raised by Mr. Schrems in his complaint and that the Irish DPC was incorrect in rejecting the complaint given the existence of serious doubt as to whether the U.S. provide an adequate level of protection of personal data. Nevertheless, the Irish High Court found that it is necessary to evaluate this case according to the EU law. It determined that the Safe Harbour did not adhere to the standards derived from both Articles 7 and 8 of the EU Charter and the guidelines established by the CJEU in its decision in *Digital Rights Ireland and Others*.[93] The EU Charter's goal is to safeguard the EU citizens' fundamental rights, hence it would be unacceptable if national authorities could violate it without facing repercussions. Further, the Irish High Court observed that Mr. Schrems has not formally disputed the legitimacy of the Safe Harbour Decision, but rather whether the Irish DPC was bound by such decision or whether the EU Charter gave him the authority to deviate from it. In those circumstances, the Irish High Court referred the following questions to the CJEU for a preliminary ruling:

1. Whether the Irish DPC was unconditionally bound by the Safe Harbour Decision while investigating an individual's complaint that personal data is being transferred to the U.S. where allegedly the laws and practices do not provide an adequate level of protection of personal data?
2. Alternatively, should or must the Irish DPC undertake an investigation with all the facts taken into consideration?

2.3.2. Judgement

This case (hereinafter referred to as: the "**Schrems I**") was decided on 6 October 2015 in the midst of the ongoing reform of data protection laws at the EU level, which centerpiece was finalization of the GDPR.[94] Only a fortnight before the final ruling, on 23 September 2015, the Advocate General Yves Bot issued his non-binding

[93] C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.
[94] Jenny Metzdorf, 'Case note on C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] <https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20Schrems.pdf> accessed 7 August 2022.

legal opinion.[95] In it, he stated that the Safe Harbour Decision for data transfer between the EU and the U.S. does not adequately protect the privacy of the EU citizens and must be ruled invalid.[96] Furthermore, he explained that such decision could not restrict the powers of the national supervisory authorities conferred under the Data Protection Directive.[97] The Advocate General's opinion had been the subject of a heated dispute, and the U.S. even released a statement contesting it.[98]

Nonetheless, the CJEU's final ruling closely echoes the view of the Advocate General Bot, and the following two aspects of the ruling are especially noteworthy.

a) Powers of the national supervisory authorities

First of all, the CJEU highlighted the significance of protecting personal data as a fundamental right, which is guaranteed by Articles 7 and 8 of the EU Charter.[99] Additionally, at the beginning of the analysis, it stated some of the principles of the Data Protection Directive, which should also be interpreted in light of the EU Charter, particularly the fact that the said directive allowed the EU Member States the ability to establish national supervisory authorities.[100] It is clear from Article 28(1) and (6) of the Data Protection Directive that the powers of such authorities only pertain to the processing of personal data carried out on the territory of their own Member State, and that they are not empowered, under Article 28, to oversee the processing of such data that takes place in a third country.[101] However, the CJEU's ruling states that the national supervisory authorities are in fact in charge of monitoring personal data processing carried out on their own territory, including transfers of such data outside the EU.[102] The national supervisory authorities must therefore be able to independently assess whether the transfer of a person's data to a third country complies with the obligations set forth by the Data Protection Directive, even if an adequacy decision has been adopted.[103]

---

[95] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2014] ECLI:EU:C:2015:650, Opinion of AG Bot.
[96] Ibid., para 216.
[97] Marina Škrinjar Vidović, 'Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities' [2015] 11 Croatian Yearbook of European Law & Policy 259, 263.
[98] Ibid.
[99] n 91, para 37.
[100] Ibid., para 40.
[101] Ibid., para 44.
[102] n 97, p 264.
[103] Ibid.

As a result, a person cannot be dissuaded from filing a complaint with the national supervisory authority regarding the protection of its rights and freedoms, and such authorities must have the ability to independently assess whether the data transfer complies with the EU standards.[104]

b) Invalidity of the Safe Harbour Decision

In this regard, the CJEU determined that the prior mentioned self-certification process imposed by the Safe Harbour, in which a company declares it will abide by the principles set forth by it, could only constitute a reliable measure of sufficiency if it was supported by mechanisms to track down and penalize companies that do not obey the principles.[105] The CJEU came to the conclusion that the Safe Harbour does not have that kind of system in place and that the principles for data transfer could be overridden by national security requirements set out in the U.S. law.[106]

Further, the CJEU found that whereas the EU legislation, as construed in light of the EU Charter and other case law, restricts state intrusion to what is absolutely essential, the Safe Harbour Decision permits the U.S. authorities to store all personal data on a general basis.[107] The CJEU ruled that such widespread data gathering and processing (i.e., mass surveillance), without the prospect of an effective remedy, violate the rights protected by the EU Charter.[108]

Lastly, Article 3 of the Safe Harbour Decision[109] limited the ability of the national supervisory authorities to take action to stop data transfers in the event that the level of data protection in the U.S. was insufficient.[110] This was also ruled to be against the Data Protection Directive in accordance with the previously defined roles and independence of the national supervisory authorities (discussed in section a)).[111]

All things considered, the CJEU declared the Safe Harbour Decision invalid.

2.3.3. Implications of the judgment

[104] n 84.
[105] n 97, p 267-268.
[106] Ibid.
[107] Ibid.
[108] n 91, para 95.
[109] n 81.
[110] n 97, p 268.
[111] Ibid.

In a statement[112] issued on the same day as the day of the final ruling, the U.S. Secretary of Commerce Penny Pritzker said that the U.S. Government is "*deeply disappointed in today's decision from the European Court of Justice, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy*". Furthermore, she added that "*the court's decision necessitates the release of the updated Safe Harbor Framework as soon as possible*".[113]

The Safe Harbor framework has been under revision since late 2013 to address concerns of the EU about the U.S. standards for data privacy and protection, particularly in the aftermath of the alleged "Snowden leaks".[114] Following *Schrems I*, the European Commission issued a statement[115] in which it echoed the abovementioned requests from the U.S. for the conclusion of a new and improved agreement and outlined three major goals for managing data transfers between the EU and the U.S. in the interim:

1. the protection of personal data transferred across the Atlantic;
2. securing the continuance of transatlantic data flows (by utilizing additional mechanisms under the Data Protection Directive);
3. cooperating with the national supervisory authorities to make sure that any alternative data transfer methods are handled in a coordinated manner (considered by many to be essential to avoid possibly conflicting national supervisory authorities' decisions and offer certainty for citizens and businesses alike).[116]

Following the European Commission's statement, the Article 29 Working Party, an independent advisory body made up of a representative from the national supervisory authority of each EU Member State, the European Data Protection Supervisor and the European Commission, reiterated that the EU–U.S. data transfers

[112] The U.S. Department of Commerce, 'Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision' [2015] <https://2014-2017.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice.html> accessed 15 August 2022.
[113] Ibid.
[114] n 74, p 8.
[115] 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)' [2015] <https://ec.europa.eu/commission/presscorner/detail/it/STATEMENT_15_5782> accessed 16 August 2022.
[116] n 74, p 8.

were unlawful and expressed deep concern over how the CJEU's conclusions would affect other mechanisms for data sharing under the Data Protection Directive.[117] In their press release, the Article 29 Working Party urgently called on the EU to engage in conversations with the U.S. authorities "*in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights*".[118] Additionally, their statement said: "*If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions*".[119] Thus, the Article 29 Working Party effectively gave the EU and the U.S. until 31 January 2016, to come to a replacement for the Safe Harbor.[120]

2.4. The Privacy Shield

On 2 February 2016, two days beyond the deadline set by the Article 29 Working Party, the EU and the U.S. officials unveiled that they have agreed on a new framework for transatlantic data flow under the name EU-US Privacy Shield[121] (hereinafter referred to as: the "**Privacy Shield**").[122] According to the press release, the new arrangement shall provide the U.S. businesses more responsibility to safeguard the personal data of the EU citizens, as well as better oversight and enforcement from the U.S. Federal Trade Commission and the U.S. Department of Commerce through increased collaboration with the EU national supervisory authorities.[123] Moreover, European Commissioner Jourová stated that "*for the first time ever, the United States has given the EU binding assurances that the access of public authorities for national*

[117] Ibid.
[118] Article 29 Working Party, 'Statement of the Article 29 Working Party' [2015] <https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 20 August 2022.
[119] Ibid.
[120] n 74, p 8.
[121] U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce' [2016] <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> accessed 21 August 2022.
[122] European Commission, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' [2016] <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216> accessed 21 August 2022.
[123] Ibid.

security purposes will be subject to clear limitations, safeguards and oversight mechanisms" and that "*the US has assured that it does not conduct mass or indiscriminate surveillance of Europeans*".[124] A few months later, on 12 July 2016, the European Commission issued a decision[125] that deemed the Privacy Shield adequate to enable transatlantic data transfers (hereinafter referred to as: the "**Privacy Shield Decision**").

The new framework is far longer and more extensive than its predecessor. Similar to the Safe Harbour system, in order to transfer personal data outside of the EU, an organization must self-certify to the U.S. Department of Commerce that it adheres to the principles outlined in the Privacy Shield.[126] The said principles, which are as follows, closely resemble the ones set by the Safe Harbour: (i) Notice; (ii) Choice; (iii) Accountability for Onward Transfer; (iv) Security; (v) Data Integrity and Purpose Limitation; (vi) Access, and (vii) Recourse, Enforcement and Liability.[127] This time, these principles are also complemented by an additional set which include provisions around sensitive data, journalistic exceptions, due diligence and audits, travel information, pharmaceutical and medical products, etc.[128]

Contrary to the Safe Harbour, the Privacy Shield places more emphasis on effective protection of the EU citizens' rights with several redress possibilities.[129] Anyone who believes their data has been compromised under the new framework, can either file a complaint (i) directly to companies, which have 45 days to address the complaint, or (ii) to their national supervisory authorities who shall channel the complaint to the U.S. Department of Commerce and/or the U.S. Federal Trade Commission to ensure that such complaints are investigated and resolved.[130] Additionally, there will be a free arbitration mechanism available as the last option if a complaint cannot be settled by any of the other means.[131] As for the complaints regarding potential access by the U.S. national intelligence agencies, they shall be

---

[124] Ibid.
[125] 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 [2016] OJ L 207.
[126] n 120.
[127] Ibid.
[128] n 74, p 9.
[129] Ibid, p 10.
[130] Ibid.
[131] European Commission, 'EU-U.S. Privacy Shield: Frequently Asked Questions' [2016] <https://ec.europa.eu/commission/presscorner/detail/hr/MEMO_16_2462> accessed 23 August 2022.

handled by a newly founded Ombudsperson in the U.S. State Department.[132] This new office shall be independent of the U.S. intelligence services. For the first Ombudsperson, the U.S. Department of Commerce Under Secretary Catherine Novelli, which also served as the Senior Coordinator for International Information Technology Diplomacy, had been designated.[133]

2.4.1. Critiques of the Privacy Shield

A few months after the announcement of the Privacy Shield, the Article 29 Working Party reviewed the new framework and issued its opinion on it.[134] At a first glance, their view of the new agreement is mixed. Even though they welcomed "*significant improvements brought by the Privacy Shield compared to the Safe Harbour decision*" and felt that "*many of the shortcomings of the Safe Harbour … have been addressed*", three major points of concern remained.[135]

The first issue is that the Privacy Shield Decision does not require organizations to erase data if it is no longer needed.[136] Keeping data for no longer than necessary to accomplish the purpose for which it was obtained is a crucial component of the EU data protection laws.[137] Secondly, Article 29 Working Party recognized that the U.S. administration has not entirely excluded the continuation of massive data gathering, which, in Article 29 Working Party's opinion, is "*unjustified interference with the fundamental rights of individuals*".[138] The adoption of the Ombudsperson is the third area of concern. Although the Article 29 Working Party applauds this unusual move adding a new redress and monitoring tool for individuals, questions remain over the Ombudsperson's authority to carry out his or her duties.[139]

All in all, the Privacy Shield certainly is an upgrade from the Safe Harbor, but despite that, it still had its many shortcomings. It appears that both the EU and the U.S.

---

[132] Ibid.
[133] U.S. Secretary of State, 'Letter from 7 July 2016' [2016] <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0b> accessed 23 August 2022.
[134] Article 29 Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision' [2016] <https://ec.europa.eu/newsroom/article29/items/640157/en> accessed 24 August 2022.
[135] Ibid., p 2.
[136] Ibid., p 57.
[137] Ibid.
[138] Ibid.
[139] Ibid.

were in a rush to introduce a new framework and that some aspects were not taken into account (e.g., the fact that the GDPR's final text was adopted at that time and some of its many novelties were overlooked). As Evan Schuman said in his analysis:[140] "*So the EU gets a solemn promise of privacy protections, which its voters want. And the U.S. gets no delays in data transfers, which U.S. companies want — a win-win in diplomatic terms, but a lose-win in reality, though one that the Europeans can stomach. Why? Because the inevitable privacy invasions will happen very quietly.*" He was right in a way since, as we shall see in the next section, the same fate befell the Privacy Shield as its predecessor.

3. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18)[141]

3.1. Context of the case

Following *Schrems I* in which the Safe Harbour Decision had been invalidated, the Irish High Court overturned the rejection of Mr. Schrems' complaint and referred that complaint back to the Irish DPC.[142] After aforementioned judgment, Facebook and other U.S. tech companies used standard contractual clauses (hereinafter referred as: the "**SCCs**") for the EU–U.S. data transfers.[143] SCCs are another mechanism for data transfer permitted by the EU legislation and are listed in Article 46 of the GDPR as one of the exceptions to the general adequacy decision.[144] Pursuant to Article 46 (which is previous Article 26 of the Data Protection Directive), in the absence of the adequacy decision, "*a controller[145] or processor[146] may transfer personal data to a third country or an international organization only if the controller or processor has provided*

[140] Evan Schuman, 'EU-U.S. data-transfer deal will never work' [2016] <https://www.computerworld.com/article/3029377/eu-u-s-data-transfer-deal-will-never-work.html> accessed 26 August 2022.
[141] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559.
[142] Ibid., para 54.
[143] Monika Zalnieriute, 'Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security' [2022] 55 Vanderbilt Journal of Transnational Law 1, 20.
[144] Ibid.
[145] Data controller is a natural person/entity which determines the purposes for which and the means by which personal data is processed. (*see* European Commission, 'What is a data controller or a data processor?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en> accessed 24 August 2022).
[146] Data processor is a natural person/entity which processes personal data on behalf of the controller. (*see* Ibid.)

appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available". These safeguards are (i) the mentioned SCCs that have been pre-approved by the European Commission; (ii) binding corporate rules, which are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises;[147] and (iii) other *ad hoc* contractual clauses that have been agreed upon by the controller and the processor, which may be considered appropriate provided they have been submitted to and approved by the competent national supervisory authority.[148] In light of this, the Irish DPC requested that Mr. Schrems reformulate his complaint.[149]

In his newly revised complaint, Mr. Schrems alleged, *inter alia*, that the U.S. law required Facebook Inc. to make the personal data provided to it accessible to specific U.S. authorities, such as the NSA and the Federal Bureau of Investigation (hereinafter referred to as: the "**FBI**").[150] He argued that the SCCs cannot support the transfer of such data to the U.S. because the data was utilized in the context of several monitoring programs in a way that violated the EU Charter.[151] Mr. Schrems requested the Irish DPC to ban or halt the transmission of his personal data to Facebook Inc. in those instances.[152]

Based on Mr. Schrems' reformulated complaint, the Irish DPC conducted the investigation and issued a draft decision outlining the preliminary results of his inquiry.[153] Those result stated that the personal information of the EU citizens transferred to the U.S. was likely to be consulted and processed by the U.S. authorities in a way that was incompatible with Articles 7 and 8 of the EU Charter and that the U.S. law did not give those citizens legal remedies compliant with Article 47 of the EU Charter.[154] Also, according to the Irish DPC, the SCCs are unable to correct these flaws since they merely give data subjects contractual rights against the data

[147] European Commission, 'Binding Corporate Rules (BCR)' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en> accessed 27 August 2022.
[148] n 143.
[149] n 141, para 54.
[150] Ibid., para 55.
[151] Ibid.
[152] Ibid.
[153] Ibid., para 56.
[154] Ibid.

exporter[155] and importer[156] and do not bind the U.S. authorities.[157] Based on the aforesaid, the Irish DPC requested the Irish High Court to refer a question on that matter to the CJEU. Sharing the same concerns as the Irish DPC, the Irish High Court on 4 May 2018 made the reference for a preliminary ruling to the CJEU.[158] That reference included eleven questions, which can be grouped into the following two most important concerns:

1) Whether the SCCs are valid in light of the EU Charter, and do they constitute a valid legal basis for transferring and processing personal data outside of the EU?
2) Whether the Privacy Shield Decision ensures an adequate level of protection for transferred data?[159]

3.2. The opinion of the Advocate General

Before the CJEU issued its ruling, Advocate General Saugmandsgaard Øe delivered his opinion[160] in which he clarified the distinction between an adequacy decision and the SCCs, which are both considered adequate safeguards for transfers of personal data to third countries under the GDPR.[161] However, in his view, these two methods differ according to the legal basis of the transfer. One the one hand, "*the purpose of an adequacy decision is to find that the third country concerned ensures, as a result of the law and practices of that country, a level of protection of the fundamental rights of the persons whose data are transferred essentially equivalent to that provided by the GDPR, read in the light of the Charter*".[162] As opposed to that, the SCCs must ensure such a level of protection by contractual means.[163] Although this

[155] Data exporter is a term used in the SCCs and means the controller who transfers personal data.
[156] Data importer is also a term used in the SCCs and means a controller or processor located in a third country that receives personal data from the data exporter.
[157] n 141, para 56.
[158] Ibid., para 57.
[159] Ibid., para 68.
[160] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559, opinion of AG Saugmandsgaard Øe.
[161] Jonathan Toornstra, 'The AG Opinion in Schrems II: one step closer towards responsibility?' <https://www.considerati.com/publications/the-ag-opinion-in-schrems-ii-one-step-closer-towards-responsibility.html> accessed 28 August 2022
[162] CJEU, 'PRESS RELEASE No 165/19' [2019] <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf> accessed 28 August 2022.
[163] n 161.

distinction is significant, it shouldn't have an impact on how personal data is protected once it has been shared with a third country.[164]

Due to the abovementioned, the validity of the SCCs' content is less of a concern for the Advocate General, who instead switches his attention to the practical implementation of the SCCs.[165] That is why, in his opinion, he stated that there is an "*obligation — placed on the controllers and, where the latter fail to act, on the supervisory authorities — to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with*".[166] The Advocate General came to the conclusion that his analysis revealed nothing to impair the validity of the SCCs.[167]

Lastly, the Advocate General also suggested that the CJEU should refrain from addressing the legality of the Privacy Shield Decision because that decision was already the subject matter of an action for annulment pending before the General Court of the CJEU.[168][169]

3.3. Judgement

To highlight the importance of the case, the CJEU chose to rule on the preliminary reference request as a Grand Chamber – a special fifteen-judge composition reserved for high-profile cases – and issued its decision on 16 July 2020.[170] In response to the two questions mentioned above, the CJEU has determined the following:

[164] Ibid.
[165] Ibid.
[166] n 160, para 128.
[167] Bengi Zeybek, 'ADVOCATE GENERAL DELIVERS OPINION IN SCHREMS II' [2020] <https://merlin.obs.coe.int/article/8780> accessed 28 August 2022.
[168] n 160, para 179.
[169] On 25 October 2016, the French privacy activist group La Quadrature du Net, along with FFDN and FDN, initiated a lawsuit to the CJEU against the Privacy Shield, arguing that it permitted abuses of mass surveillance by the U.S. Government. (*see* 'WHAT IS SCHREMS II?' <https://www.nqa.com/nl-nl/resources/blog/october-2020/schrems-ii> accessed 18 September 2022 and Case T-738/16 La Quadrature du Net and Others v Commission [2020] ECLI:EU:C:2020:791).
[170] n 143, p 24.

a) Validity of the SCCs

First of all, the CJEU stipulated that those who intend to transfer data based on the SCCs "*must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union*" by the GDPR.[171] In order to accomplish that, the evaluation of the degree of protection provided in the context of such a transfer must take into account the contractual provisions agreed upon by the controller/processor established in the EU and the recipient of the transfer established in the relevant third country, any access by public authorities to such data, and the legal system of the third country.[172] Therefore, it is the obligation of the data controller/processor established in the EU, above all, while collaborating with the recipient of the data, to determine on a case-by-case basis whether the law of the third country provides adequate protection for the transferred data, by providing the data subjects, if necessary, "*additional safeguards, enforceable rights, and effective legal remedies*".[173] If the controller or processor is unable to provide these "supplementary measures" to offer an appropriate degree of protection or if there is a discrepancy between the law of the third country and the SCCs, they shall suspend the transfer.[174] If they fail to do so, then the competent national supervisory authority must take action to either suspend or even prohibit such transfers.[175]

In the event that national supervisory authorities in the various Member States adopt divergent decisions about the adequacy of safeguards in the third country, the GDPR provides the possibility to refer such matter to the European Data Protection Board[176] (hereinafter referred to as: the "**EDPB**") for an opinion.[177] In such case, the EDPB may, under Article 65(1) of GDPR, adopt a binding decision.[178]

---

[171] n 141, para 105.
[172] Ibid.
[173] Ibid., para 103, 134.
[174] Ibid., para 135.
[175] Ibid., para 121.
[176] The EDPB is an independent body established by the GDPR, which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. (*see* EDPB, 'Who we are' <https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en> accessed 28 August 2022)
[177] n 141, para 147.
[178] Ibid.

Notwithstanding the above, the CJEU determined that where there is an adequacy decision, such as one made pursuant to the Privacy Shield, the mentioned powers of the national supervisory authorities to suspend or prohibit the transfer of personal data are prevented.[179] An adequacy decision of the European Commission must be followed, therefore, national supervisory authorities "*cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection*".[180] Rather, the national supervisory authorities must look into the complaints that they receive and if they have any concerns about the adequacy of protection, file a case in front of national courts.[181] These courts can then ask the CJEU to issue a preliminary ruling on the validity of an adequacy decision.[182] This process is in accordance with CJEU's ruling in *Schrems I*, and as we can see in the present case and as was previously indicated, the Irish High Court, after sharing doubts with the Irish DPC's findings, addressed the CJEU about the Privacy Shield Decision.

Ultimately, the CJEU determined that, if the controller or the processor provide "supplementary measures", the SCCs are a valid mechanism for ensuring essentially equivalent protection of data transfer to third countries to that guaranteed in the EU.[183]

b) Validity of the Privacy Shield Decision

While reviewing the Privacy Shield Decision, the CJEU applied the same analytical approach it had used to evaluate the SCCs – emphasizing that the GDPR should be understood and read in light of Articles 7, 8 and 47 of the EU Charter.[184] The CJEU construed the Privacy Shield Decision to allow interference with the fundamental rights of those whose data was transferred to the U.S., noting that it gave priority to the needs of the U.S. national security authorities and law enforcement.[185] Such interferences with rights protected in Articles 7 and 8 of the EU Charter were not *prima facie* unlawful, however, according to the CJEU, the US authorities' access to and use of personal data was not restricted in a way that satisfied the requirement for essential

[179] n 143, p 25.
[180] n 141, para 118.
[181] n 143, p 25.
[182] Ibid.
[183] Ibid.
[184] Róisín Áine Costello, 'Schrems II: Everything Is Illuminated?' [2020] 5 European Papers 1045, 1050.
[185] Ibid.

equivalence.[186] Additionally, the interferences, in particular some aspects under section 702 of FISA (or Foreign Intelligence Surveillance Act)[187] and Executive Order 12333,[188] were regarded as disproportionate.[189] The CJEU held that the mentioned section 702 of FISA, which authorized surveillance programs like PRISM and UPSTREAM,[190] did not restrict the amount of data collected to what was actually necessary, placed any restrictions on the programs' reach nor applied any minimum safeguards.[191] Further, Executive Order 12333 did not give data subjects any redress against the U.S. authorities in court.

Moreover, Article 47 of the EU Charter provides those whose rights and freedoms guaranteed by the EU law are violated a "*right to an effective remedy before a tribunal".*[192] Although an Ombudsperson was established by the Privacy Shield Decision, the aforementioned surveillance programs do not grant data subjects any enforceable rights, providing no effective remedy against the U.S. authorities.[193]

With all things taken into account, the CJEU concluded that the Privacy Shield Decision "*cannot ensure a level of protection essentially equivalent to that arising from the Charter*" and was, therefore, ruled invalid.[194]

4. What next? The aftermath of *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18)

As we have seen in the previous section, the CJEU in the aforementioned case (hereinafter referred to as: the "**Schrems II**") invalidated the Privacy Shield Decision but upheld the use of the SCCs. If used, organizations need to implement "supplementary measures", where necessary, to compensate for the lack of data

[186] Ibid., 1050-1051.
[187] 50 USC ch 36 [1972].
[188] 40 Fed Reg 59.941 [1981]
[189] n 184, p 1051.
[190] PRISM and UPSTREAM were surveillance programs authorized under section 702 of FISA. In relation to the former, internet service providers were required, in accordance with court rulings, to provide the NSA with copies of all communications going to and coming from a "selector," some of which are also sent to the FBI and the CIA. In connection with UPSTREAM, the NSA has access to both the metadata and the content of communications in internet traffic flows. Specifically, Executive Order 12333 allows the NSA to access data in transit to the U.S. by accessing the underwater cables through which internet communications reach that jurisdiction. (*see* n 135, para 61-63 and n 175).
[191] n 143, p 25-26.
[192] n 141, para 186.
[193] n 143, p 26.
[194] n 141, para 181.

protection in the third country. Nonetheless, I believe the CJEU missed the opportunity to address what these "supplementary measures" are. In order to close this gap, the EDPB issued recommendations, which will be discussed in detail below, and ultimately, the new SCCs were issued.

4.1. The European Data Protection Board's recommendations

Only a few months after *Schrems II*, the EDPB has issued recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.[195] These recommendations offer a six-step roadmap to help organizations in meeting the requirements set forth by the CJEU in *Schrems II*, in particular, to assist data exporters in fulfilling their obligation to determine when supplementary measures are required for data being exported to third countries that do not have an EU adequacy decision.[196] Following are the mentioned six steps:

1. Know your transfer – Data exporters should be fully aware of their transfers of personal data to third countries. Also, they should verify if the "*transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed*".[197]
2. Verify the transfer tool your transfer relies on – These transfer tools include either the prior mentioned SCCs or binding corporate rules. If, on the other hand, the European Commission adopted an adequacy decision, then the only obligation is to monitor its ongoing validity.[198]
3. Assess whether the mentioned transfer tools you are relying on are effective in light of all circumstances of the transfer – Data exporters, in collaboration with the data importers, should conduct a Transfer Impact Assessment (hereinafter referred to as: the "**TIA**") to asses "*if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards*

[195] EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' [2021] <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 30 August 2022.
[196] Debbie Heywood, 'EDPB guidance on supplementary measures for data transfers' [2021] <https://globaldatahub.taylorwessing.com/article/edpb-guidance-on-supplementary-measures-for-data-transfers> accessed 30 August 2022.
[197] n 195, p 3.
[198] n 196.

of the transfer tools". This assessment should concentrate on pertinent third country laws and practices about the specific data being transferred.[199]

4. Identify and adopt supplementary measures – If the TIA indicated that the transfer tools are not effective, data exporters should adopt necessary supplementary measures to bring the level of protection of the data transferred up to the EU standard of essential equivalence.[200]
5. Take any formal procedural steps the adoption of your supplementary measure may require, depending on the transfer tool you are relying on.[201]
6. The final step is to re-evaluate the level of protection provided to the personal data you transfer to third countries at suitable intervals and assess whether there have been or will be any developments that may have an impact on it.[202]

4.2. The New Standard Contractual Clauses

The earlier SCCs, which were first introduced in 2001, were created for a pre-GDPR environment and thus lacked many of the protections that the GDPR requires.[203] When the CJEU's decision in *Schrems II* questioned the validity of SCCs as a data transfer mechanism unless supplementary measures are implemented, it became urgently necessary to adopt revised SCCs.[204] The European Commission, on 4 June 2021, adopted updated versions of the SCCs which adhere to the GDPR requirements, as well as take into account findings from *Schrems II* and the aforementioned EDPB's recommendations.[205] Two sets of the SCCs were issued – one[206] for use within the EU and the other[207] for the transfer of personal data to third countries.

---

[199] n 195, p 4.
[200] Marcelo Corrales Compagnucci and others, 'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)' [2021] 2021 (2) NORDIC JOURNAL OF EUROPEAN LAW 38, 42.
[201] n 195, p 4.
[202] Ibid.
[203] Phillip Lee, 'The Updated Standard Contractual Clauses: A New Hope?' [2021] <https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/> accessed 31 August 2022.
[204] Ibid.
[205] n 200, p 43.
[206] European Commission, 'Standard Contractual Clauses for controllers and processors in the EU' [2021] <https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors> accessed 31 August 2022.
[207] European Commission, 'Standard Contractual Clauses for international transfers' [2021] <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-

As opposed to the earlier set of SCCs, which provided limited options for data transfers and separate sets of provisions, the "modular approach" used by the new SCCs provides much greater flexibility.[208] Now there are four modules: (i) controller-to-controller; (ii) controller-to-processor; (iii) processor-to-processor; and (ii) processor-to-controller. Simply put, data exporting parties only apply the clauses that are appropriate to the module they select based on the nature of their exports.[209]

Additionally, according to the prior SCCs, the data exporter could only be a party established in the EU.[210] This presented obstacles for data export compliance where a data exporter was established outside of the EU, but nevertheless subject to the GDPR because of its extraterritorial scope from Article 3(2).[211] This deficiency was resolved by the new SCCs acknowledging that the entity exporting the data can be a non-EU entity.[212]

The new SCCs also have two minor but important changes over the previous SCCs: they permit contracts between multiple data exporting parties and allow new parties to be added to them over time through the so-called “docking clause”.[213] This will be a welcome relief, especially for organizations that depend on SCCs for intra-group transfers.[214] As new group companies may be formed over time or purchased, the SCCs will need to be updated to reflect these additions.[215]

Last but not least, a more thorough list of the technical and organizational measures required to guarantee an adequate level of protection, including measures to safeguard the security of the data, is provided in Annex II of the new SSCs.[216] The list is not exhaustive, but it does include actions that can be taken to help the parties.[217]

---

protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en> accessed 31 August 2022.
[208] n 200, p 43.
[209] n 203.
[210] Ibid.
[211] n 200, p 43.
[212] Ibid.
[213] n 203.
[214] Ibid.
[215] Ibid.
[216] n 200, p 44.
[217] Ibid.

Regarding the transition period, the new SCCs allowed the earlier to be used up until 27 September 2021. After that, organizations are only able to use new ones and they have until 27 December 2022 to fully adapt to the new framework.

4.3. The new Trans-Atlantic Data Privacy Framework

The European Commission and the U.S. released a joint statement on 25 March 2022 that they have reached an agreement in principle on a new Trans-Atlantic Data Privacy Framework that will promote transatlantic data flows and address the issues raised by the *Schrems II* ruling.[218] Some of the key principles of a new framework, according to the factsheet that was issued alongside the statement,[219] are:

- A new set of rules and binding safeguards shall limit access to data by the U.S. intelligence agencies to what is necessary and proportionate to protect national security. In regard to that, such agencies will implement procedures to assure efficient oversight of new privacy and civil liberties standards.
- A new, two-tiered redress system that includes a Data Protection Review Court to look into and adjudicate concerns from the EU citizens over the use of their data by U.S. intelligence agencies.
- Companies that process data transferred from the EU will continue to self-certify their adherence to the principles (which will be brought) through the U.S. Department of Commerce.
- Specific monitoring and review mechanisms.

Both the EU and the U.S. agree that a new framework will have significant positive effects on both sides of the Atlantic.[220] For the EU citizens, this deal includes new stringent obligations for the protection of their personal data.[221] Additionally, new framework will enable the continued flow of data that supports more than one trillion dollars in cross-border trade annually for people and businesses on both sides of the

[218] European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' [2022] <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 1 September 2022.
[219] European Commission, 'Trans-Atlantic Data Privacy Framework' [2022] <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 1 September 2022.
[220] The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' [2022] <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 1 September 2022.
[221] Ibid.

Atlantic and will allow enterprises of all sizes to compete in each other's marketplaces.[222]

So, when should the Privacy Shield's successor take effect? In an interview with The Washington Post, which was in June this year, the European Commissioner for Justice Didier Reynders offered update on a new framework and said: "*To have an adequacy decision on our side will take around six months, so will be [on course] for the end of the year, the first quarter of next year, if it's possible to exchange on the legal text before the summer*."[223]

Overall, we can expect the third agreement for transatlantic data transfer between the EU and the U.S. to take effect during 2023. Taking into account the mentioned key principles from the new framework, it seems that it brings certain improvements compared to its two predecessors. Nevertheless, it is also possible that some novelties (e.g., establishment of the Data Protection Review Court) ends up being a total fiasco just like some features in the Safe Harbour or the Privacy Shield were (e.g., introduction of the Ombudsperson role, which, in the end, was not nearly effective redress option). Despite everything, I personally believe that such fiascos will not occur, and that the new agreement will result in much higher level of personal data protection than before, largely because both the EU and the U.S. officials know that if their agreement is taken down again by the CJEU, it will significantly affect their credibility.

5. Conclusion

Taking into account everything previously written, it is difficult to give a conclusion. Why? Because the protection of personal data is a living thing. What I write today may not be relevant tomorrow and *vice versa.* Nevertheless, some things are certain. We live in a world of ubiquitous technology in which appears to be uncontrolled data harvesting. The EU is trying to regulate that, especially regarding international transfer of the EU citizens' personal data. And it appears they are successful.

[222] Ibid.
[223] The Washington Post, 'E.U. justice chief 'confident' data deal with U.S. will survive legal challenge' [2022] <https://www.washingtonpost.com/politics/2022/06/08/eu-justice-chief-confident-data-deal-with-us-will-survive-legal-challenge/> accessed 1 September 2022.

The EU, with its estimated population of 447 million and as one of the wealthiest consumer markets in the world, has an ability to conduct so called “legal globalization”.[224] In other words, the EU is attractive market to numerous international companies, which, if they want to conduct business, must adhere to the EU legislation. Take the well-known GDPR as an example. The U.S. companies that want to continue with their business in the EU, i.e., which offer goods or services in the EU or process the EU citizens' personal data, have two options. One of them is to fully comply with the GDPR (due to the previously mentioned extraterritoriality, which means the GDPR applies to non-EU entities) or quit doing business in the EU. I think it is unnecessary to explain how unacceptable the latter is for most companies, but unfortunately, that is sometimes the only option. According to Forbes, companies from the Global Fortune 500 list spend an estimated 7 billion euros in compliance costs for the GDPR.[225] Because of these astronomical expenses, some U.S. businesses were forced to stop doing business in the EU, especially as they found it far harder to comply with the GDPR than their peers in the EU (since many of the GDPR requirements previously existed in EU law).[226] Anu Bradford calls this phenomenon of the EU’s legislation spreading beyond its borders – the “Brussels Effect”.[227]

In this master thesis, I demonstrated that effect through two famous CJEU’s cases which regulate the transfer of the EU citizens’ personal data to the U.S. Personally, I value my privacy, especially in this modern world where everybody knows everything about everyone in just a click of a mouse. So, for me, what the EU doing and the effect it has on how my personal data will be collected is extremely important. Also, with the new agreement in place, I believe that the level of data protection will be raised to an even higher level, especially since I hope that both the EU and the U.S. have learned from the mistakes of the Safe Harbour and the Privacy Shield. After all, as they say, the third time is the charm!

---

[224] 'What is the Brussels Effect, and what does it mean for global regulation?' [2020] <https://blogs.microsoft.com/eupolicy/2020/10/26/what-is-the-brussels-effect-and-what-does-it-mean-for-global-regulation/> accessed 3 September 2022.
[225] 'The GDPR Racket: Who's Making Money From This $9bn Business Shakedown' [2018] <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=3d4860e234a2> accessed 12 September 2022.
[226] Ibid.
[227] Anu Bradford, 'The Brussels Effect' [2012] 107 Northwestern University Law Review 1, 3.

6. Bibliography

Books and articles:

- Anu Bradford, 'The Brussels Effect' [2012] 107 Northwestern University Law Review 1.
- Marcelo Corrales Compagnucci and others, 'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)' [2021] 2021 (2) Nordic Journal of European Law 38.
- Róisín Áine Costello, 'Schrems II: Everything Is Illuminated?' [2020] 5 European Papers 1045.
- Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' [2014] Collected Courses of the European University Institute's Academy of European Law.
- Harry Kalven Jr., 'Privacy in Tort Law—Were Warren and Brandeis Wrong?' [1966] 31 Law and Contemporary Problems 326.
- Tihomir Katulić, Goran Vojković, 'From Safe Harbour to European Data Protection Reform' [2016] MIPRO 2016/ISS 1694.
- Irwin R. Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' [1990] 39 Catholic University Law Review 703.
- William L. Prosser, 'Privacy' [1960] 48 California Law Review 383.
- Eva J. Pulliam and others, 'Are You Ready for 2023? New Privacy Laws To Take Effect Next Year' [2022] 12 National Law Review 1.
- Daniel J. Solove, 'A Brief History of Information Privacy Law' [2006] Proskauer on Privacy 1.
- Marina Škrinjar Vidović, 'Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities' [2015] 11 Croatian Yearbook of European Law & Policy 259.
- Samuel D. Warren, Louis D. Brandeis, 'The Right to Privacy' [1890] 4 Harvard Law Review 193.
- Monika Zalnieriute, 'Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security' [2022] 55 Vanderbilt Journal of Transnational Law 1.

EU case law and opinions of the Advocate General:

- C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238.
- Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2014] ECLI:EU:C:2015:650, Opinion of AG Bot.
- Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.
- Case T-738/16 La Quadrature du Net and Others v Commission [2020] ECLI:EU:C:2020:791.
- Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559, opinion of AG Saugmandsgaard Øe.
- Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559.

Treaties, legislation, and other legal sources:

- Convention for the Protection of Human Rights and Fundamental Freedoms, as amended [1950].
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981].
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.
- Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
- Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/1.
- Consolidated version of the Treaty on European Union [2007] OJ C 362/390.

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012] COM/2012/011 final - 2012/0011 (COD).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
- Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 11 June 2015, 2012/0011 (COD).
- 171 NY 538, 64 NE 442 [1902].
- NY Civ Rights L § 50 [2014].
- 381 US 479 [1965].
- 389 US 347 [1967].
- 410 US 113 [1973].
- 405 US 438 [1972].
- 20 USC § 1232g 34 CFR Part 99 [1974].
- 5 USC § 552a [1974].
- Pub L No 104-191 § 264 [1996].
- 15 USC §§ 1681 [1970].
- 15 USC § 6801 [1999].
- Cal Civ Code § 1798.100 [2020].
- SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE ON JULY 21, 2000 [2000].
- 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

- The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce SEC [2002].
- The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce SEC [2004].
- 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 [2016] OJ L 207.
- 50 USC ch 36 [1972].
- 40 Fed Reg 59.941 [1981]

Web based sources:

- Article 29 Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision' [2016] <https://ec.europa.eu/newsroom/article29/items/640157/en> accessed 24 August 2022.
- Article 29 Working Party, 'Statement of the Article 29 Working Party' [2015] <https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 20 August 2022.
- Ben Wolford, ’What is GDPR, the EU’s new data protection law?’ <https://gdpr.eu/what-is-gdpr/> accessed 21 June 2022.
- Bengi Zeybek, 'ADVOCATE GENERAL DELIVERS OPINION IN SCHREMS II' [2020] <https://merlin.obs.coe.int/article/8780> accessed 28 August 2022.
- CJEU, 'PRESS RELEASE No 165/19' [2019] <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf> accessed 28 August 2022.

- 'DATA PRIVACY ACT: A BRIEF HISTORY OF MODERN DATA PRIVACY LAWS' [2018] <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy laws#:~:text=The%201970s%20%E2%80%93%20The%20First%20Modern%20Data%20Privacy%20Laws&text=In%201973%2C%20Sweden%20created%20the,freedom%20to%20access%20their%20records> accessed 22 June 2022.
- 'Data Protection in France' <https://gdprhub.eu/Data_Protection_in_France> accessed 22 June 2022.
- 'Data Protection in Germany' <https://gdprhub.eu/index.php?title=Data_Protection_in_Germany> accessed 22 June 2022.
- Debbie Heywood, 'EDPB guidance on supplementary measures for data transfers' [2021] <https://globaldatahub.taylorwessing.com/article/edpb-guidance-on-supplementary-measures-for-data-transfers> accessed 30 August 2022.
- EDPB, 'Who we are' <https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en> accessed 28 August 2022.
- EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' [2021] <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 30 August 2022.
- European Commission, 'What is a data controller or a data processor?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en> accessed 24 August 2022.
- European Commission, 'Binding Corporate Rules (BCR)' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en> accessed 27 August 2022.
- European Commission, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' [2016]

<https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216> accessed 21 August 2022.

- European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' [2022] <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 1 September 2022.
- European Commission, 'EU-U.S. Privacy Shield: Frequently Asked Questions' [2016] <https://ec.europa.eu/commission/presscorner/detail/hr/MEMO_16_2462> accessed 23 August 2022.
- 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)' [2015] <https://ec.europa.eu/commission/presscorner/detail/it/STATEMENT_15_578> accessed 16 August 2022.
- European Commission, 'Standard Contractual Clauses for controllers and processors in the EU' [2021] <https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clausescontrollers-and-processors> accessed 31 August 2022.
- European Commission, 'Standard Contractual Clauses for international transfers' [2021] <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standardcontractual-clauses-scc/standard-contractual-clauses-international-transfers_en> accessed 31 August 2022.
- European Commission, 'Trans-Atlantic Data Privacy Framework' [2022] <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 1 September 2022.
- Evan Schuman, 'EU-U.S. data-transfer deal will never work' [2016] <https://www.computerworld.com/article/3029377/eu-u-s-data-transfer-deal-will-never-work.html> accessed 26 August 2022.
- Galexia Pty Ltd. 'The US Safe Harbor - Fact or Fiction?' [2008] <https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf> accessed 21 July 2022.

- International Association of Privacy Professionals, 'What does privacy mean?' <https://iapp.org/about/what-is-privacy/> accessed 1 September 2022.
- Jenny Metzdorf, 'Case note on C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] <https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20Schrems.pdf> accessed 7 August 2022.
- Jonathan Toornstra, 'The AG Opinion in Schrems II: one step closer towards responsibility?' <https://www.considerati.com/publications/the-ag-opinion-in-schrems-ii-one-step-closer-towards-responsibility.html> accessed 28 August 2022
- Kara Nortman, 'Data is the world's most valuable (and vulnerable) resource' [2021] <https://techcrunch.com/2021/03/04/data-is-the-worlds-most-valuable-and-vulnerable-resource/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACQWNuoOTAw0ffXbog0DNsjo5hYR_WInzdC2S4Ld27pcVybLIBzK7vXKGD5mbE8Zty6c-vdpLbILT82HVp05lPgWCcCu_8D-fILBAigjkJxNSRHWswPdto6Ln99s7jRf9-webjD05KrwvQ6kpDzsKtuxncf144z9FSkz6Mc5CPwi> accessed 1 September 2022.
- Kyle Levenberg, F. Paul Pittman, 'Data Protection Laws and Regulations USA 2021-2022' <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq> accessed 26 June 2022.
- Martin A. Weiss, Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' [2016] <https://sgp.fas.org/crs/misc/R44257.pdf> accessed 26 June 2022.
- Olga Stepanova, Patricia Jechel, 'The Privacy, Data Protection and Cybersecurity Law Review: Germany' [2021] <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,(BDSG)%20entered%20into%20force> accessed 22 June 2022.

- 'Overview of Privacy and Privacy Legislation' <https://projects.iq.harvard.edu/privacyproject/overview-privacy-legislation#:~:text=Warren%20and%20Brandeis%20defend%20privacy,be%20protected%20by%20contract%20law> accessed 25 June 2022.
- Phillip Lee, 'The Updated Standard Contractual Clauses: A New Hope?' [2021] <https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/> accessed 31 August 2022.
- 'PRIVACY ACT OF 1974' [2021] <https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies> accessed 26 June 2022.
- 'Sources of Data Protection Law' <https://www.clarin.eu/content/sources-data-protection-law> accessed 22 June 2022.
- Stephen Ragan, Petruta Pirvan, 'What is Convention 108?' <https://www.wrangu.com/what-is-convention-108/> accessed 22 June 2022.
- The Economist, 'The world's most valuable resource is no longer oil, but data' [2017] <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 1 September 2022.
- 'The GDPR Racket: Who's Making Money From This $9bn Business Shakedown' [2018] <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=3d4860e234a2> accessed 12 September 2022.
- The U.S. Department of Commerce, 'Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision' [2015] <https://2014-2017.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice.html> accessed 15 August 2022.
- The Washington Post, 'E.U. justice chief 'confident' data deal with U.S. will survive legal challenge' [2022] <https://www.washingtonpost.com/politics/2022/06/08/eu-justice-chief-confident-data-deal-with-us-will-survive-legal-challenge/> accessed 1 September 2022.
- The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' [2022]

<https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 1 September 2022.

- U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce' [2016] <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> accessed 21 August 2022.
- U.S. Secretary of State, 'Letter from 7 July 2016' [2016] <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0b> accessed 23 August 2022.
- 'What is the Brussels Effect, and what does it mean for global regulation?' [2020] <https://blogs.microsoft.com/eupolicy/2020/10/26/what-is-the-brussels-effect-and-what-does-it-mean-for-global-regulation/> accessed 3 September 2022.
- 'WHAT IS SCHREMS II?' <https://www.nqa.com/nl-nl/resources/blog/october-2020/schrems-ii> accessed 18 September 2022.