LUNDS UNIVERSITET
EKONOMI-
HÖGSKOLAN

GDPR Compliance in EU-US Data Transfers

Examining the impact of the EU Commission's 2023 adequacy decision on surveillance risks

Linda Kidwell

INSTITUTIONEN FÖR HANDELSRÄTT

Affärsjuridisk kandidatuppsats

15 högskolepoäng

HARH13

HT 2023

Abstract

International data transfers serve to support the global economy, facilitating international collaboration and economic expansion. However this increased productivity comes at a cost, namely amplified personal data privacy and security risks. In an era dominated by rapid technological advancements, the clandestine actions of intelligence agencies have the potential to infringe upon the privacy and integrity of individuals on a near global scale. The revelations of mass surveillance programs, as exposed by whistleblowers like Edward Snowden in the United States, demonstrate the real risks of mass data collection to individuals. Consequently, public debate and concern has escalated pertaining to the contentious balance between national security protective measures and the preservation of human rights and civil liberties.

The EU Commission's 2023 adequacy decision determined that the United States provided an essentially equivalent level of protection for European personal data. This decision follows the development of the EU-US Data Privacy Framework and has significant implications, as it permits European entities to transfer personal data directly to US companies participating in the framework. As a result, European businesses can conduct data transfers to their US counterparts without the necessity of additional protective measures, streamlining the exchange of personal data and facilitating collaboration in the modern digital economy. However, the high risk of personal data access by US state intelligence agencies makes this practice fraught with complications pertaining GDPR. This raises questions about how to achieve suitable balance between encouraging the free flow of information and protecting data privacy as well as about the validity of the EU Commission’s 2023 adequacy decision.

Table of Contents

Abbreviations

ACLU	American Civil Liberties Union
AD	Adequacy Decision
BCR	Binding corporate rules
CFR	The Charter of Fundamental Rights of the European Union
DPF	Data Privacy Framework
DPIA	data protection impact assessment
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EEG	European Essential Guarantees
EO	Executive Order
EU	European Union
FEU	The Treaty on European Union
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance court
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
NSA	National security agency
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
SCC	Standard contractual clauses
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
US	United States

1 Introduction

1.1 Background

When the European Commission issues an adequacy decision, it effectively recognizes that data can be transferred from the EU[1] to the specified third country without the need for additional data protection measures, such as standard contractual clauses or binding corporate rules.[2] By granting an adequacy decision the EU Commission declares the third country's own data protection law and practices are of an essentially equivalent,[3] although not necessarily identical, standard as those applicable within the EU. The GDPR[4] establishes the rules and conditions which must be met before an adequacy decision can be granted and used as a legal mechanism for personal data transfers to third countries from the EU. The most recent adequacy decision granted by the EU Commission has been issued due to President Biden's Executive Order 14086[5] and the EU-US Data Privacy Framework on account of the updated framework's inclusion of augmented regulations protecting European data subjects[6] from surveillance measures by US agencies and the implementation of a new redress mechanisms, and the introduction of the principles of necessity and proportionality.[7] However US law governing covert surveillance, the Foreign Intelligence Surveillance Act,[8] provides a legal basis for US intelligence agencies to conduct vast personal data processing operations in conflict with the GDPR. Case law by the Court of Justice of the European Union, particularly Schrems I[9] and Schrems II,[10] provide important context as to the challenge of practical implementation of the GDPR.

The relevance of this academic investigation is to safeguard democratic European values by examining the extent to which the privacy and security of personal data[11] subject to the GDPR may be compromised. Scrutinizing covert surveillance practices conducted by US intelligence agencies is relevant to the examination of contemporary European data protection legislation as it illuminates deficiencies in the execution of the GDPR abroad and addresses fundamental conflicts related to personal data protection and international data flows. Covert operations of intelligence agencies pose a threat with global reach to individuals' right to privacy and integrity in the current landscape of rapid technological evolution. The United States government, however, has made material efforts to align its data protection

[1] Territorial references to the European Union (EU) henceforth apply also to the EEA countries: Norway Iceland and Liechtenstein.
[2] Article 46 EU Regulation 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 (GDPR).
[3] Recital 104 GDPR.
[4] General Data Protection Regulation.
[5] Executive Order 14086 On Enhancing Safeguards For United States Signals Intelligence Activities.
[6] Article 4(1) GDPR.
[7] Executive Order 14086 Section 2(a).
[8] The Foreign Intelligence Surveillance Act.
[9] CJEU C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015 (Schrems I).
[10] CJEU C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 2020 (Schrems II).
[11] Article 4(1) GDPR.

practices with EU standards yet questions remain about the effectiveness of the new transfer framework.

1.2 Purpose and research questions

This purpose of this thesis is to describe and critically analyze the EU commission's 2023 adequacy decision, with specific concentration on the updated provisions mitigating the risk of US state intelligence agencies from conducting unlawful and disproportionate surveillance measures on European data subjects in breach of the GDPR. A thorough examination of the EU Commission's adequacy decision and the practical implications of the EU-US Data Privacy Framework is needed. To achieve the purpose of this thesis the following research questions will be investigated.

How does the EU-US Data Privacy Framework, serving as the basis for the 2023 Adequacy decision, address concerns related to the insufficient protection of European individuals' personal data from surveillance activities conducted by U.S. intelligence organizations?

Do the provisions regarding surveillance in the EU Commission's 2023 adequacy decision sufficiently align with the requirements outlined in the GDPR?

1.3 Method and material

This thesis is written with the EU legal method in combination with the traditional legal dogmatic method. The EU legal method is meant to be used when interpreting European legal sources including EU primary case law established by the CJEU, and international agreements to which the EU is party. The impact of the EU laws and institutions are particularly significant in the field of data protection, both on the EU member-state level, as well as internationally.[12] This method is therefore relevant to answering the research questions posed in this essay as CJEU cases, primarily Schrems I and Schrems II, are examined supporting this evaluation of the current state of European data protective legislation abroad in the US. The traditional dogmatic method involves investigating the solution to a legal problem by interpreting a rule of law to illustrate its present-day application. First, the legal problem is posited followed by an analysis of the applicable doctrine through which the legal solution may be determined.[13] As this thesis investigates the problems arising from the conflict between protection European data subjects from unlawful data processing by US government intelligence agencies on the dynamically evolving legal grounds, the traditional dogmatic method is used to clarify the state of legal data protection at this moment in time.

To achieve the purpose of this investigation, a variety of European legal sources are analyzed. This includes case law from the Court of Justice of the European Union, primarily Schrems I and Schrems II, which were chosen as they are the famous,

[12] Hettne, J., & Eriksson, I. O. (2011). *EU-rättslig Metod: Teori och genomslag I svensk rättstillämpning*. Stockholm: Norstedts juridik.

[13] Jareborg, N. *Rättsdogmatik som vetenskap*. SvJT. Svensk Juristtidning, 2004.

landmark cases, demonstrating the complexities of unifying data subject rights afforded by the GDPR with US national security (surveillance) practices.

The European Data Protection Board constitutes the European Commission's primary advisor on data protection matters, including third country adequacy assessments. The EU Commission's past decisions are consistently reviewed as the EDPB is tasked with ensuring the consistent application of the GDPR where it has jurisdiction.[14] With the creation of the GDPR, the board suceeded and expanded the work of its predecessor, the Article 29 Working Party,[15] with increased scope and authority. Therefore, the Article 29 Working Party and EDPB opinions and recommendations serve as primary guidelines instructing the correct application of the GDPR and are used as primary sources for this essay.

Then the General Data Protection Regulation with its binding regulatory status, is included as a focal point of this essay. The GDPR is unique in that it has extraterritorial authority in connection with the processing of Europeans' personal data.[16] This regulation's relevance lies in its strict standards and authority over cross border personal data transfers. The GDPR demands transparency and protection of individuals' rights, influencing how US entities process Europeans' personal data.[17] It is therefore crucial to consider when addressing the challenges with the application of European personal data protective interests in the US.

Then it is necessary to acknowledge EU primary law[18] as these treaties establish the legal framework followed by the EU institutions and reign over the national laws of the union's member states. The EU primary law consists of the EU general legal principles, the Treaty of the European Union, The Treaty of the Functioning of the European Union as well as the EU Charter of Fundamental rights. These are typically considered to be the EU's constitution as they may not be modified by European Institutions, only by new contracts between the member states. The Charter's rights provide more extensive protections for individuals, building on the Convention for the Protection of Human Rights and Fundamental Freedoms.[19] The meaning of the data protection principles is derived, in large part, from the GDPR and the EU Charter of Fundamental Rights, originating from Convention 108.[20] The GDPR extends and specifies these individual rights by safeguarding Europeans privacy rights even outside of the EU in the field of personal data protective legislation.

The European Commission's adequacy decision 2023[21] is used as a primary source in this essay. The EU-US Data Privacy Framework provides a modernized set of requirements for this legal transfer mechanism method while the AD justifies the use of this transfer mechanism and substantiates the conditions met by the US

[14] Article 70 GDPR.
[15] Article 29 EU Data Protection Directive 95/46/EC.
[16] Article 3 GDPR.
[17] Article 4(1) GDPR.
[18] EU Charter of fundamental rights (The Charter); Treaty on European Union (TEU); Treaty on the Functioning of the European Union (TFEU).
[19] Lundberg, K. et al. (2019). *Juridik: civilrätt, straffrätt, processrätt* 5th ed. Stockholm, Sweden: Sanoma Utbildning AB, 50.
[20] Recital 105 GDPR.
[21] EU Commission Implementing Decision of 10.7.2023 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) (Adequacy Decision).

government in achieving the adequacy status with their newly implemented data protective safeguards. This framework facilitates the secure transfer of European personal data to US entities which is of focal relevance to this essay.

1.4 Outline

The structure of this thesis is organized to ensure an accessible flow of information. The introduction provides necessary background information and formulates the purpose and research questions that will be answered in the exploratory text and the analysis of the EU Commission's 2023 adequacy decision as well as providing an explanation for the sources used and research methods chosen for this text.

The second section examines the rules and conditions governing the adequacy decision legal mechanism as a basis for transfer to third countries, exploring this particularly tumultuous legal landscape in the present day. CJEU case law is examined, primarily the Schrems I and Schrems II landmark cases, which delve into the state of European personal data protection in the United States. Relevant human rights laws in the context of data protection are also recognized along with the potential risks to individuals when those rights are breached. Alternative data transfer mechanisms are additionally discussed. The Snowden scandal revealing mass surveillance programs employed by covert US intelligence operations is mentioned here to provide constructive context for the underlying substantive claims behind Schrems II. The legal principles of necessity[22] and proportionality[23] are thereafter deliberated as these principles are newly introduced to US surveillance law under the EU-US DPF and highly relevant to the posed research questions.

The third section examines the most recent adequacy decision from the EU Commission and the Executive Order 14086 together with the EU-US Data Privacy Framework. The most relevant aspects of these new developments for the protection of European data subject rights abroad in the US include the creation of the new redress mechanism, the data protection review court, and essential updates to the rules for US intelligence agencies regulating their surveillance activities of non-US persons. The ways in which the EU-US DPF addresses the European data subject privacy concerns resulting from Schrems II specifically related to covert intelligence operations is evaluated along with the legal basis for the EU Commission’s adequacy decision. The lawful basis for US state agencies to process European personal data is reviewed followed by a discussion of the conflict between US national security legislation and the GDPR. This section provides an understanding of the legal and organizational landscape of data privacy with regard to third country data transfers between the EU and the US.

Finally this thesis culminates with the key findings, discussion of the legal implications, and the conclusions made in response to the posed research question. This structure aims to contribute to an accessible understanding of the central theme: proportionality and the current state of data protection for European data subjects

[22]Article 5(1)(c) and article 6(1) GDPR.
[23]Article 6(3-4) and recital 4 GDPR.

under the EU-US Data Privacy Framework against the backdrop of covert surveillance activities by US state intelligence agencies.

2 Adequacy decisions as a basis for third country data transfers

2.1 Introduction – The concept of adequacy

One of the legal bases provided by the GDPR include the adequacy decision[24] transfer mechanism. This decision signifies that the European Commission has determined that the third country (outside the EU) provides adequate personal data safeguards that are commensurate with the protection provided within the European Union itself. Broader laws or vague principles concerning data protection by the third country are insufficient to meet the criteria. Specific and enforceable legal frameworks must be in place for an adequacy decision to be considered. The third country must then commit to upholding relevant EU regulations, typically by joining international agreements or by the development of national legislation. When these mandatory conditions are met, an adequacy decision may be reached. In essence, adequacy decisions represent the conclusive endorsement by the EU Commission allowing for the transfer of personal data beyond EU borders without the need for additional approval from other regulators.[25] Subsequent implementation of an adequacy decision allows personal data to be transferred from any of the twenty-eight EU member states and the three EEA member countries to third countries.[26]

2.2 Rules and conditions governing adequacy as a transfer mechanism

The EU Commission must consider several criteria when deciding which countries may be granted adequacy, including the level of collaboration between the EU's current or potential industry connections with the third country in question. Free trade agreements or ongoing negotiations are considered as well as the shared values and political relationship with the EU in the international community. The quantity of personal data flowing from the EU to the third country is also a consideration.[27] Recognition of fundamental freedoms and human rights are taken strongly into account along with relevant national legislation. An analysis is performed of the third country's government access to personal data and the national practice of compliance with data protection rules and in the context of that country's national security legislation.[28] Additionally, supervisory authorities must be existing and functional in the third country, effectively enforcing compliance with data protection rules along with maintaining an advisory role to support data subjects exercising their rights and

[24] Adequacy decisions are currently issued under article 45 of the General Data Protection Regulation (2016/679) and were issued previously with reference to article 25 of the Data Protection Directive (95/46/EC).
[25] EU Commission press release. *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows* (2023).
[26] Article 45(1) GDPR.
[27] EU Commission press release. *Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers* (2017).
[28] Article 45(2)(a) GDPR.

cooperating with the supervisory authorities from the EU as needed.[29] Finally an evaluation is performed of any relevant international commitments previously made by the third country and the rule of law under which the data transfer is set to occur.[30] Essentially, it is crucial to first examine the substance of existing rules and subsequently assess the effectiveness of the mechanisms in place to ensure proper application of data protection safeguards.[31] It is crucial that the protection of personal data remains robust despite its movement.

One way in which the EDPB aids the European Commission[32] is by investigating and producing reports regarding the quality of data protection to be found in the legal framework of third countries. Recommendations from the EDPB support the EU Commission's work but ultimately, the responsibility of observing ongoing developments that have the potential to impact the legal basis of an adequacy decision remains with the EU Commission.[33] If the third country in question does not reach adequacy, other transfer mechanisms are available.[34] Regardless of which transfer mechanism is used, upholding an adequate level of data protection is paramount. Such decisions are not permanent but must be evaluated on a continuous basis to ensure validity, at minimum every four years. The right to adjust, suspend, or revoke a current adequacy decision remains a possibility held by the European Commission.[35] Although should one of those measures be employed, the EU Commission is obligated to initially seek an opinion on the matter from the EDPB.[36] Maintaining adequacy with a third country requires abundant and continuous collaboration between the EU Commission and third party state actors. As such, strong partnerships and the harmonization of data protections standards may be achieved.

2.2.1 Alternative data transfer mechanisms

When navigating international data transfers, additional data protection safeguards are required for US organizations that have not joined the EU-US Data Privacy Framework.[37] For entities that have not affiliated themselves with the EU-US DPF, additional measures such as standard contractual clauses,[38] binding corporate rules,[39] codes of conduct;[40] certification mechanisms;[41] or *ad hoc* contractual clauses may be implemented instead.[42] These alternative instruments contain the appropriate safeguards that may be utilized when an adequacy decision is not applicable.[43]

Standard contractual clauses are binding agreements that have been approved by the European Commission as a legal data transfer mechanism, as such, they may not be

[29] Article 45(2)(b) GDPR.
[30] Article 45(2)(c) GDPR.
[31] Article 29 Working Party Adequacy Referential, 2017 WP 254.
[32] Article 70(1) GDPR.
[33] Article 45(4) GDPR.
[34] Article 45 GDPR.
[35] Article 45(5) GDPR.
[36] Article 70(1)(s) GDPR.
[37] Article 46(1) GDPR.
[38] Article 46(2)(c-d) and article 93(2) GDPR.
[39] Article 46(2)(b) and article 47 GDPR.
[40] Article 40, 41 and 46(2)(e) GDPR.
[41] Articles 42(2) and 46(f) GDPR.
[42] Article 46(2)(b-c) GDPR.
[43] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

changed in any way by the entities who use them. SCCs provide minimum safeguards for data controllers and processors to adhere to, however, business entities may add additional protection measures as long as they dont undermine the original requirements.[44] Employing SCCs is advantageous as they are streamlined for convenient use while ensuring GDPR compliance by participants. SCCs are commonly used and advantageous as they are simplified and established to the point that negotiating specific contractual terms is unnecessary (unlike the BCR transfer method). Ad hoc contractual clauses[45] require additional effort before being used as these are customized clauses developed to meet the unique needs of data processors and controllers within and outside of the EU. Such contracts are subject to approval by a national supervisory authority but do not have the authority to bind third country governments so using this instrument requires careful analysis of the impact of the condition of data protection legislation in that third country, as demonstrated by the Schrems II case.[46]

Binding corporate rules are similar to SCCs but are used for data transfers between groups of already joined businesses or entities. This method ensures that regardless of which country some of the business entities may be established, the data protection measures required by GDPR are equally fulfilled by all. Before implementation, the BCRs must be individually developed to cover the relevant needs of the business and authorized by a competent supervisory authority.[47] BCRs must contain all the crucial data subject rights and required principles under European data protection legislation.[48] They are used to demonstrate corporate accountability and their successful implementation can save the business both time and money when international personal data transfers can be streamlined in this manner.

Codes of conduct[49] can be created by organizations that represent groups of data controllers or processors, often from a particular industry. Such codes may be created to provide additional industry specific guidelines or further developed as a personal data transfer mechanism.[50] Such instruments can be used by entities both within and outside of the EEA and must be both legally binding and enforceable. However, before an entity in a third country can join the code, they must demonstrate sufficiently high levels of data protection practices to qualify.[51] The development of codes of conduct would be a positive phenomenon as it would increase the consistency of GDPR application across industries.

Data protection certification mechanisms are promoted by supervisory authorities subject to the GDPR.[52] Certification is encouraged but not mandatory as it serves to increase transparency practices to the benefit of the data subjects.[53] Businesses would also benefit from being certified as supervisory authorities would take it into account

[44] Recital 109 GDPR.
[45] Article 46(3)(a) GDPR.
[46] Schrems II para 132.
[47] Article 47(1) GDPR.
[48] Recital 110 GDPR.
[49] EDPS Guidelines 04/2021 on Codes of Conduct as tools for transfers.
[50] Article 40(2-3) GDPR.
[51] EDPS Guidelines 04/2021.
[52] Article 42(1) GDPR.
[53] Recital 100 GDPR.

in the context of evaluating possible sanctions in the occurrence of a data breach, certification serves as a tool for accountability. Notably, this transfer mechanism is only valid for personal data transfers from the country in the EU which issued the certification.[54] Using this instrument requires an analysis of the third country's relevant data protection practices and necessitates authorization by a national supervisory authority or by the EDPB.[55]

In terms of the possibility of US state surveillance, these transfer methods under article 49 GDPR are less susceptible when the data transfer is direct. This risk emerges when EU personal data is hosted by US electronic communication service providers because US surveillance legislation too lacks geographical limitations. This means that even if the data center hosting the European personal data is geographically located within the EU, as long as the US company has "possession, custody, and control," then they are forced to provide requested information and to do so confidentially under current US legislative practice.

The final option for international data transfers in the case where an adequacy decision is nonexistent and required safeguards are absent can sometimes be made on the basis of derogations.[56] A derogation can be applied when an exception is permitted under the GDPR such as when data processing is necessary for the fullfillment of a contract[57] or for a reason of suffiient public interest.[58] This option may be exercised when the data subject has been sufficiently informed of any risks connected to the measure and when they have specifically consented to the transfer.[59]

Lacking an adequacy decision,[60] personal data transfers may only be made to third countries when the data controllers or processors have maintained such satisfactory protective safeguards.[61] The protective measures outlined above, governing the transfers subject to appropriate safeguards, are meant to be interpreted against the background of the fundamental rights of the Charter.[62] All of these alternative data transfer mechanisms importantly contribute towards increased harmonization of the application of GDPR in practice. Regardless of which measure is chosen, the personal data is meant to experience a level of protection that is essentially equivalent across the board.[63] Each data transfer mechanism from the EU to international organizations or third countries must not undermine the protection guaranteed by the GDPR.[64] On the other hand, if the personal data is transferred into the EU from abroad, while the majority of the GDPR will apply, the rules of chapter V specifically governing third country data transfers, will not.

[54] EDPB Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.
[55] Article 42(5) GDPR.
[56] Article 49 GDPR.
[57] Article 49(1)(b) GDPR.
[58] Article 49(1)(d) GDPR.
[59] Article 49(1)(a) GDPR.
[60] Article 45(3) GDPR.
[61] Article 46(1) GDPR.
[62] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[63] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[64] Recital 101 GDPR.

2.2.2 The human right to privacy

The human right to privacy is a fundamental principle established in European primary law, protecting individuals from unwarranted intrusions into their personal lives. The commanding data protection legal principles are derived, in large part, from the GDPR and the Charter, itself originating from Convention 108.[65] Among these core freedoms are the right to respect for private and family life, home, and communications[66] and the protection of personal data. In the European Union it is thus established that personal data must be processed in a lawful, fair, and legitimate way and only for specified purposes.[67] Personal data should be maintained to ensure its accuracy when appropriate and must also not be collected excessively in relation to the purpose of the processing.[68] The storage of personal data is not permitted for longer than is necessary to fulfill the lawful purpose for which the data was originally collected.[69] Organizations handling personal data must ensure that it is processed safely and securely as protection from unauthorized processing, accidental loss or damage, is indispensable. Appropriate technical and organizational measures are required to fulfill this principle and maintain the necessary levels of security and confidentiality.[70] Data subjects are to be informed when their personal data is processed in a transparent manner. This information must be easily accessible and include the identity of the data controller and the purpose of the personal data processing along with any other relevant information to ensure fairness in processing.[71]

The right to respect for private and family life, the home, and correspondence is further protected by article 8 of the European Convention on Human Rights. Nevertheless, exceptions to these data subject rights may at times be applied under certain conditions such as in the context of safeguarding national security or preventing criminal activity.[72] The Convention 108, which has been ratified by over fifty countries, remains the only instrument that is a binding and universally accepted international agreement addressing data protection.[73] An illustrative example of data processing that may or may not infringe on the right to privacy is in a situation where automated decision making activities occur, such as credit scoring systems to determine mortgage eligibility based on personal financial data or automated resume tools that screen out job applications based on predetermined criteria. Such data processing measures certainly would increase speed and efficiency for the business carrying out these tasks, but such measures could also easily result in discrimination or unlawful profiling depending on the pre-decided specifications to the processing. Automated decision making based on personal data processing may affect data subject rights and is therefore only allowed under certain circumstances according to the GDPR.[74] Such cases where automated decision making may be permitted is when the automated decision is necessary for the performance of a contract or when

[65] Recital 105 GDPR.
[66] Article 7 Charter.
[67] Article 8 Charter and article 5(1)(a) GDPR.
[68] Article 6(3-4) and Recital 4 GDPR, and *proportionality principle.*
[69] Article 5(1)(e) GDPR and *principle of storage limitation.*
[70] Article 5(1)(f) GDPR and *security and confidentiality principle*.
[71] Article 8(2) Charter; Article 5(1)(a) GDPR and *the principle of transparency*.
[72] Article 23 GDPR.
[73] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[74] Article 22(1) GDPR.

a data subject has provided their explicit consent.[75] However in the context of third country data transfers, if the required conditions are not found in the relevant legal framework abroad, then the data subject would retain their right not to be subjected to an automated decision.

Albeit the right to privacy is not absolute as established by current legislation[76] and case law,[77] These freedoms are meant to be marginally flexible to evolve with the changes brought about by the advances of modern society. Any limitation to these fundamental rights, however, must be lawful and respect the essence of fundamental rights.[78] In the context of data protection, data subjects must also be able to understand and predict how a measure limiting these rights would apply to them.[79] In the context of state surveillance, this requirement of foreseeability may be met by legislation sufficiently clarified that citizens may understand the conditions under which state authorities can lawfully employ surveillance activities.[80] The ECtHR have additionally decided that if the legal foundation is unclear and if the data protection safeguards are lacking, state surveillance would not be considered lawful and would constitute instead a violation of the right to privacy provided by article 8(2) of the Convention. Under those circumstances state surveillance would be considered unlawful regardless of whether the surveillance could be argued to have a proportionate measure and legitimate purpose.[81]

The Charter, meanwhile, permits the establishment of more extensive protections than what it outlines as the fundamental rights it encompasses provide a baseline of "minimum protections."[82] Navigating the limitations to these rights to privacy and personal data is a delicate balance as any limitations to these rights must be lawful, necessary, and proportional.[83] Further, it is crucial that any limitations of these rights may under no circumstances undermine the fundamental essence of these freedoms.[84] By upholding these principles, trust may be facilitated between individuals and their governments and other entities. Insufficient personal data protection measures pose the risk of unauthorized access which could lead to potential for identity theft, financial fraud, or other forms of personal violation. On the other hand, overly stringent measures could impede legitimate use of personal data which would hinder technological advancements and economic activity. Balancing effective protection with responsible use is imperative to mitigate these risks.

2.3 Necessity and proportionality principles

When a new data processing measure is being considered, particularly acts that pose significant risks to the rights and freedoms of natural persons such as secret surveillance, the data controller must conduct a data protection impact assessment

[75] Article 22(2) GDPR.
[76] Article 8(2) ECHR; Recital 4 GDPR; Article 9 of Convention 108.
[77] CJEU joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Hartmut Eifert* para 73.
[78] CJEU joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, para 137-154.
[79] Recital 41 GDPR and ECtHR case, *Zakharov v Russia*, para 229.
[80] ECtHR *Big Brother Watch and others v United Kingdom*, 2018, para 306.
[81] ECtHR case, *Benedik v. Slovenia*, para. 132.
[82] Article 52(3) Charter.
[83] Article 6 GDPR.
[84] Article 52(1) Charter.

before the processing takes place.[85] Determining the necessity and proportionality of the personal data processing in relation to the rights of the data subjects is key. To uphold the principle of necessity, data processing should be evaluated to have a specific, legitimate purpose.[86] The principle of proportionality is also well established in European law, meaning that data processing must be relevant and limited to what is necessary in relation to the purposes for the data processing.[87] Ultimately in the context of data protection this means that the data processing must not exceed what is necessary and must be deemed appropriate under its individual circumstances. The concept of proportionality applied to personal data has been considered by some as one of the most significant advancements in European data privacy law in the last decade.[88]

2.3.1 Necessity testing before data transfers

To fortify the principle of necessity, organizations are encouraged to be transparent with how they go about implementing it. In the context of mass data collection, this could mean developing data privacy policies that clearly state the exceptions permitted and the applicable regulations.[89] Necessity testing is particularly relevant to conduct before sending personal data by relying on appropriate safeguards or to countries without a steadfast adequacy status.[90]

Before conducting the proportionality test, an assessment of the necessity of the proposed data processing measure must be conducted on an objective basis. Necessity refers to the evaluation of the measure and the legitimacy. The evaluation must be made to appraise whether the data processing will be effective to reach the goal or purpose while also being a less intrusive method than other potential options.[91] If the intended data processing passes the necessity test, the proportionality[92] of the data processing must be subsequently assessed.[93]

2.3.2 Proportionality testing before data transfers

The GDPR proportionality test builds on the requirements of the Charter specifying the limitations of art 7 and 8. *"Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."*[94] When conducting these tests consideration must be given to the balance between the various competing interests. The CJEU stressed that this balancing act must assess proportionality on a case-by-case basis, in concreto.[95] The balancing test is key to assessing proportionality and involves weighing the harm of the data processing against the significance and legitimacy of its intended purpose. When

[85] Article 35(1) and (3) GDPR.
[86] Article 5(1)(c)GDPR.
[87] Article 52(1) Charter; Article 5(4) TEU; Article 6(3-4) and recital 4 GDPR.
[88] Lee A. Bygrave, Data Privacy Law. An International Perspective, Oxford University Press, 2014, page 147
[89] Adequacy Decision para 5.
[90] Article 49 GDPR.
[91] Article 5(1)(c) and Article 6(1)(c) GDPR; *principle of data minimization*.
[92] Article 6(3-4) and Recital 4 GDPR.
[93] Article 35(7)(b) GDPR.
[94] Article 52(1) Charter.
[95] CJEU Case C-101/01, *Lindqvist*, 2003 para 89.

conducting a proportionality test it is also important to consider which previously existing measures may be potentially employed to reach the same outcome for the stated goal.[96] In instances where an EU national court determines that a member country's national law is not compatible with article 8 of the ECHR, the CJEU has upheld that under those conditions, that legislation cannot meet the mandate of proportionality.[97]

When carrying out a proportionality test, a review of the potential risks involved with the data processing, mitigating factors, and the sufficiency of protective safeguards are examined. To uphold this principle, the benefits derived from the data processing must outweigh the potential harm inflicted on data subjects in relation to their fundamental rights. Careful balance stricto sensu must be achieved between the means of data processing and the intended goal. The final step involves assessing any factors that may be mitigated in the interest of the data subjects. This includes proposing potential technical and organizational safeguards, which, when implemented, could render the modified data processing measures proportionate. The revised personal data processing measure should embody a fair balance.[98] Examples of safeguards could include human verification, added restrictions to personal data access and encryption among others.

Periodic reassessments are essential to reevaluate the impact on data subjects This means revisiting the necessity and proportionality tests to ensure that the measures remain aligned with the evolving context and requirements, post factum.[99] When conducting these tests in relation to proposed surveillance measures it is crucial to assess how intrusive the data collection is. Surveiling authorities must weigh the impact on the private lives of both the targeted individuals as well as third parties whose private lives may also face intrusion; a concept known as collateral intrusion. Surveillance involving collateral intrusion raises significant concerns. While there might be a legitimate reason to monitor an individual, the broader question arises regarding the privacy of everyone that person interacts with and is an important consideration when conducting balancing or proportionality tests. In the Digital Rights case,[100] the CJEU judged that when dealing with interferences of fundamental rights, the legislator's power is limited. In this case, the CJEU emphasized that minimum protective safeguards must be provided to protect against the risk of abuse and unlawful access.[101]

In sum, proportionality testing under current EU law must first have a legitimate aim for the proposed measure. Secondly, the chosen measure must be suitable to achieve the specified aim. The processing must also be deemed necessary meaning that there is no less intrusive alternative available to achieve the same purpose. Furthermore, the measure must be reasonable and take into account the competing interests of

[96] Article 29 Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 2014 p 9.
[97] CJEU Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof* 2003 para 91.
[98] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data p 12-13.
[99] Article 29 Working Party, Working document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
[100] CJEU Case C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, 2014.
[101] CJEU Case C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, 2014 para 47-54.

different actors involved. Performing this testing should not only be done in accordance with the GDPR, but it is also imperative to thoroughly create document throughout the process to demonstrate compliance. If possible, this documentation should be made public to ensure accountability and transparency.

2.4 Landmark legal precedence

2.4.1 Schrems I and Safe Harbour

The Safe Harbor framework, once a novel mechanism facilitating EU-US data transfers, was contested by the Schrems I case,[102] challenging its adequacy in protecting European data subjects' privacy rights. In light of the Snowden scandal, Austrian citizen, Max Schrems brought the case against Facebook as he was concerned that US intelligence agencies had the ability to access his and other's personal data, in conflict with the GDPR. At that time, Facebook was among the companies that had self-certified and joined the Safe Harbour framework. Having pledged to follow its binding rules, they could lawfully utilize this mechanism when needed for data transfers at that time. Ultimately the case went to the CJEU and the Safe Harbour framework was annulled in 2015 due to its safeguards against US surveillance practices being found inadequate.[103]

According to the CJEU Schrems I decision, it was established that a third country must have an "essentially equivalent" level of data protection as those afforded by EU legislation. The data protection measures must not necessarily be duplicates to the rules of the GDPR, but demonstrably close enough. This rule allows for some flexibility as the level of adequacy required can be achieved through a combination of supervision by independent bodies and enforceable data subject rights and obligations for data controllers in the third country.[104] Evaluating the effectiveness of data protection processes relies on having robust legal frameworks and efficient enforcement mechanisms.[105] The European Court of Justice set the standard that the level of protection in third countries must be similar to what is legally guaranteed within the EU even if the methods to achieve the required data protection may not be identical.[106] Following the CJEU ruling, the court found that if independent supervisory authorities determined that a data subject's claim against an adequacy decision was valid, then they should have the ability to participate in the legal proceedings.[107] The CJEU stated that the responsibility remained with the national legislature to create laws allowing the national supervisory authority to raise valid concerns in front of national courts. If the courts find sufficient doubt as to the third country's adequacy decision then they can seek a preliminary ruling to examine its legitimacy.[108]

Upon assessing the state of the Safe Harbour transfer mechanism, the CJEU was critical. The court found that Safe Harbor did not include rules restricting the US

[102] CJEU Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 2015.
[103] *Schrems I.*
[104] Recital 104 GDPR.
[105] GDPR Adequacy Referential, p 2.
[106] *Schrems I* para 72-74.
[107] Article 58(5) GDPR.
[108] *Schrems I* para 65-74.

state agencies from overstepping the fundamental rights of data subjects. The court found that there was a high risk of US government overreach in personal data processing when arguably justified for the sake of maintaining national security. Schrems I demonstrates a case where the third country legislation went beyond necessity, when indiscriminate storage of European personal data was permitted without specification of criteria or limitations.[109] Following Schrems I the European Essential Guarantees were developed by the Article-29 Working Party. The EEGs build upon the Charter[110] and the ECtHR articles[111] relevant to surveillance issues. The four essential guarantees are as follows: (1) personal data processing must be performed on a legal basis; (2) the principles of necessity[112] and proportionality must be demonstrated as well as maintained; (3) interdependent supervisory authorities must exist to oversee the personal data processing; and (4) data subjects must have the practical ability to exercise their rights under GDPR as well as access to an effective redress mechanism. While the implementation of these rules varies in operations concerning national security, the essence of these four essential guarantees must be honored in.[113]

2.4.2 The Snowden revelations

The Snowden scandal of 2013 resulted in knowledge of the mass surveillance programs employed by the US National Security Agency being made public. Whistleblower Edward Snowden, who had security clearance and worked as a computer systems contractor for the NSA, revealed two main types of data collection methods used by the agency: Upstream, which involved the interceptions of communications on fiber cables as data is transmitted, and PRISM, which directly collected data from the servers of major US service providers including Microsoft, Google, and Facebook among others. Given that US data centers host a major portion of the world's data, the PRISM program provided the US government with incredible insight to individuals' private lives, both foreign and domestic. These surveillance activities were ultimately found to be in violation with the Foreign Intelligence Surveillance Act, as determined by the US Court of Appeals for the Ninth Circut. Nonetheless, Snowden fled to Russia when the scandal broke and still faces espionage charges in the US to this day.[114]

The groundwork behind the legality of these surveillance measures lies in the fallout of the 11 September 2001 terrorist attacks on the World Trade Center in New York City. Soon after the attack, new anti-terrorism legislation, the Patriot Act was passed by the US Congress. This legislation greatly enhanced the lawful surveillance capabilities of state agencies such as the NSA, leading to heightened intelligence activities and intensified anti-terrorist measures to prevent the reoccurrence of a similar event. This act increased the state agencies' authority to access records, conduct secret searches on private property, and broadened "tap and trace" searches

[109] see also S and Marper v United Kingdom, ECtHR, para. 67: "The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8.
[110] Articles 7,8,47,52 Charter.
[111] Article 8 ECHR.
[112] Article 5(1)(c) and 6(1) GDPR.
[113] Article 29 Working Party Adequacy Referential adopted on 28 november 2017 WP 254.
[114] Constitutional Rights Foundation, *Edward Snowden, the NSA mass surveillance*, (2016).

which expanded the exceptions permitting geographical location-tracking of electronic communication transmissions.[115]

2.4.3 Schrems II and Privacy Shield

The EU-US Privacy Shield framework was enacted in 2016 following the downfall of the Safe Harbor framework.[116] Only companies that pledged to follow the binding Privacy Shield rules could utilize this mechanism for streamlined data transfers. Other US entities that did not join the Privacy Shield still had to utilize other available transfer mechanisms due to the lack of comprehensive data protection law in the US at that time.[117] When Privacy Shield was implemented in 2016 the European Commission issued a press release indicating that they had solved the problems surrounding unlawful data gathering by US actors, the EU Commission stated that the US had given the EU assurances that no indiscriminate surveillance would be conducted by governmental agencies, even for national security purposes.[118] Meanwhile Austrian activist Max Schrems was dissatisfied with what he believed to be an inadequate remedy to his original complaint regarding the probability of continued, unlawful personal data processing by US intelligence agencies. Together with his legal team, he once again sought to challenge Facebook and the lawfulness of the transference of European data subjects' personal information to the US. The case eventually made its way back to the Court of Justice of the European Union.

Due to the Schrems II case, the purposes for which signals intelligence data could be lawfully collected in bulk in the US according to the PPD-28 were analyzed by the court.[119] Signals intelligence was the specific term used by the NSA in reference to the data collected from electronic signals and systems. Data collection for this type of intelligence purpose was rationalized by the objective of gaining insights into the actions and agendas of foreign adversaries and providing essential information to US policymakers its military. However, no crime was needed under PPD-28 to justify the execution of this type of mass personal data collection, merely the threat of a crime that could cross a border was necessitated. Additionally, when signals intelligence were collected temporarily, the purpose limitations were not applicable.[120] This meant that if US intelligence agencies collected a mass quantity of data for the purposes of sifting through it, the purpose limitations stated above had no application so long as the data was subsequently disposed of. The specific constraints for the duration for which the personal data may be retained were not clearly defined.

During the Privacy Shield joint review, discussions revolved around interpreting and applying the legal requirements before bulk data collection according to US national

[115] The Patriot Act Section 213-218.
[116] 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.
[117] EU Commission press release. *Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers* (2017).
[118] EU Commission press release. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows* (2016).
[119] Annex VI, Presidential Policy Directive 28 - Signals Intelligence Activities.
[120] Footnote 5 PPD-28.

security law.[121] According to the PPD-28 it was stated that as long as the bulk data collection was only acquired temporarily, then the limitations on bulk data collection were not to apply to signals intelligence data.[122] This condition allowed US authorities to pursue targeted data collection in the interests of maintaining national security. However, the collection of personal data en masse results in increased risks for data subjects; before national security interests are used to justify mass data collection, prior independent authorization is essential to protect against arbitrary and otherwise unlawful data processing.[123] The CJEU found that the bulk data collection occurring under the legislative framework of EO 12333 and PPD-28 were happening, not only without a clear and precise limitation of the scope, but without any initial review by a court.[124] Ergo, it can be interpreted e contrario that so long as the scope is sufficiently precise, bulk data collection may be permissible.[125] This point serves to demonstrate the necessity of setting a clear scope and precise purpose limitations for data processing as a lack thereof escalates the high likelihood for unlawful or unethical data processing.

In the Schrems II decision, the court emphasized that when it came to assessing the data protection adequacy of a third country's laws, it was important to go beyond examining surveillance practices within the European data controller's own borders as the third country national legislation allowing for covert monitoring of EU personal data outside of the third country's geographical territory must be investigated as well. The CJEU stressed that the adequacy status provided by the EU Commission was contingent on necessary limitations to foreign government access to personal data, even subsequent to transfer. Schrems II resulted in the revelation that US intelligence organizations could lawfully access European's personal data in their own jurisdiction, due to permissive US legislation[126] in direct conflict with the GDPR and Europeans' fundamental right to respect for their private family life and their right to protection of personal data.[127] It was also found that the data subject redress mechanism was insufficient due to the lack of power held by the associated Ombudsperson to independently influence US intelligence agencies[128] in violation of the Charter.[129]

The CJEU finally concluded that the Foreign Intelligence Surveillance Act lacked sufficient limitations to intelligence agency authority in conducting mass personal data collection. As such, FISA could not adequately uphold a level of data protection sufficient to meet the requirements of the GDPR or the CFR.[130] The Privacy Shield was thus determined to be in severe conflict with the requirements set out by article 45(1) GDPR governing transfers based on an adequacy decision. The CJEU judged that the SCCs and BCRs between EU and US entities already in place could remain so, but the Privacy Shield had to be invalidated. The fallout of Schrems II revealed

[121] Executive Order 14086 Section 4(b).
[122] Section 2 footnote 5 PPD-28.
[123] ECtHR *Big Brother Watch judgment*, para. 350.
[124] *Schrems II* para 83-185.
[125] EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
[126] FISA and Executive Order 12333.
[127] Article 7 and 8 Charter.
[128] *Schrems II,* para 195.
[129] Article 47
[130] *Schrems II,* para 180.

that the framework did not meet the standards of GDPR for essentially equivalent protection,[131] ultimately leading to its subsequent dissolution. The CJEU ruled that the mass surveillance in the US was so extreme that it violated the "essence" of fundamental rights,[132] This is deeply significant because the CJEU had previously only used this language to describe torture. The legislation allowing for the surveillance of electronic communications at the known scale was found to contravene the fundamental right to respect for private life as prescribed by the Charter, in violation of its core meaning.[133]

[131] Article 45(1) GDPR.
[132] Article 52 Charter and *Schrems II* para 94 and 95.
[133] Article 7 Charter.

3 The EU Commission's adequacy decision for personal data transfers to the US

3.1 Introduction –the launch of a new transfer mechanism

On 10 July 2023 the European Commission's adequacy decision regarding personal data transfers to the United States was implemented.[134] The adequacy status was reached after the successful development of the EU-US Data Privacy Framework, crafted in collaboration between the EU Commission and the US Department of Commerce. It serves as a legal transfer mechanism for organizations on either side of the Atlantic and streamlines the transferring of data from the EU to US entities. This framework, facilitating the secure transfer of European personal data, is the third of its kind.

The EU-US DPF includes increased transparency and stronger protections for European individuals' data abroad. Upon implementation of the EU-US DPF, the EU Commission judged that the US fulfilled the requirements set out by article 45 of the GDPR regarding the standard of protection for personal data transfers to the US organizations that join the framework.[135] US entities are not obligated to join the framework, however, joining is done voluntarily and when an organization has done so, the framework's requirements become binding and enforceable under US law. This framework falls under the jurisdiction of and is enforced by the Federal Trade Commission and the US Department of Transportation (for the time being, in the future other statutory entities may be added).[136] US entities will have to self-certify that they live up to the framework's requirements. Once certified, the joined companies are publicly listed by the US Department of Commerce.[137] However, US entities who do not join the EU-US DPF, still require additional data protection safeguards to facilitate the use of an alternative transfer mechanism when performing their own international personal data processing activities.[138]

3.2 EU-US Data Privacy Framework

The EU-US Data Privacy Framework serves as a regulatory mechanism allowing for the free flow of personal data between participating US companies and the EU and the three EEA member countries, (Norway, Iceland, and Liechtenstein). This new

[134] EU Commission Implementing Decision of 10.7.2023 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 (Adequacy Decision).
[135] EU Commission press release. *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows* (2023).
[136] Section 5 of the Federal Trade Commission Act prohibiting unfair or deceptive acts in or affecting commerce.
[137] Section I.3 of Annex I of the Adequacy Decision.
[138] Adequacy Decision para 48-52 and Article 46 GDPR.

adequacy decision was subsequently issued in line with article 45 GDPR regarding personal data transfers from the EU/EEA to third countries. This framework replaces the transfer instruments that were previously overturned following the CJEU judgements of Schrems I and Schrems II.[139] The EU-US DPF was necessitated after the downfall of its predecessor, the EU-US Privacy Shield Framework after the successful argumentation in Schrems II that the personal data of European individuals was at an unacceptable risk of being inappropriately accessed by United States intelligence agencies and that European data subjects did not have a sufficient redress mechanism to exercise their rights abroad.[140]

US companies who join the EU-US DPF do so through the US Department of Commerce and are required to self-certify and demonstrate their commitment to upholding the embodied principles.[141] This framework seeks to alleviate the issues brought to light by the Schrems II ruling and as such, introduces a new redress system, including a Data Protection Review Court available to assist Europeans with their concerns regarding access of their personal data by US government agencies when personal data transfers are performed on the basis of an adequacy decision. The benefits of this deal support the economic cooperation between the EU and the US while providing additional safeguards for European data subjects.

The scope of the recently established EU-US data privacy framework is multifaceted, addressing critical aspects of personal data transfers to the US since the fall of its predecessor. From the date of application, data transfers using the framework are permitted by the adequacy decision without the need of another transfer tool for affiliated companies. The adequacy decision is relevant to organizations geographically located within the EU and other entities abroad that are subject to the GDPR due to the extraterritorial nature of the regulation.[142] The EU-US DPF indicates the renewed commitment of the US government to honor the values established by the GDPR and is the culmination of successful collaboration with the EU Commission.

3.3 Legal grounds for processing European personal data by the US government

Data access for national security purposes by American law enforcement are primarily governed by the Foreign Intelligence Surveillance Act, Executive Orders, the Attorney General Regulation, as well as the Fourth Amendment of the US Constitution which protections US persons from unreasonable searches and seizures by their government. In the aftermath of the Schrems II judgment, the EU Commission had to reevaluate the compatibility of the GDPR with the relevant sections of FISA[143] and EO 12333.[144] Prior to the adoption of the EU-US Data Privacy Framework, the EDPB issued an official opinion on the draft of the adequacy decision acknowledging improvements, particularly with regards to the new redress mechanisms, but called for a reassessment by the EU Commission of the procedures

[139] Adequacy Decision para 4-6.
[140] Article 15-21 GDPR.
[141] Annex I, Section III.6. Adequacy Decision and para 45-48.
[142] Article 3(2) GDPR.
[143] Specifically sections 105, 302, 402, 501 and 702 FISA.
[144] Executive Order 12333 United States Intelligence Activities.

concerning US intelligence agencies related to Executive Order 14086. The aim was to proactively and more substantially address the considerable risk of unlawful US governmental access raised by the CJEU. While the EDPB acknowledged that the legal avenues for US state intelligence agencies were limited by the introduction of EO 14086, they took issue with the risk for GDPR noncompliant data collection and retention still made possible by what the board considered to be deficient safeguards in the DPF.[145] The EDPB acknowledged that EO 14086 put strong requirements in place governing sufficient specification of the purposes of data collection, but a key concern remained EO 12333 which simultaneously allowed for the bulk collection of data without prior permission from an independent authority in the US legal system. As such, the Board stressed that 'processing should be based on clear, precise and accessible rules' in line with the European Essential guarantees.[146]

An extensive review of the EU Commission's Adequacy decision will be performed after one year and at minimum once every four years thereafter. (Note that the EDPB is critical to this point and would prefer increased monitoring).[147] EU member states and the EDPB may contribute feedback on the functionality of the EU-US DPF but ultimately the responsibility remains with the EU Commission to determine how often it is necessary to keep reviewing and modifying the decision.[148]

Legislation jeopardizing personal data protection, The Foreign Intelligence Surveillance Act, was originally put into effect after the Watergate scandal of the early 1970s. This scandal involved the break-in at the Democratic National Committee headquarters at Watergate orchestrated by agents eventually linked to President Richard Nixon himself. The scandal exposed the depth of abuses of power and obstructions to justice committed by the Nixon administration, ultimately leading to the President's resignation from office.[149] Following the explosive scandal, FISA was created to help regulate US government surveillance for intelligence investigations while seeking to simultaneously allow for the maintenance of state secrecy when needed for national security purposes. FISA covers electronics surveillance among other types of searches and this act implemented a unique US Federal court that conducts classified proceedings to evaluate search warrants provided under this legislation.[150] A warrant from the Foreign Intelligence Surveillance Court must be obtained to permit electronic surveillance of foreign actors. FISA is applicable, not to every US company, but when electronic communications service providers are used. Therefore, all telecom and cloud companies, commonly used by the public, are encompassed by this regulation. The second prerequisite was that the data collected concern foreign intelligence information. Foreign intelligence information in this context encompasses data related to protection of the US from foreign threats such as terrorist attacks, sabotage, or clandestine intelligence activity. It also covers data connected to the national defense and foreign affairs concerning foreign powers or

[145] EDPB Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
[146] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures and *Schrems II* para 175-180.
[147] EDPB Opinion 5/2023.
[148] Adequacy Decision para 3-4.
[149] Research guides: *Richard Nixon's political scandal: Researching Watergate* in the manuscript collections at the Library of Congress, 2021.
[150] US Department of Justice The Foreign Intelligence Surveillance Act.

territories, regardless of whether it involved US citizens.[151] Notably, however, there exists an exception applying to the US President who has the power to waive the court order requirement from the FISC for up to one year. This deviation is meant to be utilized when intelligence is being collected from places controlled by foreign actors or when communications between foreign powers are being targeted and with the approval of the Attorney General.[152]

During the period that the research for this essay was being conducted, Section 702 of the Foreign Intelligence Surveillance Act was being reevaluated by the US Congress as it was set to expire. The American Civil Liberties Union along with dozens of other civil society organizations raised publicity and lobbied Congress to persuade them not to renew this legislation on the grounds that US state agencies had demonstrably abused this power and betrayed the public trust by violating their fourth amendment constitutional rights.[153] This legislation was initially intended to protect national security interests but evolved into a tool for domestic surveillance instead. The efforts to prevent the renewal of Section 702 FISA were ultimately unsuccessful, and it currently remains in effect with the authority granted under the FISA Reform and Reauthorization Act of 2023.[154] The act is reauthorized for eight years from December 2023. Some updates were made, however. The new legislation strengthens accountability by imposing new penalties including criminal liability and administrative penalties for FISA noncompliant actions by government officials. Simultaneously the bill expands government agencies' abilities to use FISA to investigate non-US persons living abroad for the purpose of discovering bad actors involved in illegal drug activity affecting the US. This expansion of authority is justified by the arguable need to modernize FISA to keep up with new threats, particularly concerning the trafficking of illicit drugs into the country. The new restrictions added to the reformed bill do seek to provide assurances regarding increased protection for American citizen's personal data only, leaving all non-US persons subject to this continued oversight at the discretion of US state agencies.[155]

The signing of US Executive Order 14086 on Enhancing Safeguards for US Signals Intelligence Agencies sought to address the privacy concerns raised by the Schrems II judgment. Subsequent to the overturning of the previous data transfer mechanism, Privacy Shield, negotiations to remedy this issue took place between the European Commission and the US Government.[156] Consequently, Executive Order 14086 was issued by US President Biden in October 2022. Executive orders are official directives issued by the incumbent US president that circumvent the need for approval by the US Congress. The only way to retract an existing executive order is for the sitting US president to issue a new EO for that very purpose. Regarding intelligence activities, the EO 14086 introduced the principles of necessity[157] and

[151] 3365(2) § US Code Title 50.
[152] 1802 § US Code Title 50.
[153]ACLU *ACLU Urges Congress to Oppose Attempt to Sneak Section 702 Reauthorization into "Must-Pass" Defense Spending Bill.* American Civil Liberties Union. (2023).
[154] FISA Reform and Reauthorization Act of 2023.
[155] The Permanent Select Committee On Intelligence. *House Intel Committee approves FISA Reform and Reauthorization Act of 2023.* 2023.
[156] Adequacy decision para 6-8.
[157] Article 5(1)(c) and 6(1) GDPR.

proportionality to the framework.[158] EO14086 affects the transfer of European personal data as it regulates data collection by and information sharing between US state actors. As such, the order was highly relevant to Schrems II as the assessment was made of its practical effects on the personal data collection processing activities done by US intelligence agencies. New data protection requirements were designed in EO 14086, paving the way for inception of the EU-US Data Privacy Framework. In response to the complaints brought up by the Schrems II ruling, EO 14086 implemented the two GDPR principle requirements of necessity[159] and proportionality into US law.[160] As a result, European personal data could thereafter be accessed by US intelligence agencies only when such data processing was done when necessary and proportionally, within the scope of public, or an otherwise legitimate interest.

Large electronic communications companies like Google were encouraged to individually add their own "supplementary measures" to augment the new data protection requirements of the EO. Such measures included, for example, added technical security steps such as encryption as well as physical hindrances like physical barriers to data centers. However, additional safeguards put into place by individual companies can be somewhat misleading to data subjects.[161] Logically, added data safeguards can serve to protect personal information from data breaches. These measures, however, prove ineffective when pertaining specifically to access by US state agencies considering present US surveillance legislative allowances. The obstacles to enforcing the GDPR when European personal data is held by US entities raises concerns about its possible efficacy.

Executive Order 14086 replaced the previous Presidential Policy Directive 28 in its entirety except for section 3, section 6, and the classified annex. PPD-28 was issued in January 2014 under the Obama administration and primarily addressed the intelligence activities of US agencies, particularly in relation to the treatment of personal data of foreigners, that is, non-US persons. Its focus was on protecting privacy rights and limiting intelligence access. Emphasis lies on the safeguarding of personal information of non-US people in the context of their personal data collection through signals intelligence activities and restricting access to that personal information.[162] While the language of EO 14086 closely resembles its predecessor, PPD-28, the former provides additional clarity and introduces new data protection safeguards, building on FISA and EO 12333. EO 14086 includes twelve new objectives for legitimate signals intelligence collection[163] and six new objectives for legitimate bulk data collection[164] However, the vagueness of some of the stated aims leaves room for potential misuse. One such glaring concern is that the order permits the US President to quietly add undisclosed objectives if public disclosure is deemed a risk to national security.[165] EO 14086 also includes some additional justifications for mass surveillance activities, citing health crises or

[158] EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
[159] Article 5(1)(c) and 6(1) GDPR.
[160] Executive Order 14086, Section 2, (a), (ii), A and B.
[161] Article 4(1) GDPR.
[162] PPD-28.
[163] Executive Order 14086, Section 2, (b), (ii), A, 1 to 5.
[164] Adequacy Draft Decision, recital 134 and EO 14086, section 2(c)(ii).
[165] Executive Order 14086, Section 2(b)(i)(B).

climate change, expanding the scope of permissible bulk data collection under the new order.

The shift from the previous requirement of being "necessary" to now being "necessary and proportionate" reflects an alignment with the principles outlined in Articles 7, 8, and 52 of the Charter of Fundamental Rights. EO 14086 establishes new requirements for the US intelligence agencies to update their policies to reflect the new requirements of necessity[166] and proportionality including the requirement for US agencies to renew their processes in collaboration with the Attorney General, the Civil Liberties and Privacy Office, and the Privacy and Civil Liberties Oversight Board. The agencies must publicize these changes as much as possible and they are given one year to become compliant.[167] However, there remains an apparent incongruence between the emphasis on proportionality in the new EO and the lack of corresponding changes to existing regulations such as the Foreign Intelligence Surveillance Act and the PRISM program. As such, the legal interpretation of the term "proportionality" is undergoing turbulence considering that under the new EO, surveillance will be proportionate while simultaneously regulations such as FISA and the PRISM program remain unchanged. The purpose of these objectives serves to ensure that the personal data collection is not only necessary but proportionate. Executive Order 14086 provides detailed guidelines specifying when data collection is permitted for intelligence purposes, applicable to European residents as well as US residents, to ensure that Europeans experience the same level of data protection as US citizens.[168] It is crucial to note, however, that EO 14086 only applies to data transferred from the European Union to the US *after* its implementation in July 2023. This implies that under the present conditions, EU companies would need to remove and retransfer all personal data to the US to benefit from the updated safeguards. Under these circumstances, the prospect of a substantial portion of personal data undergoing retransfer is highly improbable.

3.4 The adequacy decision pertaining to surveillance practices

The European Commission was obligated to conduct a comprehensive analysis of the state of data safeguards in the US to assess whether the existing protections were "essentially equivalent" to those in the EU before issuing its adequacy decision.[169] The 2023 adequacy decision pertaining to data transfers to the United states fully acknowledges that US state agencies may access European personal data once received as well as abroad[170] although emphasis was placed on the implementation of the new safeguards provided by the EU-US DPF. These new protections include ordering targeted collection over bulk collection[171] when possible, in the context of signals intelligence collection. Notably the EDPB is critical to the permitting of large-scale data collection by US actors, pointing out that EO 14086 and EO 12333 do not adequately regulate the need for independent prior authorization prior to bulk

[166] Article 5(1)(c) and 6(1) GDPR.
[167] Executive Order 14086, Section 2(c)(iv)(B) and (C).
[168] Adequacy Draft Decision, Recital 150.
[169] Article 45(2) GDPR and Adequacy Decision para 3.
[170] Adequacy Decision para 121-122 and Executive Order 14086 Section 5(f).
[171] Executive Order 14086, Section 2, (c), (ii), A.

data collection.[172] Safeguards preventing inappropriate retention are implemented involving increased oversight and the establishment of specified retention periods.[173] The new ruling that non-US persons be subject to the same personal data retention rules as US persons, reflects another material change.[174] Even safeguards against the dissemination of personal data were implemented.[175] The EU Commission justified its adequacy decision in part with the support of the aforementioned safeguards in combination with the acknowledgement of more general requirements that US intelligence agencies were subject to regarding purpose limitation, data minimization and security.[176] Deviations from this right are to be "strictly necessary" to minimize interference with data subjects. Surveillance by US national security agencies (or indeed any third country state actor) is not considered democratically justified when the surveillance is not strictly necessary. [177] The practice of spreading personal data between state agencies after collection remains somewhat unclear, however, as personal data may be collected and then shared with other law enforcement organizations. Some of those agencies may not, themselves, be allowed to collect that personal data directly for the purposes of criminal investigations. When sharing personal data between state agencies, protective safeguards should still be maintained to mitigate the potential risk of harm.[178] There also appears to be a gap in the rules, namely, that the safeguards outlined for bulk data collection[179] do not apply during the initial phase of targeted US signals intelligence when the bulk data is being processed on a temporary basis.[180]

3.4.1 Oversight

The adequacy status was in part reached based on numerous new oversight requirements for US state agencies which play a pivotal role in upholding the legality of personal data processing.[181] Such independent oversight in the context of surveillance practices is crucial to maintain lawfulness of processing[182] which is particularly important pertaining to covert data collection as data subjects are unlikely to possess the ability or resources to object in any meaningful way.[183]

3.4.2 The new redress mechanisms

The new redress mechanisms established by the EU-US Data Privacy Framework seek to tackle the challenge of providing effective recourse for European individuals to exercise their data subject rights in the US. Individuals are now free to choose the mechanism they prefer and the potential options for recourse can exist in both the EU and the US. Complaints can be made directly to different branches of the US

[172] EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework para 144-146.
[173] Adequacy Decision para 105.
[174] Adequacy Decision para 157 and Executive Order Section 2(c)(iii)(A)(2)(a)-(c).
[175] Executive Order 14086 Section 2(c)(iii)(A)(1)(c).
[176] Adequacy Decision para 159-160.
[177] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures p 8.
[178] EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework 149-155.
[179] Executive Order 14086 Section 4(b).
[180] Executive Order 14086 Section 2(c)(ii)(D).
[181] Adequacy Decision para 107-111.
[182] Article 8(3) Charter.
[183] EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework para 163-165.

government including the Federal Trade Commission and the Department of Commerce. Other options include an independent mediation body, chosen by the entity involved with the alleged improper data processing, and of course, in the data subjects own country, the national data protection authorities are enabled to cooperate with US entities to help European data subjects.[184]

This newly established Data Protection Review Court was established by the US Attorney General following the order of EO 14086[185] and includes more robust authority to address violations compared to the preceding Ombudsmechanism. The EDPB expressed satisfaction at the progress made in addressing European data subject rights with the new data protection review court but remains wary of the practical implementation.[186] It's important to note that the data protection review court's proceedings will be kept confidential, and the judgements issued from it cannot be appealed, leaving a legal gray area.

The United States government has introduced new protective measures of data subject rights specifically in terms of legally dubious surveillance. A new redress mechanism has been introduced that European residents may make use of if they are suspicious of data processing activities pertaining to intelligence actors in the US. The fact that European residents have no burden to provide proof that their personal data is being mishandled before the complaint will be investigated is of paramount significance. The EU Commissions concluded that together with the increased oversight, the introduction of these new redress mechanisms satisfied the requirements of lawfulness and proportionality.[187]

3.5 Impact of improper bulk data collection

The purpose of the protection of personal data is to mitigate adverse impacts against individuals. In the context of mass personal data collection and surveillance, one critical concern is the risk of profiling and discrimination. In this example, accused but not convicted, individuals are particularly vulnerable to unjust treatment, in conflict with the fundamental principle of non discrimination. Surveillance, being inherently intrusive into individuals' private lives, raises additional concerns when considering special category data (information about health, family life, sexual activity, etc) under the GDPR.[188]

Mass surveillance threatens the foundational freedoms of the EU, which include freedom of thought, conscience and religion, freedom of expression and information, and freedom of assembly and association.[189] Advocate General Cruz Villalon suggested that the mass retention of personal data would have a "Chilling effect." (He was referring at the time to the Data Retention Directive[190] which is no longer in effect) This type of surveillance poses a significant threat to European individuals'

[184] Adequacy decision para 65-72.
[185] Adequacy Decision para 6 and 176.
[186] EDPB Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
[187] Adequacy Decision para 89-90 and *Schrems II* para 174-175.
[188] Article 9 GDPR.
[189] Articles 10-12 Charter.
[190] EU Directive 2006/24/EC.

right to privacy and carries substantial impact on freedom of expression[191] of European citizens. Constant and secretive data collection is harmful, individuals feeling like they are constantly under surveillance would be detrimental to their well-being.[192] Beyond the perils surveillance brings for individuals, additional risks threaten society at large. Personal data collected by mass surveillance could provide bad actors with the power to sway public opinion or manipulate people for political purposes.[193] This practice would threaten stability and trust across society at large.

[191] Article 11 Charter.
[192] CJEU Case C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, 2014 para 37 and 72.
[193] EDPS Opinion 3/2018 on online manipulation and personal data, footnote 42.

4 Discussion and conclusion

4.1 Conflict between concurrent legislation

The legal framework relevant to bulk data collection[194] in the US are primarily the Foreign Intelligence Surveillance Act and Executive Order 12333. Given that FISA applies when an electronic communications service provider is being employed and when the data in question concerns foreign intelligence information, the act applies to US data controllers and processors that handle European individuals' personal data, for example Facebook. This is deeply problematic because given the GDPRs extraterritorial nature,[195] the act of processing that personal data falls under the conflicting rules set by the GDPR. FISA split personal data into two categories: US and non-US persons. This is of great significance because the 4th amendment of the US Constitution, protecting individuals from unreasonable searches and seizures by the US government, is only applicable to US-persons, hence the distinction. Taking into account that FISA is applicable without probable cause, without necessitating that a crime has taken place, and without a warrant from a judge, the infringement on individual privacy rights are explicit. Moreover, interpretation of the applicable scope of this act is troublingly left vague, subject to interpretation.

To help address this vulnerability, the European Essential Guarantees were developed to specify *inter alia* the conditions under which third country national security agencies were justified to carry out surveillance measures of European personal data.[196] Yet these guarantees are unsuitably named given that the embodied protections are far from guaranteed. They are, in fact, wholly undermined by the enduring authority of FISA. These measures, while lawful in the US at this time, leave European data subjects (among others) profoundly vulnerable to US government overreach, overstepping their fundamental rights in unambiguous opposition to the rules set by the GDPR[197] and the other underlying European freedoms sheltering personal data protection rights.[198]

While the US government is subject to sweeping criticism for the mass data collection by its intelligence agencies and it is established that these practices do indeed violate European law when European data subjects are affected, the GDPR does notably allow for exceptions to its application[199] under certain conditions.[200] These exceptions apply to personal data processing by member state authorities within the EU on the grounds of protecting national security[201] as well as for law enforcement in the efforts of maintaining public security and national defense and for the actions imperative to hinder and prevent criminal activities.[202] This exception

[194] Executive Order 14086 Section 4(b).
[195] Article 2 and 3 GDPR.
[196] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures p 5.
[197] Article 1 GDPR.
[198] Articles 7-8 ECHR and Article 52(1) Charter.
[199] Specifically restricting the rights provided by Article 5, Articles 12-22, and Article 35 GDPR.
[200] Article 2(2), Article 23(1), and Recital 19 GDPR.
[201] Article 23(1)(a) GDPR and CJEU, C-623/17 *Privacy International/Secretary of State for Foreign and Commonwealth Affairs*, (2020).
[202] Article 23(1)(b-d) GDPR.

even extends to allow for EU state agencies to conduct surveillance of European data subjects when the rationalization can be made for the purposes of safeguarding correlative interests.[203] Such covert monitoring activities may be executed with the aim of hindering criminal activity or even in the context of investigating individuals in regulated professions for a possible breach of ethics.[204] These exceptions for state law enforcement agencies within the EU and the relative lack of oversight by EU institutions are in stark contrast to the rigorous critique lobbied towards the US government for, to a certain measure, comparable practices.

4.2 Impact of Schrems II on the EU-US Data Privacy Framework

The cornerstone legal cases, Schrems I and Schrems II, sounded the alarm in Europe pertaining to the ongoing bulk data processing being performed by US intelligence actors and thrust these actions into the limelight. The resulting impact of Schrems II includes causing the void of a transfer mechanism to the US based on adequacy,[205] subsequently filled by the creation of the EU-US Data Privacy Framework. In terms of Schrems II ramifications on the contents of this new data transfer framework in the endeavor of hindering covert surveillance activities, it includes the development of new binding limitations that US intelligence agencies are subject to going forward, restricting their bulk personal data collection concerning European personal data, as well as the lauded introduction of the principles of necessity[206] and proportionality[207] into US legislation.

Fallout of Schrems II included the creation of a new Data Protection Review Court to meet the complaint pertaining to the glaring lack of an effective redress mechanism available to EU data subjects in the United States.[208] While the GDPR provides legislation considerably limiting the oversight of European personal data by outside interests[209] and progress has been made in that regard in the US with the development of new redress mechanisms.[210] Internally, however, EU laws governing surveillance vary considerably as that sovereignty is largely left to the member state governments themselves.[211] Now European individuals are provided with new redress mechanisms in the US but a comparably authoritative mechanism is not accessible to US data subjects.[212] At this time such a corresponding redress mechanism does not appear on the horizon however in the spirit of reciprocity such a development would moreover be beneficial for spreading the values and principles of European personal data protection in the international community.

[203] Article 2(2)(d) and article 23(1)(h) GDPR.
[204] Recital 73 GDPR.
[205] Article 45 GDPR.
[206] Article 5(1)(c) and 6(1) GDPR.
[207] Article 52(1) Charter of Fundamental Rights of the European Union; Article 5(4) TEU; and Recital 4 and Recital 170 GDPR.
[208] *Schrems II* para 191.
[209] Chapter V GDPR.
[210] Adequacy Decision, Annex I, Section II.7 and III. 11.
[211] Article 2(2), Article 23(1), and Recital 19 GDPR.
[212] Swire, P. iapp The Privacy Advisor. *A guide to the attorney general's finding of 'reciprocal' privacy protections in the EU.* 2023.

4.3 Endurability of the 2023 adequacy decision against the backdrop of the GPDR

Given that FISA has not undergone substantial alterations since the Privacy Shield was invalidated, the EU Commission's justification for granting its third US adequacy decision is called into question. The US EO 14086, with its expanded legal grounds for mass surveillance activities, citing health crises and climate change, modernized the scope of permissible surveillance under the new order.[213] In the context of a pandemic, surveillance could be performed to monitor contact tracing, helping to control the spread of illness. Personal data collection could also be monitored in bulk to aid the effort of preparation for climate change related disasters so as to allocate resources efficiently and coordinate emergency responses.[214] These hypothetical scenes demonstrate some of the potential benefits to public monitoring in these conditions. Nevertheless, there remains ambiguity concerning the practical application of these measures given the publicized disclosures of the extreme overreach of past US intelligence agencies under these circumstances.[215]

The judicial authority of the principles of necessity[216] and proportionality[217] in the context of European personal data processing have been well established by now.[218] Additional data protective technical or organizational safeguards, while valuable and worthy of realization, are ultimately inadequate in third countries in cases where the government in that country oversteps the European principles of necessity[219] and proportionality.[220] Despite the new provisions in the 2023 adequacy decision based on the progress made by the EU-US DPF and the changes implemented to shield European personal data from US surveillance interests, the GDPR rules governing adequacy as a transfer mechanism[221] remain manifestly unfulfilled against the backdrop of current US surveillance law. In spite of changes made to the US legal framework and the implementation of the EU-US Data Privacy Framework, critical risks for improper bulk data collection in the US remain that threaten the integrity of European data subjects personal information hosted by US data centers. Thus, the sustainability of the third adequacy decision seems deeply improbable with consideration to the looming threat of Schrems III.

4.4 Possible solutions

To address the difficulty of preventing improper access by US intelligence agencies to European personal data, one potential solution would be to keep the data segregated. Specifically, when European personal data is hosted by US entities, developing the option to outsource it exclusively to separate European entities geographically and materially subject to the GDPR only could be considered. While this possibility does not fully exist today, as personal data protection awareness rises, public pressure may bring this prospect into reality in the future. Implementing such

[213] Executive Order 14086 Section 2(b)(i).
[214] Adequacy decision para 134.
[215] Primarily in reference to the Snowden revelations.
[216] Article 5(1)(c) and 6(1) GDPR.
[217] Recital 170 GDPR.
[218] Article 52(1) Charter of Fundamental Rights of the European Union; Article 5(4) TEU; and Recital 4 and Recital 170 GDPR.
[219] Article 5(1)(c) and 6(1) GDPR.
[220] EDPB 2020 p.27.
[221] Article 45 GDPR.

drastic measures would, however, be inefficient and require significant effort by both the EU and US entities involved.

The EU and the US could enter a treaty together with the objective of enabling EU institutions access to the European personal data collected by the US intelligence agencies. This would consist of a small step towards improved compliance with the GDPR,[222] although ultimately the impediments to protecting Europeans fundamental rights would endure. Despite this shortcoming, developing increased collaboration between the EU institutions and the US government may have beneficial effects for European data subjects as one could presume that if EU institutions are informed about the personal data collection activities of US state agencies, such activity would be less likely to occur without sufficiently robust justification.

4.5 Finals thoughts and conclusion

Notable strides have been taken to safeguard European personal data from unauthorized processing by US intelligence agencies as demonstrated by the Executive Order 14086 and the EU-US Data Privacy Framework, reflecting the shared commitment to address issues raised by the Schrems II ruling including the introduction of the Data Privacy Review Court and heightened standards for US state intelligence regarding surveillance activities. By doing so, this framework improves the balance between personal data protection and the legitimate needs of law enforcement. With the approval of the EU Commission, the EU-US Data Privacy Framework helps to establish an adequate level of protection for personal data transferred from the EU to joined entities in the US. However, the fact that the surveillance permitting legislation, FISA and EO 12333, remain resolutely in effect, significantly undermine the updated framework's ultimate impact. Challenges remain as the present legal landscape grapples with the inherent conflict between personal data protection and state agency security interests. The need for continued efforts to address this complexity in both the EU and the US jurisdictions persists. While progress has been made, an enduring solution to this issue is elusive due to the fundamental contraction between personal data protection and law enforcement surveillance objectives.

Contemporary US state surveillance practices subvert the fundamental rights to an effective redress mechanism, the right to privacy, and the right to personal data protection.[223] While the CJEU championed European values with their landmark judgements, Schrems I and Schrems II, given the public knowledge about bulk data collection conducted by US intelligence agencies, the annulment of the previous adequacy decision cannot be particularly unexpected. Indeed, the EU Commission notably undermined the European protective standards by granting the previous adequacy decision for the US in the first place. By doing so, the EU Commission fell short in their purpose of upholding European values and fundamental laws and in pursuit of other aims including international economic collaboration and greater participation in the modern digital community. Moreover, it is interesting that the

[222] Article 48 GDPR.
[223] Articles 7, 8, and 47 Charter.

CJEU did not invalidate SCCs as a data transfer mechanism after the downfall of the preceding adequacy status despite the fact that those clauses, while binding for the joined parties, had no authority to prevent US governmental personal data access, lawfully justified by the latter's domestic legislation.

The Schrems II judgment did state that data controllers and processors were obligated to diligently examine the necessity and possibility of applying additional data safeguards, however, specifically what these additional protective measures might be were not addressed by the court and alas, remain unclear.[224] While the CJEU demonstrated resilience and authority by overturning the two previous adequacy decisions, it is important to acknowledge that ultimately compromises were made. In that case, compromise was seemingly inevitable given the huge daily exchange of personal data transference to US entities against the backdrop of profoundly disparate legal frameworks.

The CJEU demonstrates the fortitude of the European judiciary while the EU Commission conversely reveals apparent weakness in the executive branch on the issue of personal data protection. The expanded data protection rights afforded by the GDPR were democratically implemented by the EU legislature and then ferociously upheld by the European judiciary. Then nonetheless the regulation was demonstrably subdued by the executors, the EU Commission, when they proceeded to grant a third adequacy status in clear violation of European data subjects fundamental rights and freedoms, and in transgression of the GDPR. The effectiveness of these democratically developed personal data principles are therefore called into question. If they are not upheld in practice, then one might wonder about the extent to which these sweeping measures are merely political theater.

Reconciling the obligations of applying personal data safeguards to the standard of the GDPR while that personal data is simultaneously subject to the US regulatory framework remains deeply problematic given that many of the commonly used data centers are subject to US jurisdiction. Evidently personal control over data is forfeited when personal data transfers conducted by global, decentralized entities like Facebook take place. By granting this third adequacy decision, the EU Commission is compromising the fundamental freedoms of European data subjects under external pressures and in favor of the advantages of personal data transferred to the US. This legal friction provokes contemplation about the state of democracy in the EU. Moreover, the introduction of the principle of proportionality to US surveillance legislation with the simultaneous granting of US adequacy status, despite the known and pervading risk of personal bulk data collection by US state intelligence agencies, means that the legal meaning of this concept of proportionality will be fundamentally altered. The principle will de facto be forcibly extended to encompass the present state of mass personal data collection.

As democracy is intrinsic to the rule of law in the EU, persistent efforts to implement these data protection regulations are critical for safeguarding fundamental human rights and reflecting the collective values of the European Union. The persistence of

[224] *Schrems II* para 133.

this judicial conflict between personal data protection and national security interests pose a threat to our democracy. While the GDPR focuses on the right to data protection, its instrumental significance in the modern era pertains to its close connection to other important fundamental rights such as the freedom of expression, the freedom of association, and the freedom of movement.[225] These rights are interlinked, and any erosion of one poses a threat to the integrity of the others. This dilemma provokes contemplation about which principles should take precedence in European democracy and ultimately raises questions about what manner of society we want to live in.

[225] Articles 10, 11, and 12 Charter.

Bibliography

EU legal citations

Charter of Fundamental Rights of the European Union

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

EU 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

EU Regulation 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)

European Commission Implementing Decision 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.

Treaty on European Union

Treaty on the Functioning of the European Union

US legal citations

Constitution of the United States of America

Executive Order 12333 United States Intelligence Activities

Executive Order 14086 On Enhancing Safeguards For United States Signals Intelligence Activities

FISA Reform and Reauthorization Act of 2023

Federal Trade Commission Act

Presidential Policy Directive Signals Intelligence Activities

The Foreign Intelligence Surveillance Act of 1978

USA Code Title 50 War and National Defense

USA Patriot Act

Publications

ACLU *ACLU Urges Congress to Oppose Attempt to Sneak Section 702 Reauthorization into "Must-Pass" Defense Spending Bill. American Civil Liberties Union.* 2023

Article 29 Working Party Adequacy Referential adopted on 28 november 2017 WP 254

Article 29 Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 2014

Article 29 Working Party, Working document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)

Constitutional Rights Foundation, *Edward Snowden, the NSA mass surveillance*, 2016

EU Commission press release. *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows,* 2023

EU Commission press release. *Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers*, 2017

EU Commission press release. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*, 2016

EDPB Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

EDPB Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework

EDPS Guidelines 04/2021 on Codes of Conduct as tools for transfers

EDPS Opinion 2018 european data protection supervisor

EDPS Opinion 3/2018 on online manipulation and personal data

Hettne, J., & Eriksson, I. O. *EU-rättslig Metod: Teori och genomslag I svensk rättstillämpning*. Stockholm: Norstedts juridik. 2011

Jareborg, N. *Rättsdogmatik som vetenskap*. SvJT. Svensk Juristtidning, 2004

Lee A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, 2014

Lundberg, K. et al. *Juridik: civilrätt, straffrätt, processrätt* 5th ed. Stockholm, Sweden: Sanoma Utbildning, 2019

Research guides: *Richard Nixon's political scandal:* Researching watergate in the manuscript collections at the Library of Congress, 2021

The Permanent Select Committee On Intelligence. *House Intel Committee approves FISA Reform and Reauthorization Act of 2023.* 2023

Swire, P. iapp The Privacy Advisor. *A guide to the attorney general's finding of 'reciprocal' privacy protections in the EU*. 2023

U.S. Department of State. *PPD 28: Policies and procedures*. U.S. Department of State, 2015

Case law

Court of Justice of the European Union

Cases C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert

Case C-101/01, Lindqvist, 2003

Cases C-203/15 and C-698/15, Tele2 Sverige AB, 2016

Case C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, 2014

Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 2020

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015

Cases C-465/00, C-138/01 and C-139/01, Rechnungshof 2003

Case C-623/17 Privacy International/Secretary of State for Foreign and Commonwealth Affairs, 2020

European Court of Human Rights

Case of Big Brother Watch and others v. The United Kingdom, 2021

Case of Benedik v. Slovenia, 2018

Case of Zakharov v Russia, 2015

Case of S and Marper v United Kingdom, 2008