*Giovanni Tricco**

THE NEW TRANSATLANTIC DATA AGREEMENT PLACED IN CONTEXT: DECODING THE SCHREMS SAGA WITHIN THE DIGITAL ECONOMY

Abstract

Any time we use digital services we create data. That data travels around continents, constituting the fundamentals of the digital economy. Begun in 2015, the Agreements that allowed this kind of free flow of data between the EU and the US have been invalidated – the Safe Harbour and the Privacy Shield – bringing uncertainty in the work of over 5300 companies that based their practices on such frameworks which allowed data to move borderless, as well as, threatening the digital rights of European citizens who do not see their data adequately protected across the Atlantic. Indeed, in Data Protection Commission v. Facebook Ireland – Schrems II – the CJEU claimed that US surveillance law offers inadequate safeguards for EU citizens' data. In the summer of 2023, the transatlantic actor unlocked the gridlock with the new adequacy decision of the EU based on the new Transatlantic Data Privacy Framework, amid debate on the adequacy offered by it. The question of whether the new pact will ensure long-standing data flow between the two sides of the Atlantic remains open.

The question is of extreme importance, such data transfers are fundamental to conducting international trade and commerce in today's globally connected world. Therefore, people and businesses can use cross-border data flows to communicate online, map global supply chains, share research, provide cross-border services, and drive technological innovation. The trade and investment relationships between the US and the EU are broad and highly intertwined. The United States and the European Union have the highest cross-border data flows in the world, valued at $7.1 trillion dollars annually, which are critical to much of the economic interaction between the two countries. The article aims to shed light on the problems experienced with the invalidation of the previous two agreements, with an analysis of American surveillance laws and questioning whether the new agreement could be the base for a stable transatlantic digital economy.

JEL CLASSIFICATION: F52; K24; K33; L38.

SUMMARY

* PhD candidate in the Joint International Doctorate in Law, Science and Technology at the University of Bologna & Vrije Universiteit Brussel.

surveillance law – 3.1 Case-law as basis for the wide scope of U.S. foreigner surveillance law – 3.2 United States foreign surveillance law: section 702 FISA and Executive Order 12333 – 3.2.1 The Foreign Intelligence Surveillance Act (FISA): section 702 – 3.2.2 Executive Order 12333 and PPD-28 – 4 Towards a stable digital economy or unfolding a new chapter in the Schrems saga? – 5 Conclusions

1 Introduction

On the 10th of July 2023, the European Union granted an adequacy decision based on the new Transatlantic Data Privacy Framework to heal the gridlock that the digital economy was facing. The research intends to navigate the challenges that the new Privacy Framework will face in the time ahead to pass the test of a well-expected Schrems III. Namely posing appropriate safeguards against the intrusion of US surveillance authorities in European data and the establishment of a functional court to ensure judicial redress for Europeans in case of misuse of their data.

The two transatlantic actors adopted historically different approaches to privacy and the protection of data. The EU considers the privacy of communications and the protection of personal data as fundamental rights, under EU law, whilst US law protects certain data on a sectoral basis, without comprehensive federal legislation. These differing approaches have resulted in a discernible privacy law gap. The research accompanies the readers on the differences and similarities between the two frameworks and surveillance capabilities, till analysing the possible legal and policy challenges that must be overcome to ensure that the new Framework will withstand a new challenge in the European courts.

The article will be structured in three main sections. The first section aims to describe and explore the scenario surrounding EU-US Data transfer agreements, from an economic, legal, and political perspective. Thus, it continues with a brief analysis of European Data Protection Law and compares the different approaches to privacy and data protection on the two sides of the Atlantic. Indeed, the disagreement between the transatlantic actors is a consequence of different approaches, understanding, and cultures of privacy and data protection, each with its intuitive sensibility that has resulted in two very diverse privacy laws. An analysis of the development of privacy law on both sides of the Atlantic is needed to understand the actual situation. Then, it concludes with an analysis of the failure of the two previous data transfer agreements.

The second section explores the main reason for the concerns of the CJEU, namely United States Surveillance law, through an analysis of the case law that has widened the capabilities of the U.S. Intelligence Communities over the years, as well as the laws that confer such powers to the U.S. authorities: section 702 of the Foreign Intelligence Service Act and Executive Order 12333.

The third section tries to analyse whether the new Privacy framework negotiated by European and United States officials will satisfy the concerns raised by the CJEU in

Schrems II, to constitute a proper and stable new 'Enhanced Privacy Shield' that would constitute a stable basement for the digital economy.

The topic is of extreme importance, first to ensure an adequate level of protection of citizens' data, secondly to foster the interoperability and openness of the internet to permit the digital economy to flourish as a borderless data economy in the near future of safe digital trade.

2 Transatlantic Data Transfers Placed In Context: Political, Historical, And Economical Considerations

The stakes are high, in the near future if a transatlantic data agreement does not survive the scrutiny of the CJEU legal uncertainty will persist and future economic losses for the digital economy of the EU and the U.S. will escalate. According to forecasts of DIGITALEUROPE by 2030 if a stable agreement that enables lawful and consistent data transfer is not in place the European Union economy could lose:

- €1.3 trillion in cumulative economic growth by 2030, which is the equivalent of the GDP of the Spanish economy each year.
- €116 billion in annual exports, which is the equivalent of the annual exports of Sweden or the aggregate annual export of several smaller Members of the EU.
- 1.3 million job losses, primarily high-skilled professions.

If the agreement constitutes a stable mechanism of data transfer the EU economy would benefit from:

- €720 billion in cumulative extra growth by 2030, equivalent to an increase of 0.6% in GDP every year.
- €60 billion in annual exports, of which half come from the manufacturing sector, boosting the position of European SMEs.
- 700 thousand new jobs will be created.[1]

Hence, it is crucial that the new agreement constitute a lasting Data Flow agreement, fostering, and sustaining the data economy. The article questions whether this will be the case or if another Schrems saga looms on the horizon.

[1] DIGITALEUROPE, 'Data Flows & the Digital Decade' (2021) <https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf> accessed 11 March 2024. Digital Europe is a trade association representing the interest of the tech industry in Europe.

2.1 A different approach on privacy and data protection

The disagreement between the transatlantic actors resulted from a different approach, understanding, and cultural background of privacy and data protection, each with its intuitive sensibility that has resulted in two diverse privacy laws.[2] An analysis of the development of privacy law on both sides of the Atlantic is needed to understand the diatribes experienced.

Notwithstanding, in both Europe and the United States, early discussions regarding data protection and privacy focused on the same concern about increasing surveillance capabilities of government and administrative bodies.[3] Nevertheless, a consensus arose that the 'fair information principles'[4], which define how personal information should be handled, would be the best way to address these concerns. These principles centred on policies of transparency on the use, disclosure, secondary use, correction, and security of personal data. However, the principles did not lay out specific legal obligations, although they did give a framework for weighing data privacy against other considerations.[5] Therefore, since their establishment, the fair information principles guided the United States approach regarding privacy protection.[6] Moreover, their influence extended far beyond the United States, the ideas provided the groundwork for the adoption of future legal frameworks worldwide. Indeed, not just for U.S. laws such as the Privacy Act of 1974[7], but also for the first data protection laws implemented in Western Europe such as in France and Germany in the 1970s.[8] For example, the Lander of Hesse in Germany established the first data protection law worldwide in 1970.[9] The latter was followed by Germany and France which adopted the first federal and national data protection legislation in 1978.[10]

Although the principles adopted by Western democracies in the early 1970s were similar, significant disparities soon appeared in how such policies should be implemented and who would fall within their scope. The initial discussion focused on

[2] James Q Whitman, 'The two western cultures of privacy: Dignity versus liberty' (2003) 113 Yale LJ 1151.
[3] Colin J Bennett '*Regulating privacy*' (Cornell University Press 2018).
[4] IAPP, 'Fair Information Practice Principle' <https://iapp.org/resources/article/fair-information-practices/> accessed 11 March 2024.
[5] Robert Gellman, 'Fair Information Practices: A Basic History' Version 2.22 (2022) <file:///C:/Users/tmikoni/Downloads/SSRN-id2415020.pdf> accessed 11 March 2024.
[6] Alan F Westin, 'Social and political dimensions of privacy (2003) 59(2) Journal of social issues 431.
[7] The United States Department of Justice, 'The Privacy Act of 1974' <https://www.justice.gov/opcl/privacy-act-1974> accessed 11 March 2024.
[8] Marc Rotenberg, 'Fair information practices and the architecture of privacy (What Larry doesn't get)' [2001] Stanford Technology Law Review 1.
[9] Government of the state of Hessel, 'Data Protection Act 1970' <https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes> accessed 11 March 2024.
[10] For France, see Loi N° 78-17, 6 January 1978 <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460?init=true&page=1&query=Loi+N%C2%B0+78-17&searchField=ALL&tab_selection=all> accessed 11 March 2024; for Germany, Federal Data Protection Act 1977 <https://www.gesetze-im-internet.de/englisch_bdsg> accessed 11 March 2024.

discussion on governmental use of personal data quickly evolved to encompass the private industry as more private enterprises advanced their data processing methods to gather considerable amounts of personal data for business goals, therefore, advocating the government to adopt business-friendly laws.[11]

Disagreements on how to construct such legal frameworks and policies result from different values and cultures on which different legal systems are based as stated by Whitman: "*any person has legal and social values of the societies in which we live. In particular, we have […] intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture.*"[12] Therefore, as a result, different approaches take place. Such variances can be connected to the conceptions of privacy designed by Post namely: "*privacy as an aspect of dignity and privacy as an aspect of liberty.*"[13] The European approach to privacy is based on the concept of dignity, while the American approach is based on the pursuit of liberty. The former is concerned with the right to govern the information that is made public about oneself to maintain control over one's public image; the latter is much more focused on liberty versus the state, i.e., freedom against government intrusion.[14]

In addition, the past history of fascist and totalitarian governments in Europe affected many European countries' perspectives on data privacy adding to the European political class and citizens' requests for rigorous data protection procedures, particularly for personal data, for example, Nazis through the control of the state and information technology were able to continuously abuse private data to detect Jews or other minority groups.[15] Consequently, Germany was one of the initial nations to implement data privacy regulations as a result of Nazism atrocity and World War II, Germans remain particularly worried about invasions of privacy even on these days.[16]

It is acknowledged that both the transatlantic actors are devoted to protecting individual privacy rights and personal data. Nonetheless, the approaches in the United States and the European Union can result in nuanced differences. Therefore, variances in values and approaches are reflected in the difficulties that the international community has faced.

[11] Monika Zalnieriute, 'Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security' (2022) 55(1) Vanderbilt Journal of Transnational Law 1.
[12] James Q Whitman (n 2) 1160.
[13] Robert C Post, 'Three concepts of privacy' (2001) 89 Geo LJ 2087.
[14] James Q Whitman (n 2).
[15] Olivia B Waxman, 'The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History' (*Time*, 24 May 2018) <https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/> accessed 11 March 2024.
[16] James B Rule and Graham W Greenleaf, *Global privacy protection: the first generation* (Edward Elgar Publishing 2010).

2.2 The European approach

The EU considers privacy and personal data protection to be fundamental rights. Indeed, these rights are included in Article 7 and Article 8 of the European Union's Charter of Fundamental Rights (CFREU)[17], which has binding force on all EU member states by its adoption as primary law in the Treaty of Lisbon in 2009. These rights granted by the Charter, which are comparable to a constitutional right in the United States[18], are based on Art.8 of the European Convention of Human Rights (ECHR).[19] Furthermore, Article 52 of the CFREU states that any restrictions on such rights must adhere to the proportionality principle, while Article 47 guarantees to every European citizen the right to seek judicial redress for any violations.[20] Thus, all the jurisdictions to which the data of European citizens are addressed cannot circumvent those principles that are integral parts of EU law, it must be ensured the protection of personal data, their process according to the principle of proportionality, and a mechanism of redress must be assured for any case of disuse of data. For Europe, the protection of privacy and data protection has always been at the centre of the political agenda since the adoption of the Data Protection Directive and then to the adoption of the General Data Protection Regulation in 2018. As already mentioned, the GDPR created a set of standards directly enforceable and consistent for personal data protection across the EU aiming to protect people's fundamental rights in the digital era. Moreover, Chapter V GDPR linked to the principles enshrined in the CFREU covers the outward dimension of data to guarantee the same level of protection for European data outside the EU.

2.3 The United States approach

Unlike the EU, in the United States there is no federal legislation that controls the acquisition and use of personal data of consumers. However, The U.S. Supreme Court has inferred from the Constitution an individual's right to privacy, with a mainly focus on the protection from government interference, indeed the 4th Amendment encompasses the "search and seizure" provisions which provide that: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"[21] The Amendment derives from

[17] Charter of Fundamental Rights of the European Union 2012/C 326/02 of 26 October 2012 [2012] OJ C326/391.
[18] Emily Linn, 'A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement' (2017) 50 Vanderbilt Journal of Transnational Law 1311.
[19] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14).
[20] Kristin Archick and Rachel F Fefer, 'U.S. – EU Privacy Shield and Transatlantic Data Flows' (2021) Congressional Research Service <https://crsreports.congress.gov/product/pdf/R/R46917> accessed 11 March 2024.
[21] U.S. Constitution., IV amendment.

the notion that each man's home is his castle and that such a 'castle' shall not be violated by any government interference.[22] In addition, in *Katz v. United States*[23] has been acknowledged that the Amendment "protects people, not places," eliminating the requirement of real physical trespass and subjecting electronic surveillance to the Amendment's restrictions, furthermore it was established the so-called expectation of privacy test upon which one may 'justifiably' rely to preserve as private what expected to maintain as such, even in public from the interference of the authorities.[24]

Moreover, the leeway of the federal government has been restricted by The Privacy Act of 1974 which regulates how the federal government handles personal information to guarantee that data held by federal agencies are not disclosed without consent, except for certain exemptions[25], on the other hand, the Electronic Communications Privacy Act of 1986 placed upon governmental officials' restrictions on telephone wiretaps such as electronic data transmission.[26]

Furthermore, since the limitation in the constitution to protect the data of citizens and the lack of a unique federal law that governs data protection several federal laws have been adopted by Congress to give statutory protections for citizens' personal information.[27] Indeed, rather than a single complete comprehensive regulation, the United States adopted in the years a kind of 'patchwork' of federal laws that regulate firms' data protection practices.[28] The United States adopted a specific sectoral approach, trusting on a mixture of legislation, regulation, and self-regulation. These laws vary in scope depending on who is in charge of enforcement and the kind of penalty related to them. Among these laws actually in force in the U.S. are: Children's Online Privacy Protection Act (COPPA); Electronic Communications Privacy Act (ECPA); Health Insurance Portability and Accountability Act (HIPAA); Federal Trade Commission Act (FTC Act) et. all.[29]

Therefore, the type and grade of protection granted to data depends on which sectors the data are processed and which federal law covers that circumstance. As an example, *The U.S. laws protect specialized information, such as health care or financial data, by implementing a data-specific approach to regulating data privacy. In these cases, The*

[22] Cornell Law School, Fourth Amendment, Legal Information Institute, <https://www.law.cornell.edu/constitution/fourth_amendment> accessed 11 March 2024.
[23] *Katz v. United States* 389 U.S. 347 (1967).
[24] Cornell Law School, 'Katz and the Adoption of the Reasonable Expectation of Privacy Test' Legal Information Institute <https://www.law.cornell.edu/constitution-conan/amendment-4/katz-and-the-adoption-of-the-reasonable-expectation-of-privacy-test> accessed 11 March 2024.
[25] The Privacy Act of 1974 (n 7).
[26] Electronic Communications Privacy Act of 1986 <https://www.congress.gov/bill> accessed 11 March 2024.
[27] Stephen P Mulligan and Chris D Linebaugh, 'Data Protection and Privacy Law: An Introduction' (2019) Congressional Research Service <https://crsreports.congress.gov/product/pdf/IF/IF11207> accessed 11 March 2024.
[28] Zachary S Heck, 'A Litigator's Primer on European Union and American Privacy Laws and Regulations' (2018) 44 Litigation 59.
[29] For the full list see note 27.

Federal Trade Commission (FTC) has the authority to pursue enforcement proceedings against corporations that mislead customers about their privacy practices, however, it lacks the authority to enforce comprehensive online privacy standards.[30] On the other hand, other laws apply comparable principles to private businesses. The Stored Communications Act (SCA) which is part of the ECPA, bans internet service providers from unlawfully accessing or disclosing some electronic communications.[31] Moreover, several laws while just not limited to data protection, impose restrictions on the businesses' procedure to manage personal information. As an example, The FTC Act bans misleading procedures that could be carried out by companies.[32]

From the point of view of general regulation for private entities and their practices, it is well-established self-regulation through industry best practices.[33] Indeed, the typical U.S. liberal approach has fostered the self-regulatory regime in order to foster innovation in fast-paced sectors such as artificial intelligence (AI) or e-commerce that base their functioning on the process of consumer data. Such an approach gives businesses the possibility to adapt easily to shifts in technological innovation while assuring a better business-oriented framework, therefore instead of relying on government authority for enforcement, the U.S. model relies on self-policing. Notwithstanding, a part of the public opinion advocates for stronger laws on privacy in the U.S. supporting the view that gaps are present in the actual legal framework.[34]

In conclusion, while the EU views privacy protection as a fundamental human right, the United States views these rights as a commodity, leaving the matter to market forces.[35] The United States employs a risk-based approach in which companies are legally responsible for managing data wherever it is transferred and stored, in opposition we have seen that the EU takes a more rigid compliance-based approach since data is considered embedded in every person, then needing fundamental protection.[36] Therefore, it is understandable that the difficulties in concluding a stable agreement for international transfer result from nuanced differences in histories, cultures, and values between the two transatlantic actors.

[30] Archick and Fefer (n 20).
[31] Charles Doyle, 'Privacy: An Overview of the Electronic Communications Privacy Act' (2012) Congressional Research Service <https://crsreports.congress.gov/product/pdf/R/R41733> accessed 22 March 2024.
[32] Federal Trade Commission Act (1914) 15 U.S.C. §§ 41-58.
[33] Sandeep Mittal, 'Critical Analysis of Divergent Approaches to Protection of Personal Data' (2017) 8(7) International Journal of Advanced Research in Computer Science 58.
[34] Archick and Fefer (n 20).
[35] Stephen J Kobrin, 'Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance' (2004) 30(1) Review of International Studies 111.
[36] Nigel Cory, Daniel Castro and Ellysse Dick, 'Schrems II': What Invalidating the EU-US Privacy Shield Means for Transatlantic Trade and Innovation' (Information Technology and Innovation Foundation, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/> accessed 11 March 2024.

2.4 Failures of previous transatlantic agreements on data transfer

Agreements on Data transfer between the EU and the U.S. have an extended and complex history of common commitments to reach a valuable solution. On one side, the privacy and data protection principles have taken a market-oriented approach in the United States. Instead, as we already analysed the GDPR is based on non-negotiable fundamental rights that must be guaranteed. Nevertheless, the United States considers its differentiate approach depending on the sector of application of privacy regulation was crucial for the success of American technological innovation, not over-regulating the business landscape. Therefore, a brief historical context of the previous agreements is required to comprehend the standoff in which we are today.

2.4.1 The Safe Harbour Agreement and Schrems I

Following the adoption by the European Union of its Data Protection Directive in 1995, the U.S. and the EU started an effort to establish a framework that would allow U.S. firms to fulfil adequate level of data protection required by the directive to avoid interruptions in personal data transfers from the EU.

The negotiation resulted in The Safe Harbour Privacy Principles[37], established by the U.S. Department of Commerce in 2000. The European Commission recognized that U.S. companies that were compliant with these principles would meet EU requirements for transferring personal data outside of the EU.[38] The Safe Harbour agreement, allowed a company or organisation in the United States to voluntarily issue self-certification to the Department of Commerce on a yearly basis to ensure its compliance with the adequacy decision. That would imply the respect of seven basic privacy principles, among which: *notice, choice, onward data transfer, security, data integrity, access, and enforcement, other than related requirements deemed necessary to meet the EU's data protection adequacy standards.*[39]

The FTC implemented the agreement, classifying any infringement of the Safe Harbour Privacy Principles as misleading activity according to Section 5 of the Federal Trade Commission Act banning "*unfair or deceptive acts or practices in or affecting commerce.*"[40] In addition, to ensure that the companies would continue to attain their voluntary self-certification every year they were obliged to re-register with the

[37] U.S. Department of Commerce, Safe Harbor Privacy principles of 21 July 2000, <https://rm.coe.int/16806af271> accessed 11 March 2024.
[38] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and 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 L215/7.
[39] Archick and Fefer (n 20).
[40] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 section 45.

Department of Commerce, which contained a registry of all the organizations compliant with the Safe Harbour.[41]

However, not everyone was pleased with the safeguards put in place. Some Safe Harbour detractors sustained that the deal was simply a "minimalist solution" and that the U.S. never meant to follow on its promise to increase safeguards in the future.[42] Others underlined the FTC's lack of enforcement capabilities, which had not launched an enforcement case until 2009. Therefore, it was argued that these flaws demonstrated the agreement's incapability to guarantee meaningful data protection for EU citizens.[43] Moreover, the Snowden leaks, which encompassed allegations of extensive internet data surveillance by U.S. intelligence authorities, only served as the last step to erode the European Union's confidence in cross-border data exchanges with the U.S. Indeed, the revelations regarding the National Security Agency's (NSA) programs such as PRISM and UPSTREAM had a strong impact on the European Union, encouraging EU data protection law reform while negatively damaging trust in cross-border data flows.[44] The NSA through PRISM had access to sensitive information such as emails, documents, or photos from different American tech companies among which Google, Facebook, Apple, and Microsoft.[45] Moreover, via UPSTREAM the NSA was directly accessing communications made over fiber cables and communication infrastructure, in addition, such surveillance tactics may be implemented without a warrant if the collected data were related to foreigners located on the other side of the Atlantic.[46] Such actions were possible under the Foreign Intelligence Surveillance Act, known as FISA, which focuses on the capabilities of the U.S. government's collection of foreign intelligence data in order to bring forward U.S. counter-intelligence objectives. In particular, Section 702 FISA permits the U.S. authorities to search, collect, and process foreign intelligence data from foreigners situated outside of U.S. territory and jurisdiction without a warrant.[47]

Therefore, under those circumstances in October 2015 a judgment of the European Court of Justice (CJEU) invalidated the Safe Harbour Agreement. The judgment is known as Schrems I.[48] Indeed, the CJEU ruling originated from a complaint filed by an Austrian

[41] Mike Ewing, 'The Perfect Storm: The Safe Harbor and the Directive on Data Protection' (2001) 24 Houston Journal of International Law 315.
[42] W Gregory Voss, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) 19(11) Journal of Internet Law 1.
[43] McKay Cunningham, 'Complying with international data protection law' (2016) 84 U Cin L Rev 421.
[44] ibid.
[45] Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *(The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 11 March 2024.
[46] Craig Timberg, 'NSA Slide Shows Surveillance Of Undersea Cables' (Washington Post, 10 July 2013) <https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html> accessed 11 March 2024.
[47] Peter Margulies, 'Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on US Surveillance Policy' (2015) 72 Washington & Lee Law Review 1283.
[48] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* ECR 650.

law student, Maximillian Schrems, with Ireland's Data Protection Authorities. Schrems complained about Facebook's transfer of his data from its EU-based servers in Ireland to its U.S.-based servers. In light of the 2013 exposures of U.S. NSA surveillance activities, Schrems filed several complaints with Ireland's DPA affirming and claiming that it was not present concrete protection against intelligence surveillance intrusion in US privacy law. Even though Schrems' complaint was dismissed by Ireland's DPA, the Irish High Court sustained his appeal and referred the issue to the CJEU. The court said that before concluding that the Safe Harbour principles guaranteed an adequate level of protection for EU individuals' personal data, the European Commission did not investigate properly into U.S. domestic legislation or international commitments.[49]

In particular, as well noted by Kuner the CJEU found that *Facebook's commercial transfer of personal data to the U.S., followed by further processing by U.S. public authorities for national security purposes, and combined with a lack of mechanisms for E.U. citizens to raise concerns to obtain redress, resulted in Safe Harbour failing to provide essentially equivalent protection as required by EU law in its Data Protection Directive and according to European Union Charter of Fundamental Rights (EUCFR)*.[50] Therefore, permitting U.S. authorities to interfere with personal data of citizen transferred across the Atlantic.

In particular, around 4,500 enterprises and organizations based their practice upon the Safe Harbour framework, therefore an immediate stop to the transfer of data could be disastrous for EU-U.S. economic ties. However, the EU declared a grace period of 4 months during which the outcome of Schrems I was not enforced. Thus, U.S. and EU officials could negotiate a new deal.[51]

2.4.2 The Privacy Shield and Schrems II

In February 2016, the negotiation between the U.S. and the EU gave its outcome, the EU-U.S. Privacy Shield was adopted. The newly established agreement was supposed to guarantee to companies the transfer of EU citizens' personal data to the U.S. while adhering to the requirements listed by the CJEU when it declared Safe Harbour invalid in 2015.[52] However, since the beginning the proposal announced was criticised in the EU, doubts were presented on the capability of the agreement to provide adequate

[49] Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid' (Press release No. 117/15, 6 October 2015) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> accessed 11 March 2024.
[50] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18(4) German Law Journal 881.
[51] Article 29 Working Party, 'Statement of the Article 29 Working Party' Press Release, 16 October 2015 <https://ec.europa.eu/justice/article-29/press-material/press release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 11 March 2024.
[52] Martin A Weiss and Kristin Archick, 'US-EU data privacy: from safe harbor to privacy shield' (2016) Congressional Research Service <https://sgp.fas.org/crs/misc/R44257.pdf> accessed 11 March 2024.

protection for EU data subjects, adding that if these issues were not resolved prior to the Privacy Shield's implementation, the agreement could be challenged in front of the CJEU.[53] Nevertheless, the Privacy Shield agreement included commitment from U.S. officials in the form of letters that U.S. government access to EU citizens' personal data would be limited, as well as redress mechanisms such as the establishment of a Ombudsman at the U.S. Department of State to receive complaints from EU citizens in case of misuse of their data by U.S. national security authorities.[54] In July 2016 the Privacy Shield entered into force after the grant of an adequacy decision by the Commission with the hope that it would constitute a reliable compliance framework to transfer personal data for commercial purposes across the Atlantic. The adoption of the adequacy decision on behalf of the Commission was accompanied by the conviction on both sides that Privacy Shield had much greater privacy protections and oversight mechanisms than Safe Harbour, other than containing several redress options and enhanced safeguards relating to U.S. government access to personal data. However, questions still remained whether the agreement would survive future legal challenges in front of the CJEU.

The Privacy Shield basic structure was comparable to the one of the Safe Harbour; it was built on principles derived from EU data protection law that corporations can voluntarily self-certify to, and whose compliance is monitored by the Federal Trade Commission and Department of Transportation.[55] Nevertheless, the Privacy Shield is more complex and structured than the Safe Harbour agreement. Indeed, the Privacy Shield required the respect of seven primary principles namely: (1) *notice to provide transparency to individuals; (2) choice allowing individuals to opt out; (3) accountability for onward data transfer when data is sent to a third party; (4) security to protect data collected, (5) data integrity and purpose limitation for personal data collection, (6) access of individuals to personal data collected Recourse, (7) enforcement and liability for compliance. In addition, the framework included 16 supplemental principles creating different obligations for the companies to comply with.*[56] While participation in the Privacy Shield framework was on voluntary basis, when a company joined the framework, it was obliged to comply with the principles embedded in it.

[53] Article 29 Data Protection Working Party, 'Opinion 1/2016 on the EU-US Privacy Shield Draft Adequacy Decision' <https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2016/wp238_en.pdf> accessed 11 March 2024.
[54] European Commission, 'EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield' (Press Release, 2 February 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216> accessed 11 March 2024.
[55] Article 29 Data Protection Working Party (n 53).
[56] EU-US Privacy Shield Framework <https://www.privacyshield.gov/eu-us-framework> accessed 11 March 2024.

Moreover, an annual joint evaluation of the program could be conducted by the European Commission and the Department of Commerce, with experts from U.S. national intelligence authorities and European DPAs.[57]

Moreover, every European citizen had a variety of redress options under the Privacy Shield. Individuals could file complaints directly to companies or EU DPAs, which could submit unresolved concerns to the FTC. If the FTC declines to pursue a claim, Privacy Shield provided claimants with a free alternative dispute resolution mechanism. Indeed, a Privacy Shield Ombudsman was created to handle complaints about possible access and exploitation of EU citizens' personal data by U.S. national intelligence authorities. Although the Ombudsman was independent from the intelligence agencies, he is authorized to investigate matters referred by EU DPAs.[58]

Therefore, the Privacy shield at first instance assured more protection of the data of European citizens under many aspects, offering diverse means of redress and stronger data protection mechanisms. However, such efforts were not considered appropriate and sufficient to offer an adequate level of protection to European data in the United States territory. Indeed, a closer analysis of the new system reveals no significant upgrading in effective administrative and judicial redress for data subjects that have their data transferred.[59] In Schrems II, the CJEU broadly followed the pattern that used in Schrems I, indicating that a corporation to undertake business in the EU had to ensure adequate protection of data under EU law even when the data is transferred.[60] As a consequence, the Privacy shield after just four years into force has been invalidated by the CJEU judgment, known as Schrems II.

Since the CJEU's Schrems I decision invalidating Safe Harbour in 2015, Facebook Ireland announced that it was transferring most of its data to its U.S. servers via standard contractual clauses (SCCs), according to article 46 GDPR. SCCs are standard contract provisions that the EU 'pre-approve' to ensure that data transferred is protected according to EU standards. Therefore, Maximillian Schrems brought a new claim with Ireland's Data Protection Authority, inquiring the capabilities of SCCs to provide an adequate level of data protection, given the fact that U.S. surveillance laws could grant U.S. authorities access to personal data transferred to Facebook servers in the U.S. The case was brought to the High Court of Ireland, which then submitted doubts regarding the legitimacy of SCCs to the CJEU.[61]

[57] 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 L207/1.
[58] European Commission, 'Guide to the EU-U.S. Privacy Shield' (2016) <https://ec.europa.eu/newsroom/just/items/605819> accessed 11 March 2024.
[59] Elaine Fahey and Fabien Terpan, 'Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield' (2021) 28 Indiana Journal of Global Legal Studies 205.
[60] Case C-311/18 *Maximillian Schrems v. Data Protection Commissioner* ECR 559, para 186.
[61] Xavier Tracol, '"Schrems II": The return of the privacy shield' (2020) 39 Computer Law & Security Review 1.

In the judgment issued in July 2020, although Advocate General Saugmandsgaard Øe suggested that the legal validity of the Privacy Shield was not needed of evaluation and ruled upon, the CJEU believed otherwise.[62] The Court considered the legality of the Privacy Shield decision in light of the GDPR's requirements, as well as Article 7 of the Charter's right to respect for private life, Article 8 of the Charter's right to personal data protection, and Article 47 of the Charter's right to effective judicial protection.[63] The two main takeaways have been: that the Privacy Shield framework could not be considered valid for transferring personal data from the EU to the U.S. given the breadth of data collection powers authorised in U.S. electronic surveillance laws and the lack of redress options for EU citizens. Indeed, the Ombudsman did not offer any guarantee of its independence from the executive, nor its capabilities to adopt decisions that are binding on U.S. intelligence agencies. It follows that the adoption of President Barack Obama's Presidential Policy Directive No. 28 (PPD-28)[64] which aimed to place limits upon U.S. surveillance powers was not instrumental to reassure the European counterparts. Indeed, the European Court sustained that the U.S. framework was lacking both an independent check on U.S. surveillance practices and sufficient and specific limits on surveillance's scope.[65]

The CJEU found in particular that Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow intelligence services to gather more information than is strictly necessary, allow the collecting of more information not respecting the principle of proportionality enshrined in European law.[66]

The Grand Chamber's decision had sweeping practical repercussions. Indeed, a research conducted by the International Association of Privacy Professionals showed how SCCs were used by 88 percent of enterprises that transfer personal data outside of the EU, while the Privacy Shield was used by 60 percent.[67] Indeed, over 5,300 firms used the Privacy Shield standard for transatlantic data transfers, including digital giants Google, Facebook, Amazon, and Twitter.[68]

The invalidation of the Privacy Shield and the doubts about the legitimacy of the SCC brought confusion among businesses that formerly relied on it. Therefore, a new

[62] Case C-311/18 *Maximillian Schrems v. Data Protection Commissioner* ECR 559, Opinion of AG Saugmandsgaard Øe, paras 174-186.
[63] Xavier Tracol (n 61).
[64] The White House, Presidential Policy Directive/PPD-28, Signals Intelligence Activities, (Office of the Press Secretary 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> accessed 11 March 2024.
[65] *Maximillian Schrems v. Data Protection Commissioner* (n 62) paras 183-184.
[66] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 184.
[67] IAPP-EY, Annual Governance Report (2019) <https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2019.pdf> accessed 11 March 2024.
[68] William A Reinsch and Isabella Frymoyer, 'Transatlantic Data Flows: Permanently Broken or Temporarily Fractured?' (Center for Strategic And International Studies 2020) <https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured> accessed 11 March 2024.

adequacy decision on behalf of the Commission was needed to resolve the situation permanently.

3 An Analysis Of United States Surveillance Law

The U.S. and the EU addressed the concerns raised by the CJEU in Schrems II. In order for the U.S. government to produce an effective and long-term solution, it was required to bring changes to its surveillance ecosystem in the U.S. In order to strike a balance between national security and privacy in order to be able to achieve an adequate level of protection regarding the processing of personal data in the U.S.[69]

As already noticed, the CJEU held in the Schrems II judgment that U.S. surveillance activities carried out under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333) do not provide "the minimum safeguards" necessary under EU law to fulfil the proportionality principle. The European judges concluded that surveillance carried out under such statutes "*cannot be regarded as limited to what is strictly necessary.*"[70] Therefore, the court strongly underlined the necessity of effective safeguards against disproportionate government access to European data as well as judicial redress.

Before examining U.S. surveillance law it is important to remember, as underlined in the previous section, that the two systems adopted different kinds of regulations with different interference capabilities according to their view of privacy as an aspect of dignity in the EU and privacy as an aspect of liberty in the U.S.

Firstly, in the discussion on the balance between national security and privacy, it's often supposed that the U.S. finds a balance in favour of national security, whilst the EU takes a more strict approach that prioritises the protection of civil liberties, as the privacy of the individuals.[71] Secondly, despite historical disagreements over privacy, EU-U.S. intelligence sharing and counter-terrorism cooperation were strengthened in the aftermath of 9/11[72], effectively putting EU privacy advocates on the backburner. However, the tendency to foster such cooperation and to side-lining privacy advocates has been halted with Snowden's revelations. Indeed, the balance between national security and privacy in Europe has shifted since then, and the political pendulum in Europe has swung back in favour of privacy activists.[73] Finally, the presence of mass surveillance programs does not constitute novel practices by itself. What is remarkable

[69] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2017) 56(4) Journal of Common Market Studies 751.
[70] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 184.
[71] Francesca Bignami, 'European versus American liberty: A comparative privacy analysis of antiterrorism data mining' (2007) 48 BC L Rev 609.
[72] Davor Jančić, 'The role of the European Parliament and the US Congress in shaping transatlantic relations: TTIP, NSA surveillance, and CIA renditions' (2016) 54(4) Journal of Common Market Studies 896.
[73] ibid.

and unparalleled today respect to the past is the extent and the degree of capability of U.S. electronic foreign intelligence practices thanks to technological improvements. As a result, a rigorous examination of the extent of current surveillance capabilities, and the explanations they draw and the debates they cause is urgently required.[74] Therefore, we might conclude that modern U.S. surveillance law is out of step with the current demands of civil society regarding civil liberties.

We are going to analyse the most relevant U.S. case law on the balance between national security and privacy; then we will revert our attention to the most relevant U.S. surveillance laws. In order to be able to say which are the laws that put at stake the long-standing functioning of a transatlantic data pact.

3.1 Case law as basis for the wide scope of U.S. foreign surveillance law

Although courts have enabled reforms in certain cases, their rulings in the subject matter are often a source of transatlantic divergence, since they constitute the legal basis on which the governments construct their legal framework and policies. In particular, in this section, we are going to analyse the U.S. cases on which the U.S. administrations have developed their surveillance policies.

When balancing national security and privacy, the United States legal frameworks guarantee protections under the Fourth Amendment which impose restrictions on the government regarding surveillance practices or wiretaps. However, the strictness of these rules differs depending on which sector the U.S. authorities are acting such as for law enforcement, that encompasses crimes and offenses, or for national security.[75]

The case of Olmstead v United States (1928) sparked the first controversy about the relationship between electronic surveillance and Fourth Amendment rights. The Court concluded in this decision that intercepting telephone communications did not constitute a search or seizure within the meaning of the Fourth Amendment since it did not require a physical trespass onto a person's property.[76] The Court's decision stimulated heated controversy since it allowed non-trespassory forms of electronic surveillance.[77] In other instances, such as Goldman v United States[78] (1942) and Lee v United States[79] (1952), the contradicting 'trespass doctrine' was confirmed, establishing

[74] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker, 'After Snowden: Rethinking the impact of surveillance' (2014) 8(2) International political sociology 121.
[75] Peter Swire, 'US Surveillance Law, Safe Harbor, and Reforms Since 2013' (2015) 36 Georgia Tech Scheller College of Business Research Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709619>.
[76] *Olmstead v. United States* 277 U.S. 438 (1928).
[77] L Rush Atkinson, 'The Fourth Amendment's national security exception: its history and limits' (2013) 66(5) Vanderbilt Law Review 1343.
[78] *Goldman v. United States* 316 US 129 (1942).
[79] *Lee v. United States* 343 US 747 (1952).

for several decades the legal standard for surveillance activities at the cost of personal privacy.

As briefly cited in the previous section, in Katz v United States (1967) for the first time the Supreme Court overturned the trespass doctrine, finding that "*because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure*."[80] It was also ruled that any intrusion, also electronic, into a location in which a person detains a reasonable expectation of privacy might be an infringement of the Fourth Amendment.[81] Furthermore, FBI activities such as wiretapping was deemed 'unreasonable' since it was carried out lacking a lawful warrant.[82] As a result, in Katz a privacy-based approach to the Fourth Amendment was approved.[83]

However, it is important to take notice that the Court at the same time established the so-called 'national security exception doctrine' in footnote 23 by stating that "*whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security is a question not presented by this case*." Therefore, the U.S. government according to Atkinson welcomed such provision in the Katz case as a "judicial blessing of the national security exception" which detained an important influence on the construction of future surveillance practices.[84]

Moreover, the matter of controlling national security surveillance was eventually addressed in United States v United States District Court (1972), widely known as the 'Keith' case, in which the question of whether a warrant was required to access electronic communications for reasons of national security was addressed. While the government claimed that "*the surveillance was lawful, [even] though conducted without prior judicial approval, as a reasonable exercise of the President's power to protect national security*"[85], the Court ruled that the governmental surveillance activities for domestic national security goals could be carried only when complying with the warrant requirement. However, it was not expressly answered whether the warrant provision extended to cases involving foreign intelligence surveillance.

As a result, the District Court in Keith not only reaffirmed the existence of the national security exception doctrine, additionally, it demonstrated that there was a distinct difference between foreign security surveillance that remained under the control of the Executive, therefore free from oversight, and domestic security

[80] *Katz v. United States* (n 23) para 351.
[81] ibid para 361.
[82] ibid para 363.
[83] Paul J Larkin, 'The Fourth Amendment and New Technologies' (The Heritage Foundation 2013) <https://www.heritage.org/report/the-fourth-amendment-and-new-technologies> accessed 11 March 2024.
[84] L Rush Atkinson (n 77) 1380.
[85] *United States v. United States Dist. Ct.* 407 US 297 (1972).

surveillance that was subject to Fourth Amendment restrictions protecting the right to privacy.[86]

In addition, in United States v Truong Dinh Hung (1980), the U.S. Court of Appeals for the Fourth Circuit recognized the 'national security exception doctrine' for the first time. The Court agreed with the government that there is a foreign intelligence exception to the warrant requirement, emphasising that "*the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following Keith, "unduly frustrate" the President in carrying out his foreign affairs responsibilities.*"[87]

The judgments discussed above demonstrate that the U.S. courts often agreed and approved a national-security approach to the Fourth Amendment. It makes apparent that the Fourth Amendment rests upon a two-layer system that distinguishes between internal and foreign security surveillance. As a result, it treats U.S. and non-US citizens differently. Finally, privacy guarantees and safeguards for U.S. citizens may result limited.[88]

Therefore, on such stances, the U.S. government could adopt laws that allow them to intrude on the private sphere of foreign citizens, and that constitute the major reason for which an adequacy decision cannot be granted by the European Commission to the U.S. legal framework.

3.2 United States foreign surveillance law: section 702 FISA and Executive Order 12333

Understanding of the CJEU's approach in Schrems II requires a closer examination of U.S. foreign surveillance with a focus on Section 702 of FISA and EO 12333. The former and the latter are the two statutes through which the government conducts signal intelligence surveillance activities. The NSA outlines signals intelligence, or SIGINT, as "*intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.*"[89] Therefore, giving a broad leeway of action to U.S. authorities in their surveillance activities. In addition, the legal framework governing intelligence operations in the United States has not been updated to consider new technological realities, there are even larger loopholes that expose

[86] Elizabeth Goitein and Faiza Patel, 'What Went Wrong with the FISA Court?' (Brennan Center for Justice 2015) <https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court> accessed 11 March 2024.
[87] *United States of America, Appellee, v. Truong Dinh Hung, Appellant. United States of America, Appellee, v. Ronald Louis Humphrey, Appellant*, US Court of Appeals for the Fourth Circuit - 629 F.2d 908 (1980).
[88] Francesca Bignami, 'The US legal system on data protection in the field of law enforcement Safeguards, rights and remedies for EU citizens' (2015) Study for the LIBE Committee, GWU Law School Public Law Research Paper No. 2015-54, GWU Legal Studies Research Paper No. 2015-54.
[89] National Security Agency, Signals Intelligence (SIGINT) Overview <https://www.nsa.gov/Signals-Intelligence/Overview/> accessed 11 March 2024.

Europeans and even U.S citizens to surveillance and leave them unprotected from a legal standpoint. Therefore, U.S. surveillance law put at stake the sustainment of a stable international data transfer agreement, while raising doubt on the protection of the rights and privacy of their own citizens.[90]

3.2.1 The Foreign Intelligence Surveillance Act (FISA): section 702

The Foreign Intelligence Surveillance Act (FISA) was adopted in 1978 in the aftermath of the 1970s surveillance scandals, among which was the Watergate affair.[91] It provides the legal basis for modern US foreign intelligence activities and programs. The FISA was enacted as a result of comprehensive Senate Committee investigations into the legality of domestic intelligence activities. The goal was to guarantee better protection of civil liberties by building up a barrier between intelligence collection and enforcement.[92] In addition, FISA created a special court known as the Foreign Intelligence Surveillance Court (FISC) which would have the role to approve or refuse orders enabling electronic surveillance of specific targets.[93]

Furthermore, the terrorist attacks of September 11th, 2001 drove national security at the top of the U.S. government's priority list, resulting in an overwhelming majority vote in favour of the adoption of the US Patriot Act.[94] The latter significantly changed FISA. It gave federal law enforcement and intelligence agencies greater capability to collect and exchange evidence obtained through wire and electronic surveillance.[95] Moreover, in 2008 the FISA Amendments Act, which comprehends the "infamous" section 702, allowed the collection of communications by foreign persons that utilise U.S. communications service providers. Originally FISA was created to regulate surveillance activities targeting individuals within the United States. Section 702 was intended to extend such capabilities for the acquisition of intelligence information on non-US citizens residing outside the U.S. but without guaranteeing the safeguards provided by U.S. law, which are only relevant to U.S. citizens under the original FISA.

Section 702 has been at the centre of criticism since it provides the legal foundation for NSA surveillance techniques by allowing the agency to target freely the communications of foreign targets, without a warrant for national security purposes.

[90] Axel Arnbak and Sharon Goldberg, 'Loopholes for circumventing the constitution: Unrestricted bulk surveillance on Americans by collecting network traffic abroad' (2015) 21(2) Michigan Telecommunications & Technology Law Review 317.
[91] Francesca Bignami (n 71) 617.
[92] Robert N Davis, 'Striking the Balance: National Security vs. Civil Liberties' (2003) 29(1) Brooklyn Journal of International Law 175.
[93] Laura L Donohue, 'Bulk metadata collection: Statutory and constitutional considerations' (2014) 37(3) Harvard Journal of Law & Public Policy 757.
[94] USA Patriot Act of 2001, Public Law 107–56 of 26 October 2001, 107th Congress.
[95] Charles Doyle, 'The USA Patriot Act: a legal Analysis' (Congressional Research Service 2002) <https://crsreports.congress.gov/product/pdf/RS/RS21203> accessed 11 March 2024.

Unlike conventional FISA requests, which require a specific court order, 702 just requires the FISC to approve a singular annual government certification affirming that its procedures for obtaining and processing information are in accordance with the statute.[96] It is thus reaffirmed that U.S. surveillance law does not treat U.S. and non-US citizens in the same manner.

Section 702 has been enacted with the scope of codifying different aspects of the Terrorist Surveillance Program (TSP), which was established outside of the FISA framework by President Bush in 2001, in the section there are a locational and a substantive element.[97] The executive detains the capabilities of targeting communications of people or companies "reasonably believed to be located outside the United States" under Section 702. Mobile phone numbers and email addresses are selected to collect such communications. Moreover, to be lawful targets for surveillance activities does not suffice just to be located abroad, indeed United States persons, encompassing both U.S. citizens and foreigners with a lawful permanent residency (LPRs) located outside U.S. territory, are not targetable. However, there are included 'one-end foreign communications' which allow targeting a communication where there is at least one foreigner, also if the other part is within the United States territory, a U.S. citizen, or an LPR.[98]

Consequently, the targeting of foreign persons and companies under Section 702 results in the accidental gathering of enormous volumes of data on U.S. citizens.[99] Both the NSA, and other national agencies, among which the FBI, send requests to the database, which can provide results about people in the United States.[100]

Officials in the United States may target such communications in order to gather foreign intelligence information. Section 702 defines *foreign intelligence information as any information on attacks on the United States, espionage, sabotage, international terrorism, or the proliferation of weapons of mass destruction. Additionally, it includes a more nebulous category related to information of foreign power or foreign territory linked to the conduct of the foreign affairs of the United States.*[101] The category 'foreign affairs' in particular shows that 702's targets might cover a wide range of instances and subjects.

It appears logical to assume that to handle the extensive coverage under section 702 the U.S. employs automated technologies such as machine learning to detect trends

[96] Robert Stein, Walter Mondale, and Caitlinrose Fisher, 'No longer a neutral magistrate: The foreign intelligence surveillance court in the wake of the war on terror' (2015) 100 Minnesota Law Review 2251.
[97] Neal Katyal and Richard Caplan, 'The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent' (2008) 60 Stanford Law Review 101.
[98] Emily Berman, 'When Database Queries Are Fourth Amendment Searches' (2017) 102 Minnesota Law Review 577.
[99] *United States v. Hasbajrami* 945 F.3d 641 (2d Cir. 2019), paras 661-62.
[100] Peter Margulies, 'Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law' (2021) 104(4) Marquette Law Review 1155.
[101] USA Patriot Act of 2001 (n 94).

in the storm of digital information accessible globally.[102] AI approaches and in particular machine learning may employ deep-learning neural networks that allow to swiftly filter through various variables in large volumes of data.[103] Thus, the employment of such technologies is of real concern for the protection of people that can be targeted under such wide capabilities on behalf of U.S. authorities.

Indeed, despite their many advantages, machine learning models have several flaws. Some models may be trained on incomplete or improperly selected data, for example, can generate fragile decisions that ignore context. Indeed, such naive models pay too much attention to insignificant changes in inputs, which any normal human being would appropriately disregard. In the training of machine learning, even minor modifications might result in significant output changes.[104] Furthermore, due to the large number of variables that neural networks process, frequently ambiguous outcomes can be produced that transcend standard linguistic explanations.[105] Another issue in machine learning that is particularly relevant for surveillance practices is the inherent risk that automated techniques may reflect human biases.[106] As an example, there may be fewer photos of individuals of color in a data set used to "train" an AI model in face recognition, or the data set may not represent the entire diversity of facial features across the globe.[107] Therefore, because of the scale of U.S. monitoring, machine learning's flaws are particularly notable and demand our attention on both sides of the Atlantic. As cited above, the targeting of foreign persons under Section 702 leads to the acquisition of vast amounts of data. Lastly, while the targeting process under Section 702 can be subject of independent review, the extent of that review is restricted given the circumscribed annual approval by the FISC.

Therefore, critics of Section 702 in Schrems II focused on the following: first, a lack of constraints on the capabilities conferred to implement surveillance programs, and second, the lack of guarantees and redress mechanisms for non-US persons who might be the target of those programs.[108]

3.2.2 Executive Order 12333 and PPD-28

While FISA primarily covers surveillance activities implemented within the territory of the United States, another statute through which U.S. authorities conduct electronic

[102] Peter Margulies, 'Surveillance by algorithm: The NSA Computerized Intelligence Collection, and Human Rights' (2016) 68(4) Florida Law Review 1045.
[103] Ian H Witten and Eibe Frank, *Data mining: practical machine learning tools and techniques* (Elsevier 2005).
[104] Bita Darvish Rouani, Mohammad Samragh, Tara Javidi and Farinaz Koushanfar, 'Safe machine learning and defeating adversarial attacks' (2019) 17(2) IEEE Security & Privacy 31.
[105] David Lehr and Paul Ohm, 'Playing with the data: what legal scholars should learn about machine learning' (2017) 51 UCDL Rev 653.
[106] Ashley Deeks, 'High-tech international law' (2020) 88 The George Washington Law Review 574.
[107] Aziz Z Huq, 'Constitutional Rights in the Machine-Learning State' (2020) 105 Cornell Law Review 1875.
[108] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 180.

surveillance abroad is Executive Order (EO) 12333, which was enacted in 1981 by President Reagan.

Executive orders are directives issued by the President of the United States. Executive orders are usually intended to govern activities of Government officials and agencies, not private citizens. The authority of the President to issue executive orders is derived from statutes and Article II of the Constitution.[109]

Therefore, surveillance policies governed by EO 12333 are solely designed and implemented by the executive. EO 12333 grants the NSA capabilities to gather, store, analyse, and disseminate foreign signals intelligence information.[110]

Indeed, the types of information that may be gathered under EO 12333 are broader. Under section 702 information that can be collected is limited to the 'foreign intelligence information'. Therefore, as analysed by the Privacy and Civil Liberties Oversight Boards (PCLOB), such restrictions do not allow the unrestricted collection of information about foreigners under section 702 FISA.[111] In contrast, under EO 12333 the categories that limit the types of information that the government may collect on U.S. citizens do not apply to non-US citizens. Therefore, no explicit constraints are present.

EO 12333 is structured in three sections. The first sets the goals of US intelligence and allocates tasks and duties to the Intelligence Communities (IC)[112] constituent agencies. Part 2 of the Order describes the necessity for foreign intelligence information and sets out standards to strike a balance with the safeguards of the rights of U.S. citizens. It requires IC to implement specific measures for collecting, retaining, and disseminating information about US citizens, as well as the use of precise collection techniques, however not including non-US citizens. Part 3 discusses oversight and guides intelligence agencies on the implementation of the Order, defining the terms contained in the statute.[113]

Furthermore, EO 12333 governs internet surveillance when it is carried on foreign soil and does not fall within the definition of electronic surveillance as set out in FISA in 1978. According to the NSA, EO 12333 applies when surveillance is conducted

[109] John Contrubis, 'Executive Orders and proclamations' (Congressional Research Service 1999) <https://sgp.fas.org/crs/misc/95-772.pdf> accessed 11 March 2024.

[110] National Security Agency, Missions, Authorities, Oversight and Partnerships of 9 August 2013 <https://irp.fas.org/nsa/nsa-story.pdf> accessed 11 March 2024.

[111] Privacy and Civil Liberties Oversight Board (PCLOB), 'Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' of 23 January 2014 <https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf> accessed 11 March 2024.

[112] The United States Intelligence Community (IC) is a federation of executive branch agencies and organizations that work together and individually to perform intelligence activities required for the conduct of foreign relations and the protection of the country's national security. For more detailed information about the composition of U.S.IC see 'Members of the IC' (Office of the Director of National Intelligence) <https://www.dni.gov/index.php/what-we-do/members-of-the-ic> accessed 11 March 2024.

[113] Privacy and Civil Liberties Oversight Board (PCLOB), 'Executive Order 12333' (Report 2021) <https://documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12333%20Public%20Capstone.pdf> accessed 11 March 2024.

with different means around the world, mainly outside of the United States, when it does not fall within the scope of FISA.[114] Unlike FISA, EO 12333 surveillance does not rely on the cooperation of service providers. The technical details remain classified and opaque, but the NSA has revealed that at least it involves exploiting flaws in telecommunications infrastructure.[115] Another point of friction is the capabilities to conduct bulk collection under the Order. Bulk collection entails conducting surveillance without a specific target or other discriminants. According to the National Research Council it is a collection "*in which a significant portion of the retained data pertains to identifiers that are not targets at the time of collection.*"[116] Such kind of activity cannot be carried under section 702 FISA. However, foreign intelligence collection under EO 12333 allows the U.S. government to gather signals intelligence in bulk collection when it is deemed essential in consideration to "technical or operational considerations."[117]

Since the bulk collection is by definition conducted without any discriminants, there is a great risk that the government will even obtain lots of information about people who have no relationship to wrongdoing or foreign intelligence information. Therefore, the U.S. government was pushed to put in place strong protections to limit these dangers, since EO 12333 was issued as an executive order the executive branch could do such without Congressional action.[118]

Concerns regarding the volume and nature of intelligence collection under E.O. 12333 prompted President Obama to issue Presidential Policy Directive 28 (PPD-28) in January 2014. The latter has been the first public commitment of the US government to protect the privacy of non-US citizens. PPD-28 discusses the safeguards to be provided to non-US citizens in the context of U.S. signals intelligence programs.[119] The directive states that: "*signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.*"[120] Therefore, the PPD-28 goal was to articulate principles to determine why, whether, when, and how the United States may perform lawful foreign intelligence

[114] ibid.
[115] Richard Lawne, 'US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM' (Fieldfisher 2020) <https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups> accessed 11 March 2024.
[116] National Research Council of the National Academies, 'Bulk Collection of Signals Intelligence: Technical Option' (2015) 2-9 <https://www.nap.edu/read/19414/chapter/1#vii> accessed 11 March 2024.
[117] Presidential Policy Directive (n 64).
[118] Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman and Spandana Singh, 'Strengthening Safeguards After Schrems II: A Roadmap for Reform' (*New America*, 7 April 2021) <https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/> accessed 11 March 2024.
[119] Daniel Severson, 'American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Change' (2015) 56(2) Harvard International Law Journal 465.
[120] PPD-28 (n 65).

and counterintelligence activities. In particular, the directive considers the safeguards to be provided to non-US citizens. However, despite its lofty language, PPD-28 purported reforms essentially just formalize and incentivize already existing practices inside the U.S. Intelligence Community, with significant policy changes occurring only on the margins, ensuring that the IC continues to detain sufficient authority to maintain the status quo.[121]

Indeed, on one hand, PPD-28 limits the use of data collected from bulk monitoring to six designated purposes: *(1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cybersecurity; (5) U.S. or ally armed forces; and (6) transnational criminal acts*.[122] On the other hand, it just restricts the use of the data gathered in bulk, not the purposes for which data is collected in bulk. In practice, intelligence agencies can continue to collect large amounts of data for any foreign intelligence objective, and PPD-28 simply limits how the government can use the data once it is stored in official databases. Therefore, it does not resolve the issue of data collected about persons not linked with any of the foreign intelligence objectives.[123]

According to the U.S. government, PPD-28 constituted a significant safeguard for non-U.S. citizens' civil liberties.[124] However, the CJEU considered PPD-28's safeguards insufficient, because the NSA has withheld its power to gather bulk intelligence signals without a clear and specific target.[125] Such safeguards are deemed insufficient to protect European citizens against the bulk collection of data by U.S. authorities under EO 12333. Consequently, the CJEU's position is confirmed, U.S. bulk collection is not necessary, nor proportionate, and, neither Section 702 nor EO 12333 provides individual data subjects with a means to seek redress against U.S. authorities for surveillance abuses.[126] Therefore, the main reason for the failure of the previous transatlantic data agreement has been shown clearly.

4 Towards A Stable Digital Economy Or Unfolding A New Chapter In The Schrems Saga?

On 10 July 2023, the EU issued its adequacy decision based on the Data Privacy Framework (DPF) negotiated with the United States, constituting an important step

[121] Richard Lawne (n 115).
[122] PPD-28 (n 65) section 2.
[123] Privacy and Civil Liberties Oversight Board (PCLOB) (n 111).
[124] Alexander W Joel, 'The Truth About Executive Order 12333' (*Politico*, 18 August 2014). <https://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121/> accessed 11 March 2024.
[125] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 183.
[126] ibid paras 181-184.

forward for the appropriate functioning of the digital economy.[127] Following the analysis conducted above, the new agreement, like its predecessors, will almost certainly be brought in front of the EU judicial system where will face the scrutiny of European Judges. The disposition in the new agreement was negotiated to meet the EU's standards requirement set out in Schrems II namely:

- Ensuring that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate according to article 8 CFREU to pass the proportionality test enshrined in article 52 CFREU;[128]
- The independence of the new redress mechanism respects the European individuals' right to an effective remedy and to a fair trial, and, whether any new authority part of this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services as required by article 47 CFREU;[129]
- Lastly, if a judicial remedy against this authority's decisions or inaction is present.[130]

Now let's analyse how the new agreement tackled the issues at stake. In the wake of extensive collaboration between the US and the EU, an agreement in principle was reached in 2022, reflecting a shared commitment to facilitating data flows while protecting individual rights and personal data.[131] The subsequent Executive Order signed by President Biden and accompanying Regulations set the stage for significant improvements with respect to the Privacy Shield.

Executive Order 14086 introduces binding safeguards delineating stringent limitations on US intelligence authorities' access to EU data, aligning with the necessity and proportionality standards articulated by the CJEU. In particular, the DPF restricts U.S. signals intelligence capabilities towards 12 'legitimate objectives'. In addition, the establishment of the Data Protection Review Court (DPRC), as an independent and binding authority, enhances the redress mechanism, addressing the CJEU's concerns regarding the lack of effective remedies.[132] Indeed, the creation of the DPRC answers to

[127] European Commission, 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows' (Press release 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/eN/ip_23_3721> accessed 11 March 2024.
[128] *Maximillian Schrems v. Data Protection Commissioner* (n 62).
[129] ibid.
[130] ibid.
[131] The White House, 'Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement' (Press statement, 25 March 2022) <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/> accessed 11 March 2024.
[132] US Department of State, 'Executive Order 14086 – Policy and Procedures' (3 July 2023) <https://www.state.gov/executive-order-14086-policy-and-procedures/> accessed 11 March 2024.

the two-holding made in Schrems II bringing a new structure to provide redress in response to a complaint from an individual in a qualifying state. Now every European citizen has at his disposal a two-tiered redress mechanism. In the first tier, it is possible to lodge a complaint with the 'Civil Liberties Protection Officer' of the US intelligence community. In the second tier, EU individuals are able to challenge that decision to the newly created DPRC.[133]

The commission explained how the new court differentiates from the ombudsman present in the Privacy Shield.[134] It ensures that the members of the DPCR are selected outside of the U.S. government, are appointed on the basis of qualifications, and are independent of instruction of the government.[135] Moreover, the DPCR in the mandate to investigate complaints of EU individuals will be fully able to obtain relevant information from intelligence agencies and capable to issue remedial decisions. Therefore, it appears that the new DCPR structure, while taking a decision upon a challenge of a European citizen, is able to meet the relevant EU legal requirements for independence and effectiveness.

The European Commission, taking these developments into account, moved forward with the adoption of the DPF adequacy decision in July 2023.[136] This decision allows for the transfer of personal data from the EU to the U.S. through a certification system. U.S. companies committing to privacy principles can facilitate data flows without additional mechanisms like Standard Contractual Clauses. The DPF constitutes a step forward, ensuring safe data flows, legal certainty, and strengthening economic ties.

However, concerns persist about how the court will work in practice. Questions remain about how the US interprets "proportionate" access to data, the transparency of the DPRC, and the framework's effectiveness in addressing alternative avenues of data access.

In particular, one of the main concerns still remains Section 702 FISA and debate of its reform that is undergoing in the U.S., indeed the FISA was expected to expire at the end of 2023. As suggested by a study by the Center for Strategic & International Studies: "*FISA reform could help the United States shift away from its global reputation as a*

[133] Théodore Christakis, Kenneth Propp and Peter Swire 'The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC' (IAPP 11 October 2022) <https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/> accessed 11 March 2024.

[134] European Commission 'Question and answers: EU-US Data Privacy Framework' (2022) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045> accessed 11 March 2024.

[135] For the list of judges nominated see here: US Department of Justice 'Attorney General Merrick B Garland Announces Judges of the Data Protection Review Court' (14 November 2023) <https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court>.

[136] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023] C/2023/4745.

"digital Wild West" and move toward shared global leadership on privacy and civil liberties."[137] They suggested to Congress to consider codifying privacy safeguards already present in the DPF in a renewed version of the FISA.[138] However, for the moment the validity of FISA was merely extended to April 2024,[139] whether the Act will be modified or not will be an important point of interest for the Commission for the annual review of the DPF.

However, it is also important to point out the recent case law of the CJEU on matters of surveillance, bulk collection, and data retention. In the past years, the CJEU shifted its approach regarding matters of surveillance capabilities on behalf of public authorities. From a first wave of fierce opposition to surveillance practices – with cases such as Digital Rights Ireland[140], the Schrems Saga, and Privacy International[141] – to a more pragmatic and procedural approach to surveillance practice.[142] In particular in La Quadrature du Net[143] the CJEU shifted from a strict approach banning completely surveillance practice to a more nuanced approach setting a list of lawful data retention practices that can be undertaken by national authorities.[144]

Therefore, the recent case law suggests that the CJEU may detain a less restrictive approach to the scrutiny of possible challenges to the DPF regarding U.S. surveillance capabilities.

For the moment Max Schrems contends that the DPF bears resemblance to its predecessors, indicating a potential legal challenge akin to 'Schrems III', that would probably reach the CJEU by Early 2024.[145] The European Data Protection Board (EDPB)[146] and the European Parliament (EP)[147] have also expressed reservations, emphasizing

[137] Caitlin Chin-Rothmann, 'Reforming Section 702 of the Foreign Intelligence Surveillance Act for a Digital Landscape' (Center for Strategic & International Studies 2023) <https://www.csis.org/analysis/reforming-section-702-foreign-intelligence-surveillance-act-digital-landscape> accessed 11 March 2024.
[138] ibid.
[139] Barbara Calderini, 'Gli Usa rinnovano la sorveglianza globale, ecco perché ci preoccupa' (Agenda Digitale, 29 December 2023) <https://www.agendadigitale.eu/sicurezza/privacy/usa-sinfiamma-il-dibattito-sulla-sorveglianza-dopo-la-proroga-delle-norme-antiterrorismo/> accessed 11 March 2024.
[140] Joined Cases 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* ECR 238.
[141] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* [2020] OJ C 433.
[142] Maria Tzanou and Karyda Spyridoula, 'Privacy international and quadrature du Net: One step forward two steps back in the data retention saga?' (2022) 28 (1) European Public Law 123.
[143] Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and others v Prime Minister and others* ECR 791.
[144] Tzanou and Spyridoula (n 142).
[145] 'European Commission Gives EU-US Data Transfers Third Round at CJEU' (NOYB 10 July 2023) <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> accessed 11 March 2024.
[146] European Data Protection Board 'EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain' (28 February 2023) <https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en> accessed 11 March 2024.
[147] European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-U.S. Data Privacy Framework (2023/2501(RSP)) [2023] OJ C/2023/1073.

concerns about the adequacy of safeguards and the potential for legal invalidation by the CJEU. The Parliament points out that: "*the EU-U.S. Data Privacy Framework fails to create essential equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU*".[148]

Therefore, despite the progress the path to a stable transatlantic data transfer framework remains complex. The Commission continuously monitors development in the US and will conduct its first review in July 2024. It will be a first watershed moment in order to understand how the agreement worked in practice and to grasp future implications.

While privacy concerns are valid, drawing premature conclusions might be counterproductive. A 'Schrems III' scenario, with another legal battle in front of the European Court of Justice, would only come with more uncertainty for EU individuals. While we navigate this evolving landscape, cautious optimism and a keen eye on the Commission's upcoming review seem prudent.

In this paper, we aimed to offer an understanding of past legal precedents, coupled with a forward-looking perspective, which will be crucial in determining whether the DPF heralds a stable digital economy or unfurls a new chapter in the Schrems saga.

5 Conclusions

The evolution of EU-U.S. data transfer agreements shows a continuous struggle to reconcile disparate perspectives on privacy and data protection. The new Transatlantic Data Privacy Framework demonstrates an effort to bridge the transatlantic privacy divide. It offers a potential solution to the challenges posed by the previous diatribes. Therefore, it was beneficial to reflect on the lessons learned from the failures of its predecessors.

The historical differences in privacy approaches between the EU and the U.S. are rooted in distinct legal frameworks and cultural nuances. Those differences have underscored the complexity of achieving a long-term transatlantic data transfer mechanism. The Privacy Shield and its predecessor, Safe Harbour, faced important challenges due to divergent surveillance laws and insufficient safeguards against U.S. intelligence intrusions, leading to their eventual failure.

The concerns raised by the Court of Justice of the EU in the Schrems II case highlighted the need for robust safeguards against government surveillance, sparking

[148] ibid point 19 of the resolution.

renewed negotiations and the development of the Transatlantic Data Privacy Framework. The framework, ushered by Executive Order 14086 and accompanying regulations, introduces binding safeguards and establishes a Data Protection Review Court to address privacy complaints.

However, the journey towards a stable and reliable transatlantic data transfer mechanism is far from over. Despite the improvements brought by the new framework, uncertainties persist. Questions surrounding the interpretation of "proportionate" access to data by U.S. authorities, the composition of the Data Protection Review Court, and the framework's ability to address data accessed through alternative avenues remain unresolved.

Privacy activist Max Schrems and others argue that the new framework echoes the shortcomings of its predecessors and falls short of instigating substantial changes in U.S. surveillance law. The concerns expressed by the EDPB and the European Parliament further underscore the need for vigilance.

The successful implementation and longevity of the Transatlantic Data Privacy Framework hinge on its ability to withstand legal scrutiny and address the core issues that brought down previous agreements. The recent nuanced approach of the CJEU on matters of data retention on behalf of public authorities may end up playing an important role in the matter.

The July 2024 review by the European Commission will serve as a pivotal moment to assess the framework's efficacy and adherence to EU legal standards.

With the looming possibility of a 'Schrems III', it remains imperative for both sides of the Atlantic to bear in mind the previous difficulties. Indeed, the quest for a durable and reliable transatlantic data transfer framework remains a work in progress, requiring persistent collaboration, mutual understanding, transparency, and a strong commitment to safeguarding the privacy rights of individuals on both sides of the Atlantic. Additionally, the actual international geological scenario reminds us that the Transatlantic partnership must be fostered in the midst of a future of uncertainty. Only through such efforts we pave the way for a safe and prosperous digital economy.