universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

"Who determines the cloud? The (in)compatibility between US governmental access to personal data in the cloud and GDPR"

verfasst von / submitted by

Martina Wedenig, LL.B., LL.M.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2023 / Vienna, 2023

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Dr. Axel Anderl, LL.M. (IT-Law)

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen inländischen oder ausländischen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

Wien, September 2023

Martina Wedenig, LL.B., LL.M.

I. Table of contents

II. Index of abbreviations

Art	Article
AG	Attorney General
Art 29 WP	Article 29 Data Protection Working Party
BCR	Binding Corporate Rule
C2C	Controller to controller
C2P	Controller to processor
CFR	Code of Federal Regulations
Ch	Chapter
CIA	United States Central Intelligence Agency
Cir	Circuit
CJEU	Court of Justice of the European Union
CLPO	ODNI's Civil Liberties and Privacy Office
DNI	Director of National Intelligence
DoC	United States Department of Commerce
DoJ	United States Department of Justice
DPA	Data Protection Authority
DPF	EU-US Data Privacy Framework
DPRC	Data Protection Review Court
e.g.	for example
EC	European Commission
ECS	Electronic communication service
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EEG	European Essential Guarantees
EGC	European General Court
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
EPIC	Electronic Privacy Information Center
et seq	et sequitur / et sequentes
EU	European Union
EUR	Euro
FBI	United States Federal Bureau of Investigation
Fed. R. Crim. P.	Federal Rules of Criminal Procedure
Fed.Reg.	Federal Register
FIP	Fair Information Practices
FIPP	Fair Information Privacy Practices
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
Fn	Footnote
GPO	United States Government Publishing Office

H.R.	United States House of Representatives
HR	Human resource
IAPP	International Association of Privacy Professionals
IC	Intelligence Community
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	Media access control
Mio	Million
MLAT	Mutual Legal Assistance Treaty
NIPF	National Intelligence Priorities Framework
NSA	United States National Security Agency
NSL	National Security Letter
NSM	National Security Memorandum
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OFR	Office of the Federal Register
OJ	Official Journal
p	page
Par	Paragraph
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
Pub. L.	Public Law
RCS	Remote computing service
Rec	Recital
ROPA	Record of processing activities
SA	Supervisory authority
SCC	Standard Contractual Clauses
Sec	Section
TIA	Transfer impact assessment
U.S.C.	United States Code
UK	United Kingdom
UN	United Nations
Union	European Union and EEA Member States Iceland, Liechtenstein and Norway
US or U.S.	United States of America
USD	United States Dollar
Vol	Volume
WIPO	World Intellectual Property Organization

1. Introduction

The transatlantic economy is the largest in the world. With USD 6 trillion in total commercial sales and close to one-third of the world's gross domestic product, it is not only the largest but also wealthiest market. It is a place for investors, traders, employees, economic growth, and data sharing. With approximately EUR 1.1 trillion in the trade of goods and services in 2021, the European Union (EU) and the United States of America (US), not only constitute the two leading service economies in the world but are also each other's most important economical partners.[1]

Cloud computing and data transfers extending across multinational computer networks are the core of doing business in today's globalized world. The cloud is nowadays operated on an interconnected basis, where servers are maintained in various geographic locations. The term "cloud" is interchangeably used with "cloud computing" and consists of a global network of servers working together remotely and acting as a single ecosystem designed to store and manage data. Types of cloud systems vary based on their different topologies and the methods by which resources are deployed, however, the general idea of an on-demand remote network remains the same.[2]

The storage and easy access to data from almost anywhere in the world is not only convenient but raises a lot of challenges for law enforcement and national security. Even though many major cloud service providers reside in the US, in a vast majority of cases data travels through various countries or regions. This international scope and sometimes unclear data location brings traditional national legal processes how to request and obtain data for investigation purposes to their limits. Despite progressive globalization, under the international law's principle of sovereignty codified in international law as well as the United Nations' (UN) Charter[3], countries are independent in shaping their legal sphere.[4]

[1] *Hamilton/Quinlan*, The Transatlantic Economy 2022, p v, vii, viii.
[2] *ISO*, ISO/IEC 19831:2015, 3.3; *Mell/Grance*, The NIST Definition of Cloud Computing, p 6; *Microsoft*, What is the Cloud?.
[3] The Charter of the United Nations, United Nations Conference on International Organization San Francisco (June 26, 1945, as amended) <un.org/en/about-us/un-charter/full-text> (last retrieved Aug. 13, 2023).
[4] Art 2 (1) UN Charter; *Schwartz*, Legal Access to the Global Cloud, p 1681-1683.

On the one side, data privacy laws, such as the General Data Protection Regulation (GDPR)[5], protect natural persons and their personal data with a broad scope and extraterritorial applicability. On the other hand, countries are striving to strengthen their position in gaining easier access to obtain data for criminal and national security purposes which results again in a far extraterritorial reach. In any case, any extraterritorial application of a regulation ultimately leads to an overlap of applicability with a foreign state's regulations and their competences.[6]

In the context of the US and EU and their access and restrictions to personal data, controversies due to their different legal regimes as well as the mutual understanding of privacy have remained unresolved for years. The Snowden revelations in 2013 ultimately brought legal uncertainty for those who need to obey the laws of both regimes.[7]

More than 5 years ago, GDPR came into force and changed the legal landscape of data handling on a global basis. Just a few months earlier, the US enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[8], giving US authorities (in addition to already existing regulations such as Foreign Intelligence Surveillance Act of 1978 (FISA)[9] and Executive Order (EO) 12333[10]) extraterritorial access to electronically held data in the cloud for law enforcement purposes. In its fundamental decisions *Schrems I*[11] and *Schrems II*[12], the Court of Justice of the European Union (CJEU) clearly stated the requirements of an international data transfer of personal data to third countries which clarified the adequacy of the then existing EU-US data transfer mechanisms and legal regimes on both sides.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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, OJ L 119/1 (May 4, 2016).
[6] Art 1 (1) and (2) GDPR; Sec 102 (1) – (4) CLOUD Act, see reference *infra* Fn 8.
[7] *Guardian*, Edward Snowden says surveillance technology is more intrusive than ever.
[8] Clarifying Lawful Overseas Use of Data Act, Pub. L. 115–141, 132 Stat. 1213 (Mar. 23, 2018) <congress.gov/115/plaws/publ141/PLAW-115publ141.pdf> (last retrieved Aug. 13, 2023).
[9] Foreign Intelligence Surveillance Act of 1978, Pub. L. 95–511, 92 Stat. 1783 (Oct. 25 1978) <govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf> (last retrieved Aug. 13, 2023), as amended = 50 U.S.C. §§ 1801 et seq. (2023).
[10] Executive Order 12333, United States Intelligence Activities, 40 Fed. Reg. 235 (Dec. 8, 1981), amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008) <dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf> (last retrieved Aug. 13, 2023).
[11] C-362/14 *(Schrems I)*.
[12] C-311/18 *(Schrems II).*

Fast forward ten years to the year 2023, the global landscape of privacy has undergone extensive changes. So has surveillance technology. According to *Snowden* such technology is far more intrusive than ever not only due to governmental and big tech companies' current levels of access, but also due to nowadays commercially available surveillance cameras, spyware, use of facial recognition, and the advent of artificial intelligence.[13]

This long-lasting transatlantic discrepancy in the handling of and access to personal data has a strong impact on international business. Besides the fact that the EU as well as US are eager to find a long-lasting and amicable solution at a political level, and even with the newly enacted EU-US Data Privacy Framework now in place, uncertainty for companies remains which demands for self-independent solutions.

1.1. Scope and limitations

This master thesis clarifies the requirements of data transfers from the EU to the US for companies based on the current relevant transatlantic legal framework and intents to provide options for data exporters on how to legally and securely transfer data. It focuses on the US governmental access to electronically held personal data in view of relevant federal US regulations and provides solution approaches for those businesses affected by both regimes.

The assessment is based on the testing criteria provided by the European Data Protection Board (EDPB) in its recommendations on supplement transfer tools and the European Essential Guarantees (EEG) for surveillance measures.[14]

1.2. Research questions

This master thesis assesses whether and how data exporters are able to have a legally compliant course of action for a transfer of personal data to the US without the reliance on a US adequacy decision.

The following questions form the scope of this master thesis:

[13] *Guardian*, Edward Snowden says surveillance technology is more intrusive than ever.
[14] EDPB, Recommendations 01/2020[2]; EDPB, Recommendations 02/2020.

1. Is it possible to be legally compliant with GDPR as a data exporter who is directly or indirectly through its data importer subject to US governmental access requests to electronically held personal data?

    a. If so, in what legal and/or technical form?

    b. If not, what needs to be implemented by affected companies in order to obtain exemption from or mitigation of liability?

2. What can be done on the governmental side to provide legal certainty to affected businesses?

2. Data transfer mechanisms from the Union to the US

Any transfer of personal data from the Union[15] to the US is only allowed if all general provisions of GDPR are fulfilled and specific conditions for personal data transfers to third countries regulated in Chapter V GDPR (Art 45–50 GDPR) are met. This means that the precondition for any data transfer is the general compliance laid out in Art 5 et seq GDPR, including having a legal basis in accordance with Art 6 and 9 GDPR for each processing purpose as well as in case of outsourced data processing, the special data processor regulations under Art 28 GDPR. Only after a legitimate processing, transfer mechanisms and underlying requirements laid out in Chapter V GDPR may authorize a valid transfer.[16]

Since the GDPR does not define what a "*transfer of personal data to a third country"* entails, the EDPB issued guidelines for what qualifies as a transfer and identified three cumulative criteria: first, a controller or processor transferring data (data exporter) must be subject to GDPR; second, the exporter discloses or makes personal data available to another controller or processor (importer); which third, is in a third country.[17]

That means that GDPR including Chapter V also applies to controllers or processors already based in the US or any other third country, which meet Art 3 (2) GDPR requirements e.g., by offering goods or services to data subjects in the Union or monitoring data subject's behavior. For these cases, the specific transfer requirements, such as evaluating the risks of a data processing outside the Union, must already be assessed as part of controller's general due diligence under GDPR, since there is no direct applicability of Chapter V GDPR requirements.[18]

Under Chapter V, GDPR recognizes several transfer mechanisms laid out in Art 45 et seq GDPR. Based on the specific circumstances, data exporters must decide under which mechanism the transfer should take place. The most convenient and therefore important transfer mechanism for data exporters is a transfer based on an adequacy decision

[15] In accordance with the EEA Agreement, "Union" in the context of GDPR includes the EEA States Iceland, Liechtenstein and Norway; Decision of the EEA Joint Committee 154/2018 of July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], OJ L 183/23 (July 19, 2018).
[16] Rec 101, Art 44 GDPR; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 13 in Art 44 GDPR; *Feiler/Forgó*, EU-DSGVO Kurzkommentar (2017) Rec 5 in Art 44 GDPR.
[17] *EDPB*, Guidelines 05/2021[2] Rec 7, 9.
[18] *EDPB*, Guidelines 05/2021[2] Rec 13, 31.

(Art 45 GDPR) by the European Commission (EC). In the absence of such a decision, appropriate safeguards as stated in Art 46 GDPR, or a transfer based on an international agreement (Art 48 GDPR) may apply. In case of appropriate safeguards, the EDPB issued a six-step roadmap recommendation in accordance with the *Schrems II* and based on the principle of accountability how to assess whether and what kind of supplementary measures should be implemented to ensure compliance. Lastly, in case no appropriate safeguards are available, a data exporter may be able to transfer personal data based on derogations outlined in Art 49 GDPR on an exceptional basis.[19]

The data exporter must record and map the data transfer in accordance with its obligations of establishing a record of processing activities under Art 30 GDPR (ROPA) and its obligations of informing data subjects about the transfer under Art 13 (1) (f) and Art 14 (1) (f) GDPR including any onwards transfers. Furthermore, data minimization must be ensured.[20]

Common use cases of personal data sharing between EU and US businesses are either intracompany group related due to an international group company structure which includes the sharing and analyzing of human resource (HR), customer, and vendor data as well as any content and aggregated data from its own offerings. Or alternatively through business engagements with international customers or more importantly vendors for outsourced services such as (digital) infrastructure provision and maintenance, data aggregation or services to enhance business flexibility and value.

Unless the new processing is based on consent or Union or member state law, any change in the purpose of processing for which personal data have initially been collected must be assessed to ascertain whether the new purpose is compatible with the initial one.[21] For example, access to or disclosure of personal data for law enforcement or national security purposes by US governmental agencies is a separate processing purposes and requires a legal basis under GDPR. In most cases, this reflects an onward transfer, because it is not the initial purpose of processing at the time of data collection. In 2019, the EDPB stated that a lawful processing based on a CLOUD Act warrant can only be ascertained if the transfer is legitimized by an international agreement according to Art 6 (1) (c) and

[19] *EDPB*, Recommendations 01/2020[2] Rec 14-27; see *infra* 2.1 for adequacy decision, 2.2 for appropriate safeguards, 2.3 for international treaties and 2.4 for derogations.
[20] *EDPB*, Recommendations 01/2020[2] Rec 8-13.
[21] Rec 50, Art 6 (4) GDPR.

Art 48 GDPR or if necessary to protect the vital interests of an individual based on Art 6 (1) (d) and Art 49 (1) (f) GDPR. With an updated legal landscape around limitations and redress option regarding national security purposes on the US side and the EU-US Data Privacy Framework adequacy decision (DPF)[22] in place since July 2023, it will further be assessed whether the EDPB's outcome still applies.[23]

GDPR imposes high fines for non-compliance. Infringements related to the transfer of personal data to a recipient in a third country pursuant to Art 44 to 49 GDPR are subject to administrative fines up to EUR 20 Mio. or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Furthermore, data subjects have the right to an effective judicial remedy in case their rights under GDPR have been infringed due to non-compliance with GDPR and have a right of compensation for damages caused by a GDPR infringement.[24]

The following sub-chapters assess which transfer tools are provided under GDPR and which ones might be a feasible legal basis for data exporters transferring data to US data importers.

2.1. Adequacy decision (Art 45 GDPR)

Adequacy decisions are issued by the EC for a specific country or region, when it has decided that this third country provides an adequate level of protection by assessing its laws, effective and enforceable privacy rights as well as remedies and independence of supervisory authorities.[25] Once an adequacy decision is in place, data transfers do not need any additional authorization or safeguards and the data exporter can treat the data transfer in the same way as if such transfer would be within the Union.[26]

Prior to the current framework, the EC had already issued two adequacy decisions for the US: the Safe Harbor adequacy decision (Safe Harbor)[27] between the year 2000 until 2015

[22] Commission Implementing Decision (EU) C(2023) 4745 final of July 10 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.
[23] *EDPB*, Impact of US CLOUD Act Annex, p 4, 7, 8.
[24] Art 79, Art 82 (1) and (2), Art 83 (5) (c) in accordance with Art 44-49 GDPR.
[25] Art 45 (1) and (2) GDPR.
[26] Second sentence of Art 45 (1) GDPR.
[27] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce, OJ L 215/7 (Aug. 28, 2000).

and the EU-US Privacy Shield adequacy decision (EU-US Privacy Shield)[28] between 2016 and 2022. Both decisions were not issued for the entire US but based on a self-certification system by enrolled US organizations overseen by the US Department of Commerce (DoC).[29]

The Safe Harbor Privacy Principles, issued by the DoC on 21 July 2000 were considered to ensure an adequate level of personal data protection transferred from the Union to organizations established in the US which enlisted themselves in the program. Even though the Article 29 Data Protection Working Party (Art 29 WP) raised concerns due to the continually extended US surveillance provisions, especially in light of the 9/11 terrorist attacks and the thereafter enacted Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) in 2001[30] (including section 215) and the later with Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISAAA)[31] ratified FISA 702 provision, data privacy was still considered adequate under Safe Harbor. When the former United States National Security Agency (NSA) employee and whistleblower Edward Snowden revealed US governments' actual data handling procedures in 2013, the attitude changed on EU side.[32]

Back in 2013, Maximilian Schrems was the first who challenged US surveillance practices by questioning whether transferred personal data have adequate protection in the US. In the 2015 CJEU's judgement *Schrems I*, the court agreed with Schrems' allegations and invalidated EC's Safe Harbor adequacy decision based on unproportional US mass surveillance practices.[33]

Soon thereafter in 2016, the EC and US negotiated a new adequacy framework, the EU-US Privacy Shield, based on the same principles as Safe Harbor, which again raised concerns

[28] 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, OJ L 207/1 (Aug. 1, 2016), EC C 2016/4176.
[29] Safe Harbour 2000/520/EC Art 1-3; EU-US Privacy Shield EC (EU) 2016/1250 Rec 14-18.
[30] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. 107–56, 115 Stat. 272 (Oct. 26, 2001) <congress.gov/107/plaws/publ56/PLAW-107publ56.pdf> (last retrieved Aug. 13, 2023).
[31] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110–261, 122 Stat. 2436 (July 10, 2008) <govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf> (last retrieved Aug. 13, 2023).
[32] *Art 29 WP*, WP15, p 2; *Schwartz*, Legal Access to the Global Cloud p 1691.
[33] C-362/14 (*Schrems I*), Rec 97-98.

by privacy advocates as well as the Art 29 WP and was another time challenged in front of the CJEU. 2020 in *Schrems II*, the court ruled that the EC's EU-US Privacy Shield adequacy decision is not sufficient to protect the high standards of data protection laid out in Art 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (the Charter)[34] based on the finding that US surveillance laws, specifically FISA 702 and EO 12333, have no reasonable limitation and allow bulk data collection of data subjects without any proportionality. Additionally, targeted data subjects under such US surveillance programs have no effective remedy before a tribunal and hence no effective judicial protection of its fundamental rights.[35]

In a further attempt on December 13, 2022, followed by US President Biden's release of EO 14086[36], the EC started the process to adopt a new adequacy decision for the US and published the draft adequacy decision for the EU-US Data Privacy Framework (Draft DPF)[37] for general review and comments.[38] The European Parliament's Committee on Civil Liberties, Justice and Home Affairs advised the EC not to adopt the Draft DPF and raised a number of concerns by its determination is that the drafted framework fails to create an adequate level of protection required by GDPR and the Charter.[39] The EDPB, while welcoming the updates made to the new framework, states in its opinion, that the principles laid out under the new program are essentially the same as those in the Privacy Shield and among other areas of improvement, is looking for a better understanding of applicable US law and its effect on self-certified companies.[40]

Regardless of raised concerns, the final DPF adequacy decision entered into force on July 11, 2023. As comparison, under Safe Habor as well as the EU-US Privacy Shield, about 5,000 US companies were certified. All 2620 active EU-US Privacy Shield certifications

[34] Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ L 326/391 (Oct. 26, 2012).
[35] *Art 29 WP*, WP238 p 5; *Anderl/Tlapak*, Erleichterung für US-Datentransfer; *Feiler*, Datenschutz: Ein Schild, der keine Deckung gibt; *Kristoferitsch/Stangl*, Brüchiger Datenschild; C-311/18 (*Schrems II*) Rec 171 et seq, 186 et seq.
[36] Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities, 87 Fed. Reg. 62,283 (Oct. 14, 2022) <federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities> (last retrieved Aug. 13, 2023).
[37] Draft 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 (Dec. 13, 2022) <commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en> (last retrieved Aug. 13, 2023).
[38] *EC*, Commission starts process to adopt adequacy decision for safe data flows with the US.
[39] *Committee on Civil Liberties, Justice and Home Affairs*, Draft motion EP resolution on the EU-US Data Privacy Framework, Rec 10-11.
[40] *EDPB*, Opinion 05/2023 Rec 21-39.

at the time of the enforcement of the DPF were automatically transferred to the new program. Companies are provided with a three-month period to adjust their policies to the new framework or withdraw if they do not want to participate.[41]

The DPF is substantially similar or in parts even identical with EU-US Privacy Shield in the privacy principles and the arbitral model provisions for participating US companies, the underlying legal US framework regarding EO 12333, FISA and the ECPA, the general redress and oversight options for affected individuals and the sectorial application of the DPF to only self-certified US companies.[42] Further, the DPF is still preempted by any US national security and law enforcement requests and releases US companies from their notification requirements to individuals in case of law enforcement and national security requests. The US Department of Justice (DoJ) furthermore emphasizes that the DPF is *"unrelated to, and unaffected by, the CLOUD Act"*.[43]

The new framework materially differentiates from its predecessor by its adoption of EO 14086 and its introduction of new redress and oversight mechanisms for EU data subjects and a more granular lay out of national security principles and their limitations. Formally, it provides a much more detailed breakdown and analysis of US federal law enforcement and national security regulations.[44]

Based on the *Schrems II* assessment, the changes from the EU-US Privacy Shiels to the DPF can be briefly summarized and evaluated as follows: First, the CJEU addressed bulk collection of non-US citizens' data under FISA 702 and EO 12333 as unproportionate, which to this day hasn't changed. The programs thereunder are authorized by the Foreign Intelligence Surveillance Court (FISC) based on an annual certification and not an individual assessment. New under the DPF, EO 14086 restricts such bulk collection to general legitimate objectives, however, allows bulk collection based on classified

[41] EU-US Data Privacy Framework (EU) C(2023) 4745, p 1, 64, *DoC*, EU-U.S. & Swiss-U.S. Privacy Shield; *DoC*, Data Privacy Framework Program FAQs (EU-U.S. DPF), Q3; *Whistic*, Whats the Difference Between Privacy Shield and Safe Harbor?; *Hengesbaugh*, What Privacy Shield organizations should do in the wake of 'Schrems II'.
[42] See framework principles: EU-US Data Privacy Framework (EU) C(2023) 4745, Annex I; and EU-US Privacy Shield EC (EU) 2016/1250, p 48-70; *DoC*, Data Privacy Framework Program FAQs (EU-U.S. DPF), Q2 2nd bullet point; *Hansch*, Der Entwurf eines Angemessenheitsbeschlusses für den US-EU-Datentransfer, p 22; EDPB, Opinion 05/2023 Rec 35.
[43] EU-US Data Privacy Framework (EU) C(2023) 4745, Annex I I.5, II. I. xii and 16. c.; *DoC*, Data Privacy Framework Program FAQs (General), Q2.
[44] See *infra* 3.2.2. and 3.2.4 for more details and assessment on EO 14086; EU-US Data Privacy Framework (EU) C(2023) 4745 Rec 88-200; in comparison see, EU-US Privacy Shield EC (EU) 2016/1250 Rec 64-135.

objectives if needed as well. Neither the DPF nor EO 14086 provides a clear definition of proportionality or how it will be assessed above the general objective that signal intelligence activities shall be *"proportionate to the validated intelligence priority"* and *"aim to achieve a proper balance".* Consequently, no material changes have been made in the DPF to the critiqued US regulations. Whether the US assesses the new proportionality principle equivalent to EU standards cannot be assessed based on EO 14086 or the DPF language, and so far no jurisdictional reference can be made either.[45]

Further, EU-US Privacy Shield did not provide sufficient effective and enforceable rights for affected data subjects. EO 14086 implemented an entitlement by covering any type of US intelligence activity where data subjects can submit qualifying complaints to the Office of the Director of National Intelligence Civil Liberties and Privacy Office (CLPO) and obtain a review of CLPO's decision by the Data Protection Review Court (DPRC). The implemented "right to review", however, does not encompass the right of access but only a classified right of rectification or deletion in case of a violation. It thus does not give data subjects a clear and actionable right against US authorities but only a review mechanism. Under strict circumstances the CJEU sees a classified review as justifiable in certain circumstances if necessary and proportionate to the purpose. If the purpose is unproportionate bulk collection, a valid basis is in my opinion missing to justify non-disclosure restrictions.[46]

Lastly, the oversight mechanism must be an independent and impartial tribunal which were not granted under the EU-US Privacy Shield's establishment of the ombudsperson mechanism. EO 14086 introduced the DPRC as an independent oversight panel over intelligence activities with the power to make binding decisions upon the Intelligence Community (IC). The DPRC is established within the DoJ and appointed by the AG but is not incorporated in the day-to-day supervision of the AG or may be removed or punished due to their DPRC's service. The European Court of Human Rights (ECtHR) emphasized its preferences for a judge as independent tribunal, however, clarifies that oversight may be established within the executive as long as independence means sufficiently independent from the executive branch and the authorities carrying out the surveillance. Whether the

[45] C-311/18 (*Schrems II*) Rec 178-180, 183-185; EO 14086 Sec 2. (a) (ii) (B), Sec 2. (b); *Hansch*, Der Entwurf eines Angemessenheitsbeschlusses für den US-EU-Datentransfer, p 23.
[46] C-311/18 (*Schrems II*) Rec 181-182, 186-192; EO 14086 Sec 3., 5.(h), 28 CFR Part 201; see *infra* 3.2.2.4 and 3.2.4.

newly established DPRC is independent in view of EU standards is in my opinion a question of how it is lived in practice and if the AG will treat the DPRC as truly independent.[47]

What speaks for the new DPF is the political motivation to secure the biggest common economy in the world and the commitment on EU and US side to find mutual ground. This can be seen in the now much more thorough analysis of each other's legal framework laid out in the DPF and the Attorney General's *"Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086"*. The further specifications and limits for signals intelligence activities set out in EO 14086 are more concrete and detailed and make bulk collection more justifiable and narrower than before. It further provides data subjects with enforceable rights via the qualifying complaint process and an additional oversight mechanism.[48]

Regardless of political endeavors, courts and oversight authorities have the obligation to review legal compliance without any political or commercial considerations. Main concerns regarding the DPF are that there are no material changes in US surveillance laws which have already been ruled to be unproportionate, whether the new US necessity and proportionality considerations in EO 14086 are in practice equivalent to EU standards, if the new oversight mechanism can be seen as independent in view of EU standards and whether the new redress mechanism will provide effective measures for data subjects in practice.[49]

Whether the DPF is a long-term reliable transfer mechanism to the US remains in my point of view very critical due to the fact that the decision is more politically driven than legally. The underlying US surveillance laws have so far not changed. Especially the lack of transparency of surveillance rules and the unproportionate (bulk) and unjustifiable difference of surveillance measures between US and non-US citizens do not outweigh newly implemented and in some parts fairly untransparent redress and oversight

[47] C-311/18 (*Schrems II*) Rec 193-197; EO 14086 Sec 4., 28 CFR Part 201; see *infra* 3.2.2.3 and 3.2.4; *EDPB*, Recommendations 02/2020 Rec 42.
[48] EU-US Data Privacy Framework (EU) C(2023) 4745 Rec 88-200; *DoJ*, AG Memorandum Qualifying States Under EO 14086; *Bryant*, EU-US Data Privacy Framework adopted, what now?; *Kerry*, Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?.
[49] DSB-D155.026 (Google Analytics II) D.1 d); Noyb, New Trans-Atlantic Data Privacy Framework; *Hansch*, Der Entwurf eines Angemessenheitsbeschlusses für den US-EU-Datentransfer, p 23; *Strassemeyer*, Vorhang auf für das Trans-Atlantic Data Privacy Framework, p 187; see also *infra* 3.2.4.

mechanisms on US side. Consequently, based on current information and a sole legal assessment, the DPF should in my view not uphold in front of the CJEU. A big decisive factor in my view, however, will be how the new framework is lived by the US in practice and whether enough information will be shared with the EU and public to be able to sufficiently assess actual US surveillance practices.[50]

Based on raised concerns stated above and the announcement of NOYB – European Center for Digital Rights, the privacy organization around Maximilian Schrems, to actively challenge the DPF, it is advisable for data exporters engaging with US data importers, not to solely rely on the DPF yet until its adequacy is confirmed by the CJEU. For easily replaceable short-term engagements the adequacy decision provides a valid standalone basis. However, for example, using the DPF for intracompany transfers or complex technical implementations might lead to the risk of immediately stopping not only the data transfer but the entire underlying data processing in case of an invalidation. It will further remain seen how many US companies are willing to enter and abide by the new program.[51]

2.2. Appropriate safeguards (Art 46 GDPR)

Even though an adequacy decision for the US is in place, it might not be a reliable tool for long term cooperations in case the decision gets challenged and overruled by the CJEU again. Also, data exporters may want to engage with US data importers not participating in the DPF. In any case, a data transfer may still be permissible provided that neither the Union nor member states law impose any limits, the data exporter ensures appropriate safeguards, guarantees the availability of enforceable data subject rights and effective legal remedies for data subjects appropriate to a processing within the Union.[52]

"Appropriate" in this context means according to *Schrems II "a level of protection essentially equivalent to that which is guaranteed within the European Union*"[53], which must be guaranteed by the data exporter and assessed in collaboration with the data importer on a case-by-case basis in a transfer impact assessment (TIA). In case the outcome shows that the transfer tool cannot to ensure an essentially equal level of protection in

[50] In analogy see *infra* 3.2.4. regarding the overall assessment for data exporters using appropriate safeguards.
[51] *Noyb*, Data Transfers; Noyb, New Trans-Atlantic Data Privacy Framework.
[52] Rec 108, third sentence 112, Art 46 (1), Art 49 (5) GDPR.
[53] C-311/18 (*Schrems II*) Rec 96.

practice, it must be accompanied by additional safeguards, namely supplementary measures, to the ones laid out in Art 46 GDPR.[54]

Art 46 GDPR transfer tools are distinguished between those which do not require a specific authorization prior use (par 2) and those which are subject to a pre-authorization from a supervisory authority (par 3). Regardless of the specific tool set out in Art 46 GDPR, the requirements stipulated by *Schrems II* for SCCs are applicable to all Art 46 GDPR tools due to their common contractual nature.[55]

2.2.1. Legally binding and enforceable instruments between public authorities (Art 46 (2) (a) GDPR)

This mechanism refers to data transfers between public authorities in the Union and third countries if GDPR applies to such processing. For example, public and state security as well as law enforcement matters are excluded from the material scope of GDPR. Art 46 (2) (a) GDPR requires a legally binding document, which must include data protection principles, data subject rights, appropriate safeguards, and a redress mechanism. If not legally binding, Art 46 (3) (b) GDPR instead applies. Since transfers from a public authority to a private entity or a transfer between private entities are also not encompassed by this provision, is not an appropriate tool for businesses transferring data to the US.[56]

2.2.2. Binding corporate rules (Art 46 (2) (b) and 47 GDPR)

Binding corporate rules (BCRs) are legally binding contractual policies for a group of undertakings or enterprises engaged in a joint economic activity, which must include general data protection principles and enforceable rights for data subjects for the transfer of personal data between controllers or processors located within the Union pursuant to Art 3 GDPR and controllers or processors located in a third country.[57]

BCRs require the preapproval of a competent data protection authority, the lead supervisory authority (SA), based on the consistency mechanism to ensure alignment with other supervisory authorities. The data exporter must therefore apply and provide all necessary information to the lead SA. For every BCR application, the EDPB provides its opinion.

[54] *EDPB*, Recommendations 01/2020[2] Rec 21-23; C-311/18 (*Schrems II*) Rec 131-134; Rec 108, 114, Art 46 (1) GDPR.
[55] *EDPB*, Recommendations 01/2020[2] Rec 22.
[56] *Knyrim* in *Knyrim*, DatKomm (2018) Rec 15-17 in Art 48 DSGVO; *EDPB*, Guidelines 02/2020[2] Rec 1, 4, 12, 17, 66, last sentence of 108; Art 2 (2), 46 (2) (a) GDPR.
[57] Rec 108, 110, Art 4 (19), (20), 47 GDPR.

The BCR assessment is based on the submitted policy and does not include a validation whether the general data processing principles are met for any specific processing activities, whether implemented safeguards are appropriate, or if any other (legal) requirements are met. Additionally, in case a transfer is based on a controller to processor relation, the data exporter must ensure compliance with Art 28 GDPR requirements. That means an additional data processing agreement or other legal act must be put in place for the specific processing.[58]

Once approved, BCRs can be used for all transfers within the group. All approved BCRs must be in line with the up-to-date requirements set out by the EDPB, which needs to be assessed by the data exporter. So far, 49 BCRs are currently authorized under GDPR. Under the Data Privacy Directive[59], more than 130 BCRs were approved.[60]

BCRs are most appropriate for close, long-term cooperations, such as an international group companies, which have constant data sharing. Since the BCR approval only provides the transfer basis, it still requires a case-by-case analysis whether the specific transfer does not undermine the level of protection guaranteed under GDPR. Consequently, if BCRs are intended to be used as valid transfer mechanism to the US, a TIA and potentially other safeguards must be implemented and accompany the BCRs due to its contractual nature.[61]

2.2.3. Standard contractual clauses (Art 46 (2) (c) and (d) GDPR)

Standard contractual clauses (SCCs) are formally authorized contract templates either issued by the EC with an implementing decision (lit c) or issued by a supervisory authority and adopted by the EC (lit d). SCCs can be used by data exporters as transfer tool without additional authorization by a supervisory authority.[62]

Whether SCCs are a valid transfer mechanism to the US was also part of the *Schrems II* ruling. The CJEU held that the EC SCC decision for the transfer of personal data to

[58] *EDPB*, Recommendations 01/2022 Sec 1.5, 1.8-1.12, 2.4; Art 28 (3), 47, 56 (1), 57 (1) (s), 58 (3) (j), 63, 64 (1) (f) GDPR.
[59] 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, OJ L 281/31 (Nov. 23, 1995).
[60] *EDPB*, Recommendations 01/2022 Sec 1.13; *EDPB*, Approved Binding Corporate Rules; *EDPB*, Pre-GDPR BCRs overview list.
[61] Art 44 GDPR.
[62] Art 46 (2) (c) and (d) GDPR.

processors (SCC C2P 2010)[63] is per se a valid transfer mechanism in absence of an adequacy decision, however, emphasized that the controller or processor transferring personal data to a third country is responsible to provide appropriate safeguards, enforceable rights and effective legal remedies for data subjects and must include, if necessary, additional safeguards in whichever form feasible, to guarantee these rights under the execution of SCCs.[64]

Based on the CJEU's guidance, the EC issued new SCCs for international data transfers between data exporters and data importers (SCC Int transfer 2021)[65] as well as SCCs between controllers and processors under Art 28 GDPR (SCC C2P 2021)[66] to ensure alignment with *Schrems II* and to guarantee a continuous high-level protection of this transfer tool. The EC emphasizes that the new set of SCCs are not supposed to be used as data transfer tool in case GDPR is already applicable for both the controller and processor under Art 3 GDPR in order to not duplicate GDPR obligations. For such circumstances, the EC is in the process of drafting separate SCCs.[67]

The new SCCs key changes require the contracting parties to warrant an adequate protection of personal data and require a TIA including clear documentation of the outcome of the assessed circumstances of the specific transfer. Such TIA must ensure that a transfer only takes place in case the laws and practices of the US do not contradict with the obligations outlined in the SCCs.[68]

Furthermore, the data importer must notify the data exporter and data subjects, if possible, of any legally binding requests it receives from US governmental entities or if it becomes aware of any direct access by a US public authority. Where the data importer is prohibited

[63] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39/5 (Feb. 12, 2010), as amended by Commission Implementing Decision (EU)2016/2297, OJ L 344/100 (Dec. 16, 2016).
[64] C-311/18 (*Schrems II*) Rec 131 et seq; Art 46 (1) GDPR.
[65] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199/31 (June 7, 2021).
[66] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, OJ L 199/18 (June 7, 2021).
[67] *EC*, The New Standard Contractual Clauses – Q&A p 13 et seq; SCC Int transfer 2021 EC (EU) 2021/914, Rec 1, 6.
[68] SCC Int transfer 2021 EC (EU) 2021/914 Rec 16-22, Annex Clause 14, 15.

from informing about the received disclosure request, for example when receiving a National Security Letter (NSL) or warrant which includes an order to restrict disclosure, the data importer must do all in its power to bring the data exporter and/or the data subject in the position to take appropriate action to safeguard personal data by providing either a general statement that the data importer is unable to comply with its contractual obligations set out in the SCC or where possible provide any legally permissible information about the request. It is further required to review and if possible, challenge the request before disclosing any sought personal data.[69]

SCCs can be challenged any time by the supervisory authority, especially when there is no appropriate documentation of the TIA in place. *Schrems I* further clarified that Union member states have independent control to oversee and, if necessary, order a suspension of international data transfers – even though based on an EC' adequacy decision. Accordingly, the EC emphasized supervisory authorities' power in its new SCCs.[70]

In a recent 2023 case, the Ireland's Data Protection Commission suspended Meta's data transfers based on EDPB's binding decision by ceasing processing and storing of personal data in the US within six months and fined Meta with a record sum of EUR 1.2 billion. This is based on its findings that US law does not provide an equivalent level of protection, and the SCCs including supplemental measures cannot compensate for such inadequate protection. Additionally, the Irish authority declared that no derogations according to Art 49 GDPR are justified and cannot be relied upon for the underlying transfer.[71]

Similar outcomes occurred around NOYB's targeted complaint endeavor *"101 complaints"* against the use of SCCs for Google Analytics and Facebook Business Tools by several companies in the Union. Among others, the Austrian Data Protection Authority (DPA) ruled in *Google Analytics I*[72] and *Google Analytics II*[73] that SCCs do not provide an adequate level of protection because the data importer (Google) is per definition an electronic communication service provider under FISA and hence falls under US

[69] See *infra* 3.1.1.6 and 3.1.1.7 for further details on NSLs and warrants; SCC Int transfer 2021 EC (EU) 2021/914 Annex Clause 14 (f), 15.1 (b), (e), 15.2 (a), 16 (a).
[70] SCC Int transfer 2021 EC (EU) 2021/914 Art 2; SCC C2C 2001 2001/497/EC and SCC C2P 2010 EC 2010/87/EU as amended by EC (EU) 2016/2297 Rec 3-4; C-362/14 (*Schrems I)* Rec 101, 103.
[71] *Data Protection Commission*, Decision DPC Inquiry Reference: IN-20-8-1 in the matter of Meta Platforms Ireland Limited (May 12, 2023) Sec 10.1-10.3; *Bracy*, *EDPB*, Binding Decision 01/2023; Meta fined GDPR-record 1.2 billion euros in data transfer case.
[72] DSB-D155.027 (*Google Analytics I*) Ruling 2.b).
[73] DSB-D155.026 (*Google Analytics II*) Ruling 2.b).

surveillance measures which requires the implementation of effective supplementary measures. The implemented supplementary measures, however, were not effective to remove access and disclosure possibilities to personal data by US authorities and were therefore unable to ensure an adequate level of data protection. The Swedish Authority for Privacy Protection (IMY) audited CDON, Coop, Dagens Industri and Tele2 how they transferred data to the US using Google Analytics based on SCCs and came to the same conclusion that the implemented supplemental measures were insufficient.[74]

Besides adequacy decisions, SCCs are the most important transfer mechanism for data exporters based on its ready-to-use approach. The new requirements set a higher bar on compliance for both data exporters and data importers. Data exporters intending to use SCCs as legal transfer basis must therefore calculate more time to assess its legitimacy. The above examples clearly show that SCCs are nowadays under very close scrutiny and should be assessed and monitored diligently by data exporters.

2.2.4. Code of conducts (Art 46 (2) (e) and 40 GDPR)

Codes of Conduct (CoC) are sets of specific rules and policies approved by a competent supervisory authority, mostly used by a sector or categories of companies which set out specific processing characteristics for a certain sector. While CoCs are primarily used for national (one member state) or transnational (several member states) data transfers, it may also be used as an appropriate safeguard tool for international data transfers once adopted and approved by the EC by giving them a general validity within the entire Union. Only those CoCs can be used as a valid basis for data transfers.[75]

Using CoCs as a basis for international data transfers would require the same principles and standards as applicable for any other transfer tool under Art 46 GDPR. This also includes adhering to *Schrems II* requirements due to its contractual nature.[76] So far, the EC has not issued an implementing act to grant a CoC validity in the entire Union and therefore shouldn't be considered by data exporters in need of a timely solution.

[74] *EDPB*, Report 101 Task Force p 3; *IMY*, Four companies must stop using Google Analytics.
[75] *EDPB*, Guidelines 04/2021[2] Rec 20-23; Rec 98, 99, Art 40, 46 (e) GDPR.
[76] *Bayrische LB Datenschutz*, Internationale Datentransfers Rec 104, 106.

2.2.5. Certification mechanism (Art 46 (2) (f) and 42 GDPR)

The primary goal of such certifications is the enhancement of transparency and includes data protection seals and marks, which should provide an easy way to assess if data importers meet the appropriate level of data protection. The certification mechanism does not require a separate authorization by a supervisory authority for a data transfer when used together with binding and enforceable commitments of the data importer to implement appropriate safeguards and data subject rights. The specific criteria and certification body must be approved by the SA in consultation with the EDPB. It underlies the same scrutiny as any other Art 46 GDPR tool and does not relive the data exporter of its responsibilities to ensure adequate data protection for the transfer.[77]

The *Centre for Information Policy Leadership* stresses the importance of certification mechanisms and encourages the EC and EDPB to make it a priority in developing an EU-wide GDPR certification for data transfers. These should also interact with BCRs and adequacy decisions.[78] To my knowledge, there hasn't been any approved certification mechanisms so far, which makes it therefore not an appropriate tool to consider for businesses transferring data to the US.

2.2.6. Appropriate safeguards with prior authorization (Art 46 (3) GDPR)

Appropriate safeguards, which require prior authorization of the supervisory authority are limited to contractual clauses between data exporters and importers and administrative arrangements between public authorities. The difference between contractual clauses and SCCs is that contractual clauses are individual contracts between the parties and need to be assessed and approved on a case-by-case basis. The difference between Art 46 (2) (a) GDPR tool and administrative arrangements under Art 46 (3) GDPR is that the latter is not a legally binding instrument and therefore requires a case-by-case assessment and approval by the supervisory authority. Any approval under Art 46 (3) GDPR shall be made in accordance with the consistency mechanism to ensure a uniform application in the Union.[79]

[77] *Knyrim* in *Knyrim*, DatKomm (2018) Rec 65-67 in Art 46 GDPR; *EDPB*, Guidelines 07/2022[2] Rec 19-23; Rec 100, Art 42, 43, 46 (2) (f) GDPR.
[78] *Centre for Information Policy Leadership*, GDPR Implementation Project April 2017 p 2.
[79] *Knyrim* in *Knyrim*, DatKomm (2018) Rec 68-79 in Art 46 GDPR; Rec 135, Art 46 (3) and (4), 63 GDPR.

As mentioned above, administrative arrangements are not applicable for private businesses. The use of contractual clauses with prior authorization should in my opinion not be envisaged by data exporters. The case-by-case assessment by supervisory authorities may be lengthy and uncertain in the outcome.

2.3. Transfer based on international treaties (Art 48 GDPR)

Art 48 GDPR limits the recognition and enforceability of a third country's court judgement or decision of an administrative authority requesting data exporter's disclosure and transfer personal data to only those case where an international agreement between the requesting third country and the Union or a member state is in place. It clarifies that decisions from a third country authority are not legitimate grounds for data transfers. There must be an international treaty, such as a Mutual Legal Assistance Treaty (MLAT), in place, otherwise the disclosure has to follow the same Chapter V GDPR requirements as any other transfer.[80]

This provision directly addresses the extraterritorial reach of laws such as FISA and the CLOUD Act and causes conflict for controllers and processors falling under Union and US jurisdiction if an US access request is not based on an international treaty. Rec 115 GDPR states that any foreign law directly regulating the processing of personal data and not based on an international agreement may violate the protection of data subjects granted under GDPR and only transfers in accordance with GDPR should be allowed.[81]

MLATs are international bilateral treaties between two specific countries and govern the assistance of foreign countries for any criminal law enforcement activity against US or non-US persons outside the US. They require the foreign country to cooperate with and provide sought data to the US law enforcement under its own domestic law principles. MLATs honor the sovereignty of each country by seeking a cooperation mechanism between two countries for evidence collection. The foreign country processes every request under its own domestic law, and only in cases where the request fulfils domestic legal requirements and process to obtain such information, does the foreign country authorize a disclosure. As of April 2022, the US has MLATs with 76 countries, including Austria. In 2016, the US and EU signed an umbrella agreement[82] including common principles which acts as

[80] *Knyrim* in *Knyrim*, DatKomm (2018) Rec 1 and 10 in Art 48 GDPR; *EDPB*, Guidelines 02/2018 p 5; Rec 102, 115, Art 48, GDPR.
[81] Rec 115 GDPR; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 13 and 14 in Art 48 GDPR.
[82] Council Decision (EU) 2016/2220 of December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection

framework for a facilitated cooperation between competent authorities of the EU and US in criminal investigation cooperation matters, including terrorism. The treaty, however, clearly states that the agreement itself cannot be used as legal basis for a data transfer.[83]

Even though US surveillance laws have a far extraterritorial reach, MLATs are still a fundamental part of the law enforcement process to obtain sought information since MLATs cover any type of evidence. For example, the Stored Communications Act (SCA) clearly defines which type of data can be requested thereunder, the MLAT system in contrast has no such limitation. If a service provider falls under the definition of the SCA and gathers customer information for its own purpose such as for user profiles, the service provider is not acting as an ECS or RCS under the SCA and therefore the SCA is not applicable for a law enforcement information request.[84]

Due to its dual approval process the MLAT system provides robust and fair means to obtain sought data. It is, however, very much criticized for its long and burdensome process and also requires law enforcement to locate sought data to a specific country, which in some instances is not possible due to, e.g., a decentralized cloud storage solution. The increase in MLAT requests is a huge administrative burden for law enforcement and very often a hinderance in a fast-paced data driven world. Since so many cloud service providers are based in the US, the MLAT system leads to many frustrations for US law enforcement due to the vast number of requests to sought data from foreign countries.[85]

2.4. Derogations for specific purposes (Art 49 GDPR)

The last resort when it comes to a permissible data transfer are the eight derogations under Art 49 GDPR, assessed in this subchapter. These are exceptional circumstances for which a data transfer may still occur in case there is neither an adequacy decision nor appropriate safeguards in place. The fallback to derogations must meet strict conditions to ensure that

of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336/1 (Dec. 10, 2016).

[83] *Schwartz*, Legal Access to the Global Cloud, p 1720 et seq.; *EC*, Joint EU-U.S. press statement; *DoJ*, Mutual Legal Assistance Treaties of the United States.

[84] *Schwartz*, Legal Access to the Global Cloud p 1720 et seq, for further details on the ECPA applicability see *infra* 3.1.2; note that this example does not include national security, since a different provider definition is used, see *infra* 3.1.1.

[85] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3] Ch 13.3.8.

fundamental rights including Chapter V GDPR requirements are neither breached nor circumvented. In addition, EU or member state law can limit transfers.[86]

The scope and use cases of some derogations are controversial. While the EDPB follows a very strict approach in applying derogations, there are more open opinions in the literature. Art 49 (1) GDPR states that derogations can only be used in the absence of an adequacy decision or of appropriate safeguards and does not explicitly state any time-based restrictions. This understanding aligns with *Schrems II*, where the court states that an annulment of an adequacy decision or the absence of appropriate safeguards does not create a legal vacuum due to Art 49 GDPR provisions. In contrast, Rec 114 GDPR clarifies that in case there is no adequacy decision, the data exporter should use solutions that provide data subjects with enforceable and effective rights.[87]

2.4.1. Explicit consent (Art 49 (1) (a) GDPR)

Under GDPR, consent is one legal basis for the processing of personal data. Requirements for a valid consent are outlined in Art 4 (11), Art 7 and in the case of processing children's data in Art 8 GDPR. In addition, Art 49 GDPR requires explicit consent for data transfers after the data subject is being provided with the risks of such transfer.[88]

Explicit consent must bring the data subject in a position to gain a high level of control and transparency over its personal data, which requires the consent to be specific for a particular data transfer before it can take place. In particular, the data exporter must ensure to inform the data subject about all the risks such transfer encompasses. It is not necessary that consent is given right before the transfer, but it must be ensured by the data exporter to provide all circumstances about the future transfer correctly to have a valid legal basis. In case of any material changes in the process, the consent must be re-obtained otherwise it is invalid.[89]

One important aspect to ensure is that explicit consent must be freely given. It requires to consider whether the data subject can truly exercise its free will. Issues also arise when

[86] *EDPB*, Recommendations 01/2020[2] Rec 24-26; *EDPB*, Guidelines 02/2018; *Art 29 WP*, WP228 p 4 and 39; Rec 115, Art 49 (5) GDPR.
[87] C-311/18 (*Schrems II)* Rec 202; see *infra* 2.4.1-2.4.7. for each derogation and interpretation; also, *Bernsteiner*, Schrems II & Privacy Shield, in *Jahnel* (Hg), Datenschutzrecht. Jahrbuch 21 p 124, 125, 130; *Gabauer/Höller*, Datenübermittlung in die USA p 81 and 82; *Piltz*, Art. 49 DSGVO - Der Vakuum-Killer für Drittlandstransfers? p 313.
[88] *EDPB*, Guidelines 02/2018 p 5; Art 4 (11), 6 (1) (a), 7, 9 (2) (a), 49 (1) (a) GDPR.
[89] *EDPB*, Guidelines 02/2018 Sec 2.1, p 5-8.

there is a clear imbalance of power between the controller and data subject, the consent is conditional to other contractual provisions, the consent is not given granular enough or a withdrawal from consent would be detrimental.[90]

The EDPB details what an informed notice should include. Emphasize must be given that no adequacy decision or appropriate safeguards are in place to appropriately protect the data subject and its personal data. Possible risks related to the third country's transfer such as the lack of a supervisory authority, privacy principles and data subject rights must be clearly stated and that this lack of fundamental principles is the reason why an adequacy decision or appropriate safeguards cannot be used as legal basis for the specific transfer.[91]

According to Art 49 (1) (a) GDPR explicit consent has no requirement for passing the necessity test to assess whether the data are mandatory for the specific transfer purpose, nor has the transfer be occasional or non-repetitive, which aligns with Rec 111 GDPR and EDPB Guidelines. However, the EDPB further refers to Rec 115 sentence 4 GDPR and states that nonetheless the explicit consent is not limited to occasional transfers, it must be still considered as derogation being the exception from the rule. Personal data should only be transferred as long as the country provides an adequate level of data protection or appropriate safeguards are in place.[92]

Recitals, such as Rec 115 GDPR, have no binding legal force and cannot derogate a legal provision. The same applies to EDPB guidelines. Both are used for interpretation purposes to ensure a consistent application of GDPR. It will remain seen whether courts will confirm EDPBs point of view.[93]

In my opinion, the EDPB's interpretation of Art 49 (1) (a) GDPR in relation to referred Recitals is ambiguous and not in alignment with GDPR's legal text or their own guidelines. With such a narrow scope and strict applicability, any potential explicit consent derogations use case would already fall under another Chapter V provision and would make it obsolete.

---

[90] *Art 29 WP*, WP 259 rev.01 p 6-11; Rec 42, 43, Art 7 (4) GDPR.
[91] Rec 104, 108, Art 45, 46 GDPR; *EDPB*, Guidelines 02/2018 Sec 2.1.3, p 8; see also *EDPB,* Recommendations 02/2020.
[92] *EDPB*, Guidelines 02/2018, p 4-5; *EDPB*, Recommendations 01/2020[2] Rec 25; *Bernsteiner*, Schrems II & Privacy Shield, in *Jahnel* (Hg), Datenschutzrecht. Jahrbuch 21 p 123 and 124; Rec 111, Art 49 (1) (a) GDPR.
[93] Art 70 (1) (e) and (f) GDPR; C-162/97 (*Nilsson ao*), Rec. 54; *Dopplinger* in *Knyrim*, DatKomm (2019) Rec 11 in Art 70 GDPR; *Bernsteiner*, Schrems II & Privacy Shield, in *Jahnel* (Hg), Datenschutzrecht. Jahrbuch 21 p 123, 124, 130; *Gabauer/Höller*, Datenübermittlung in die USA p 81.

Consent requirements already set a very high bar and can be seen as an exemption from the rule. Since consent can be withdrawn at any time, which affects not only the controller but any recipient, it is by itself unreliable and requires a strong (technical) infrastructure to support its legality. Furthermore, one overall goal of GDPR is to strengthen the position of data subjects and give them as much control over the processing of their data as possible. This narrow interpretation would mean that data subjects – provided they are in full understanding of the risk – would not have a free choice over the processing of their own data but patronized by the legislator.[94]

Examples for lawful processing are in my view cases where companies directly engage with the data subjects or the lawfulness of processing is already based on consent in accordance with Art 6 (1) (a) or 9 (2) (a) GDPR, explicit consent may be a feasible way to transfer data to the US when it comes to potential US governmental access and risks of a potential US governmental access cannot be fully ruled out. This excludes any sort of HR related data altogether. However, in addition to other safeguards explicit consent may be justified for a few data processing activities such as marketing or promotional activities unrelated to any contractual obligation or if the provision of personal data is not necessary for the provision of the services at all but can be achieved by anonymous or test data (e.g., generic business email addresses, dummy data for product development). It would furthermore require in my view a TIA including where possible add supplementary safeguards to lower the risk of exposure.

2.4.2. Performance of a contract with and for a data subject (Art 49 (1) (b), (c) GDPR)

Data exporters may use this derogation in case the data transfer is necessary and only occasionally for the contract performance between the controller and data processor. There must be a sufficiently close and substantial connection between the transfer and the contract and can only be used for non-repetitive or non-systematic relationships. Examples given by the EDPB are one-time travel arrangements.[95] Due to the narrow scope of applicability

[94] For consent requirements see Rec 32, 42, 43Art 6 (1) (a) and Art 9 (2) in accordance with Art 7, 8, 15 (1) (c), 17 GDPR; and *Art 29 WP*, WP 259 rev.01; in agreement with consent as possible transfer mechanism: *Bernsteiner*, Schrems II & Privacy Shield, in *Jahnel* (Hg), Datenschutzrecht. Jahrbuch 21 p 123, 124, 130; *Gabauer/Höller*, Datenübermittlung in die USA p 81.
[95] *EDPB*, Guidelines 02/2018 Sec 2.2 and 2.3, p 8-10; *Knyrim* in *Knyrim*, DatKomm Rec 25-27, 32-34 in Art 49 GDPR (2018); Rec 111, Art 49 (1) (b) and (c) GDPR.

and contract requirement, this transfer basis is very limited and not appropriate for any data exporters doing consistent business with the US.

2.4.3. Public interest (Art 49 (1) (d) GDPR)

Public interest is derived from Union or member state law and must meet the necessity test in order to apply. It also includes public interests based on international agreements the Union and/or member states are part of. The fact alone that a third country has an equivalent public interest, e.g., such as combatting terrorism, is not sufficient. It must furthermore be assured that the necessity directly derives from Union or member state law in terms of reciprocity or international cooperation. International agreements where the EU and the US are part of are valid indicators. Even though Rec 111 GDPR does not require the public interest derogation in being occasional, the EDPB emphasizes that a data transfer can nevertheless not occur on a large scale based on the derogation's nature being the exemption from the rule. Rec 112 GDPR states important reasons of public interest such as competition, tax, customs, financial, social security, or public health matters including doping in sport.[96]

One example for an important public reason could be seen in the international combat of cybercrime based on the Budapest Convention on Cybercrime (Budapest Convention)[97] In accordance with the EDPB requirements on public interest, the Budapest convention recognizes common objectives and principles for an international cooperation and mutual assistance between the convention parties. The US justifies the introduction of the CLOUD Act based on the Budapest Convention. Furthermore, the US government argues that a data transfer can be based on this derogation in case of a FISA 702 order since the US frequently shares gathered information with Union member states.[98]

While these arguments would in theory open this derogation option for data exporters, there is to my knowledge and opinion in practice no reliable source or guarantee to verify this statement since such practices are unlikely to be shared with affected companies or the public, nor has the Union or any member state officially confirmed such exchange. Also,

[96] *EDPB*, Guidelines 02/2018 Sec 2.4, p 10-11; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 38-39 in Art 49 GDPR; Rec 111, 112, Art 49 (1) (d) and Art (4) GDPR.
[97] Convention on Cybercrime, ETS No. 185, Budapest (Nov. 23, 2001) <rm.coe.int/1680081561> (last retrieved Aug. 13, 2023).
[98] *EDPB*, Guidelines 02/2018 Sec 2.4, p 10; Chapter III Budapest Convention; *DoJ*, The Purpose and Impact of the CLOUD Act, p 2, 6-7, 11, 15-16; *DoC/DoJ/ODNI*, U.S. Privacy Safeguards Relevant after EU-US Data Transfers after Schrems II, p 3-5.

unless a general statement either jointly or from Union side would be precise enough to determine the specific circumstances when data is shared between the US and Union, the order would need to provide information if such data is communicated to the Union. Otherwise, the data exporter would not sufficiently be released from its accountability and liability obligations under GDPR. It is therefore my view that businesses should be cautious when relying on the public interest derogation.

2.4.4. Legal claims (Art 49 (1) (e) GDPR)

This derogation covers use cases where the transfer is necessary and only occasional *"for the establishment, exercise or defense of legal claims"*. According to the EDPB, this point governs a number of events ranging from criminal to administrative investigation, reduction or waiver of legally foreseen fines, formal pre-trial discovery procedures in civil and commencing litigation or for obtaining approvals. The transfer needs to be in close relation to the actual procedure and the personal data to be disclosed must be limited to what is relevant and necessary.[99]

How this derogation relates to Art 48 GDPR is seen controversially. As stated above, Rec 115 GDPR states that any foreign law directly regulating the processing of personal data and not based on an international agreement may violate the protection of data subjects granted under GDPR. Only transfers in accordance with GDPR should be allowed. *Knyrim* argues that Art 48 GDPR sets the limit on how far Art 49 (1) (e) GDPR can be used. In contrast, *Riedl* and *Pauly* state that the legal claim derogation goes beyond Art 48 GDPR and can even be used for cases where there is no international treaty in place. *Zerdick* and *Weiß* point out that even if a transfer would be unlawful according to Art 48 GDPR, it may still be possible to use Art 49 (1) (e) GDPR on a case-by-case basis.[100]

In case of a one-time request where the data importer falls in a category of providers under US surveillance or law enforcement laws but is unlikely to receive US governmental access requests on a regular basis, it is in my view a valid derogation to consider. First, the data importer must use every ally of challenging the legal request to the point it faces legal

[99] *EDPB*, Guidelines 02/2018 Sec 2.5, p 11-12; Rec 111, Art 49 (1) (e) GDPR.
[100] Rec 115 GDPR; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 13 and 14 in Art 48 GDPR; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 44 and Fn 63 in Art 49 GDPR with further references to *Riedl* in *Gantschacher/Jelinek/Schmidl/Spanberger*, DSGVO Art 49 Rec 11; *Pauly* in *Paal/Pauly*, DSGVO/BDSG[2] Art 49 Rec 22; *Zerdick* in *Ehmann/Selmayr*, DS-GVO, Art 49, Rec 15; *Weiß* in *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht[2] p 770.

consequences such as penalties. Second, a risk assessment based on the type of sought data and possible adverse impact of the data subject must be made. Third, transparency and information rights to affected data subjects must be assessed. If the request includes a protective order not to disclose information (not even within a reasonable time), data subjects' rights of information and redress are impinged. However, if there is the option – even combined with other measures, such as explicit consent – to reasonably provide the data subject with its due rights, this derogation seems in my view justifiable.

2.4.5. Vital interests (Art 49 (1) (f) GDPR)

When a person is in a medical emergency or another unexpected situation and incapable of providing or agreeing on a disclosure of necessary information, a transfer of personal data is legitimate if necessary related to the vital interests of a person.[101]

In the business context examples are fairly limited but could include the disclosure of employee personal data to US medical institutions or other relevant US recipients, such as law enforcement in case of an emergency.

2.4.6. Public register (Art 49 (1) (g) and 49 (2) GDPR)

Another derogation option is a transfer from a register which is intended by Union or member state law to provide information either to the public or to anyone who can prove legitimate interest in such information. A transfer of the entire record of personal data is not permissible but requires a case-by-case assessment of which data are essential for the specific transfer purpose. Where the access to the register is based on a legitimate interest of a person, a transfer can only take place at the request of this person or if it is the recipient of the data. Examples of covered registers are company registers, registers of criminal conviction, title registers, such as for land, trademarks, patents, designs and/or copyright. In contrast to the legal text and *Pauly*, the EDPB excludes private registers from its applicability under this derogation.[102]

Use cases for this derogation are limited but show that information publicly or semi-publicly available have a less restrictive transfer threshold. In practice data exporters must

[101] *EDPB*, Guidelines 02/2018 Sec 2.6, p 12-13; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 45 and 47 in Art 49 GDPR.
[102] *EDPB*, Guidelines 02/2018 Sec 2.7, p 13-14; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 49-51, Fn 69 in Art 49 GDPR with further reference to *Pauly* in *Paal/Pauly*, DS-GVO/BDSG[2] Art 49 Rec 26; Art 49 (1) (g) and 49 (2) GDPR.

maintain a very granular and informative data flow chart to ensure that data only originates from public registers. Since the data set is very limited, possible areas of consideration are business contact and affiliation information.

2.4.7. Compelling legitimate interests (Art 49 (1) § 2 GDPR)

The last resort for any data transfer justification can be based on compelling legitimate interests of the data controller accompanied by several firm conditions which needs to be assessed on a case-by-case basis: 1) there cannot be any other Chapter V GDPR transfer tool possible for the transfer; 2) the transfer is not repetitive; 3) it concerns only a limited number of data subjects; 4) it is necessary for the purpose of compelling legitimate interest which cannot be overridden by the interests of the data subjects; 5) suitable safeguards are in place; 6) the controller must inform the supervisory authority as well as the data subjects; 7) the assessment and safeguards must be documented.[103]

The EDPB provides one example for a compelling legitimate interest for a data transfer, namely in case of a unique and serious security incident where the company is protecting its systems from serious immediate damage or severe consequences.[104] This would in my point of view also include circumstances when the data exporter or importer have to report data breaches under US state law requirements or industry-specific federal laws.[105]

[103] *EDPB*, Guidelines 02/2018 Sec 2.8, p 14-17; *Knyrim* in *Knyrim*, DatKomm (2018) Rec 53-58 in Art 49 GDPR; Rec 111, 113, Art 49 (1) § 2, 49 (6) GDPR.
[104] *EDPB*, Guidelines 02/2018 Sec 2.8, p 15.
[105] See overview of US state law breach notification requirements: *Perkins Coie*, Security Breach Notification Chart; or *PrivacyRights.org*, Data Breach Notification in the US 2022 Report; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3] Sec 7.5 and 7.6.

3. Transfer impact assessment

If a transfer cannot be based on an adequacy decision according to Art 45 GDPR or derogations in accordance with Art 49 GDPR, but on appropriate safeguards outlined in Art 46 GDPR, *Schrems II* requires a proof of the effectiveness and the protection of personal data guaranteed by GDPR in practice. It must be assured that the selected tool is effective to ensure an essential equivalent level of protection under GDPR in the US. A TIA is focused on the third country's law and practice for a specific situation and whether it contradicts GDPR standards. This differences with an EC assessment for an adequacy decision where the assessment is comprehensive and looks at the overall compatibility.[106]

3.1. General TIA requirements

A TIA first lays out the specific circumstances of the transfer. In addition to the Art 30 GDPR ROPA requirements, the TIA must include recipient's types of entities, transfer sector, storage location of relevant data, data transfer format and onward transfers information.[107]

Thereafter, relevant laws and practices must be listed and assessed on a general basis to the extent they interfere with the chosen transfer tool. It should focus on laws and aspects of the legal system as outlined in Art 45 (2) GDPR related to public and national security as well as criminal law which require a disclosure of or access to personal data by public authorities. Furthermore, effective redress options, implementation of supervisory authorities and data protection safeguards as well as international commitments must be taken into consideration.[108]

Next, the findings undergo a balancing test against EU standards, in particular Art 47 and 52 of the Charter. It must be assessed whether such laws and practices, which restrict data subject's fundamental rights are limited to what is necessary and proportionate in a democratic society. If such laws do respect the essence of subject's fundamental rights, are necessary and proportionate and recognized by Union or member state law, such laws are

[106] *EDPB*, Recommendations 01/2020[2] Rec 27-49; *EDPB*, Recommendations 02/2020 Rec 52-53; C-311/18 (*Schrems II*) Rec 126, 137.
[107] *EDPB*, Recommendations 01/2020[2] Rec 33-34; Art 30 GDPR; also, SCC Int transfer 2021 EC (EU) 2021/914 Rec 20, Annex Clause 14 (i).
[108] *EDPB*, Recommendations 01/2020[2] Rec 35-37; C-311/18 (*Schrems II*) Rec 126; Rec 104, 105, Art 45 (2) GDPR; see also, SCC Int transfer 2021 EC (EU) 2021/914 Rec 20, Annex Clause 14 (ii).

in accordance with transfer tools obligations. Otherwise, they do impinge upon Art 46 GDPR requirements.[109]

European Essential Guarantees

As part of the overall TIA, the EDPB adopted recommendations based on *Schrems I, Schrems II,* Art 7, 8, 47 and 52 of the Charter as well as the jurisprudence of the ECtHR based on Art 8 of the European Convention on Human Rights (ECHR)[110] to clarify in which cases foreign surveillance measures are a justifiable interference with regard to the fundamental rights of private and family life. If so, the foreign legislation is satisfying the European Essential Guarantees (EEG). If not, the foreign legislation is not seen as essentially equivalent to EU standards.[111]

In essence, the EEG consist of the following four main criteria: 1) clear, precise, and accessible rules for processing, 2) demonstratable necessity and proportionality of legitimate processing objectives, 3) existence of an independent oversight mechanism, and 4) availability of effective remedies to individuals.[112]

Guarantee A – Clear, precise, and accessible rules

Fundamental rights granted under the Charter, including Art 7 *"Respect for private and family life"* and Art 8 *"Protection of personal data"*, apply to everyone.[113] Since the Charter is addressed to the institutions of the EU and all their actions as well as member states when implementing EU law, everyone in this context means, everybody who is affected by EU law or EU institutions' actions. The fundamental rights in Art 7 and 8 of the Charter are no absolute rights and can be limited by and in accordance with the law if

[109] *EDPB*, Recommendations 01/2020[2] Rec 35 and 40; Art 47 and 52 Charter; Art 23 (1) GDPR
[110] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms (Nov. 4, 1950), as amended by Protocols 11, 14, 15 and as supplemented by Protocols 1, 4, 6, 7, 12, 13, 16 <echr.coe.int/documents/d/echr/Convention_ENG> (last retrieved Aug. 13, 2022).
[111] *EDPB*, Recommendations 02/2020 Rec 1-8, 10-11, 13, 51.
[112] *EDPB*, Recommendations 02/2020 Rec 24 and 25.
[113] Art 7 of the Charter: *"Everyone has the right to respect for his or her private and family life, home and communications."*; Art 8 of the Charter: *"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."*.

justified. Therefore, the legal basis, its scope and applicability of any limiting law must be comprehensible and foreseeable for affected individuals.[114]

Guarantee B – Necessity and proportionality test

Based on the requirements in Art 52 (1) of the Charter, any limitation by law of Art 7 and 8 of the Charter must still respect the granted rights and freedoms and can only be justified if such law truly meets objectives of general interest which are recognized by the EU. Proportionality refers to a balance test of the sincerity of the interference versus the significance of the public interest objective.[115]

Guarantee C – Oversight

Any restriction on fundamental rights needs access to an effective, independent and impartial oversight mechanism assembled by a sovereign body, which is sufficiently independent from the executive branch. Such body must have access to all relevant information to be able to guarantee an effective review, preferably before any action takes place, however, in certain circumstances such as justified urgency a subsequent review within a short time is acceptable.[116]

Guarantee D – Redress

Affected individuals must have access to an effective remedy if it is believed that their rights have been infringed. For an effective redress mechanism, notification is necessary. Otherwise, affected individuals have no awareness of a potential violation. If notification is not feasible, redress may be appropriate under a set of conditions including an independent oversight body with access to all relevant information and the power to remedy non-compliance and an easy non evidential heavy mechanism to lodge a complaint.[117]

The TIA has two different outcomes. The assessment can effectively ensure that the data protection in the US is essentially equivalent for the specific transfer and the data importer can comply with its obligations laid out in Art 46 GDPR. If so, the data can be transferred

[114] Rec 1 and 2 GDPR; *EDPB*, Recommendations 02/2020 Rec 13, 18, 26-31; Art 52 (1) of the Charter; *EC*, When does the Charter apply?.
[115] *EDPB*, Recommendations 02/2020 Rec 19, 32-38; Joined cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net ao*) Rec 131.
[116] *EDPB*, Recommendations 02/2020 Rec 39-42. 46-47.
[117] *EDPB*, Recommendations 02/2020 Rec 43-45.

based on the chosen appropriate safeguard mechanism. Otherwise, the outcome does not effectively ensure that an essentially equivalent level of data protection is guaranteed. Then, the data exporter must either put suitable supplementary measures in place or completely refrain from a data transfer.[118]

3.2. US TIA assessment

The hereinafter conducted TIA is based on the assessment of potential US governmental access to personal data in the cloud based on the current, 2023, US legislation for the use of appropriate safeguards under Art 46 GDPR. It continues the legal assessment on US federal level of the research question whether it is possible to be legally compliant with GDPR as a data exporter who is directly or indirectly through its business partners subject to US governmental access requests to electronically held personal data. It should be assessed under which circumstances an access request may occur.

In addition to MLATs, there are four main pieces of US federal legislation, which govern the access to electronic data and the electronic surveillance by governmental agencies for law enforcement and national security purposes. On a high level, these regulations can be distinguished by its general purpose as follows:

National security

- **EO 12333** provides the overall framework of intelligence activities and governs the collection of electronic data of non-US persons communication stored outside the US for foreign intelligence surveillance purposes by the Intelligence Community.[119]

- **FISA** regulates the collection of foreign intelligence information targeting US and non-US persons inside and outside the US but stored or controlled inside the US for foreign intelligence surveillance purposes by the Intelligence Community.[120]

- **EO 14086** sets enhanced safeguards for the overall intelligence activities framework.[121]

[118] *EDPB*, Recommendations 01/2020[2] Rec 43, 49; *EDPB*, Recommendations 02/2020 Rec 51.
[119] See *infra* sec 3.2.2.
[120] *Id*.
[121] *Id*.

Law enforcement

- The **Electronic Communications Privacy Act** (ECPA)[122] governs the electronic surveillance and collection of electronic evidence for any criminal law enforcement activity against US and non-US persons stored or controlled inside the US by law enforcement agencies or the Intelligence Community.[123]

There are several other sector-specific federal regulations, which require or permit the disclosure of personal data. The applicability depends on the categories of data being processed or on the sector in which the company is operating, e.g., the bank or health care sector. Specific state laws additionally govern the access and disclosure requirements to electronically held data by companies. Those laws can be stricter than related federal regulations where federal law is not preemptive. In any case, state laws are also bound by the US Constitution. Furthermore, access to electronically held data may also be obtained through any civil litigation procedures. [124]

3.2.1. US rule of law related to electronically held data and access

3.2.1.1. International commitment

EU and US privacy laws are based on the same Fair Information Practices (FIP or FIPP including Privacy), first codified by the US Department of Health, Education and Welfare in 1973. EU member states as well as the US are members of the Organisation for Economic Co-operation and Development (OECD). FIPP were later used and build upon to the 8 principles codified in the *OECD Privacy Guidelines*[125] in 1980. Subsequent OECD guidelines and recommendations including the latest in 2022 *Declaration on Government*

[122] Electronic Communications Privacy Act of 1986, Pub. L. 99–508, 100 Stat. 1848 (Oct. 21, 1986) <govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf> (last retrieved Aug. 13, 2023).
[123] See *infra* sec 3.2.3.
[124] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.1.1., 13.2, 13.3.3.1 and 13.3.3.2; e.g.: the ECPA is not preemptive and allows stricter state statutes.
[125] *OECD*, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (adopted Sep. 22, 1980, last revised Jul. 10 2013) <legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> (last retrieved Aug. 13, 2023); The 8 Principles are: 1. Collection Limitation, 2. Data Quality, 3. Purpose Specification, 4. Use Limitation, 5. Security Safeguards, 6. Openness, 7. Individual Participation, 8. Accountability.

Access to OECD Legal Instruments Personal Data held by Private Sector Entities[126] have also been adopted by the OECD member states.[127]

Another common international commitment regarding data protection is the international combat of cybercrime based on the Budapest Convention that entered into force on July 1, 2004. Among the current 68 parties to the convention, the US and all EU member states except Ireland ratified the treaty.[128]

3.2.1.2. Data privacy principles

The core understanding of data privacy differs between continental Europe and the US. Where the continental European view sees privacy in the form of dignity and the protection of a right to respect, the US view, in contrast, focuses on the values of liberty (of the state) and individual sovereignty. This can also be seen in the differences of each regime's fundamental rights. In the former US congressman Bob Goodlatte's testimony in front of the Judiciary House Committee he states, *"our very country was born out of anger and fear of what a government can do to people when it doesn't respect their privacy".*[129]

These divergent views stem from the legal and social values of its cultures and are shaped by time, through e.g., traditions, politics, or major events. As a general rule in terms of privacy, in the EU, everything is forbidden, what is not explicitly allowed (opt-in) and in the US, everything is allowed what is not explicitly forbidden (opt-out). Differences between the US and EU can also be seen in their implementation approaches, where EU law is considered more prescriptive and process oriented. Even though neither view is per se wrong, these factors create misunderstandings and a lack of common ground when attempting to find mutual agreements.[130]

Where the EU enacted privacy and security omnibus laws such as GDPR, the US, in contrast, followed a sector specific approach. This approach started to change in the last

[126] *OECD*, Declaration on Government Access to Personal Data held by Private Sector Entities, OECD/LEGAL/0487 (Dec. 13, 2022) <legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487> (last retrieved Aug. 13, 2023).
[127] *EPIC*, The Code of Fair Information Practices; *EPIC*, Records, Computers and the Rights of Citizens.
[128] *Council of Europe*, Chart of signatures and ratifications of Treaty 185.
[129] E.g., Art 1 of the Charter refers to "dignity"; US Declaration of Independence and Preamble US Constitution emphasize "liberty"; *Whitman*, The Two Western Cultures of Privacy, p 1160-1162; *Honorable Bob Goodlatte*, Digital Dragnets: Examining the Government's Access to Your Personal Data.
[130] *Whitman*, The Two Western Cultures of Privacy, p 1160-1162; *Georgieva*, EU-US-Privacy Shield - eine Gesamtbetrachtung, p 216; *Kerry*, Why protecting privacy is a losing game today; *Dixon*, A Brief Introduction to Fair Information Practices.

few years, as more and more US States, starting with California in 2020 and followed by several other states, enacting US statewide privacy protection laws for the private sector. These movements put a high pressure on the federal legislative for a federal omnibus privacy law and the need to harmonize (and even preempt) state laws. The in 2022 introduced American Data Privacy and Protection Act (ADPPA)[131] is the first attempt to a federal privacy omnibus law.[132]

3.2.1.3. Collection and use of personal information by the US federal government

The collection and use of personal information by the US federal government is primarily governed by the Privacy Act of 1974[133]. In the 70's, the Watergate scandal exposed federal agencies' illegal surveillance and investigation methods of civilians. Additionally, the increasing use of computers by the government raised concerns about abuses of storing and retrieving personal information. The US Congress therefore enacted the Privacy Act of 1974 which regulates US Federal agencies' collection, maintenance, use and dissemination of individual's personal information, compliance with statutory norms, and grants individuals the right to access, correction and civil remedies related to its records.[134]

The Judicial Redress Act of 2015[135] extended the Privacy Act's civil remediation rights to individuals of covered countries for designated federal agency's intentional or willful disclosure of information if such disclosure has an adverse effect on the individual. The EU and its member states are covered countries. No agency of the IC or FBI, however, are part of the designated federal agencies.[136]

[131] American Data Privacy and Protection Act, H.R.8152 – 117th Congress (2021-2022): To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement (June 21, 2022) <congress.gov/bill/117th-congress/house-bill/8152> (last retrieved Aug. 13, 2023).
[132] For an overview of enacted and anticipated US privacy regulations, see *Fazlioglu*, US Federal Privacy Legislation Tracker; and *Desai*, US State Privacy Legislation Tracker.
[133] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (Dec. 31, 1974) <govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf> (last retrieved Aug. 13, 2023) = 5 U.S.C. § 552a (2023).
[134] § 2 Privacy Act of 1974; *DoJ*, Overview of the Privacy Act of 1974; *US Government Accountability Office*, Protecting Personal Privacy.
[135] Judicial Redress Act of 2015, Publ. L. 114-126, 130 Stat. 282 (Feb. 24, 2016) <congress.gov/114/plaws/publ126/PLAW-114publ126.pdf> (last retrieved Aug. 13, 2023) = 5 U.S.C. § 552a note (2023).
[136] Sec 2 (a) Judicial Redress Act of 2015; 5 U.S.C. § 552a (b), (g) (1); *DoJ*, Judicial Redress Act, Sec B. 1. and 2.

Under the Privacy Act of 1974, an agency is only allowed to disclose held information for US law enforcement activities pursuant to a court order or to another agency if authorized by law and the head of the other agency has made a written request specifying the sought information and the law enforcement activity.[137]

3.2.1.4. Agencies

The US distinguished between federal, state, and local law enforcement agencies, which all have a different scope of jurisdiction in the area of law enforcement. There are currently more than 90 federal agencies and with more than 140.000 full-time law enforcement officers and more than 17,000 state and local law enforcement agencies.[138]

The IC encompasses 18 federal agencies, including the Federal Bureau of Investigations (FBI), Central Intelligence Agency (CIA) and the National Security Agency (NSA) with the purpose to collect and analyze foreign intelligence and counterintelligence information and assist the US president, policy makers, law enforcement as well as the military in their decision-making processes. Some of those agencies are both law enforcement agencies as well as IC.[139]

3.2.1.5. Electronic surveillance

In general, electronic surveillance is an act of observing someone for the acquisition of information by an electronic, mechanical, or other device and includes methods such as wiretapping, bugging, videotaping, geolocation, tracking, data mining, social media mapping or the monitoring of data and traffic on the internet. There are two main categories how to gather information: either by wire, which includes the transfer via wire, cable, or a similar method, or electronic, which consist of a transfer by electronic means.[140]

Electronic surveillance is defined differently by EO 12333 and FISA, while the ECPA does not have an overarching definition but defines specific measures such as "intercept". Readers must therefore be aware of its different scope and applicability.[141]

---

[137] 5 U.S.C. § 552a (b) (7) and (11).
[138] *International Association of Chiefs of Police*, Types of Law Enforcement Agencies; *DoJ*, 2020 – Statistical Tables.
[139] *Office of the Director of Intelligence*, Our Organization, *Office of the Director of Intelligence*, Mission.
[140] *Cornell Law School*, surveillance; *Cornell Law School*, electronic surveillance.
[141] The Wiretap Act refers to the FISA definition, see 18 U.S.C. § 2511 (2) (a) (ii), § 2511 (2) (e).

EO 12333 defines electronic surveillance as "*acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication […] but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.*"[142]

In contrast, electronic surveillance under FISA means either (a) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication: (1) sent by or intended to be received by a particular, known US person who is in the US, if the contents are acquired by intentionally targeting that US person; (2) to or from a person in the US, without the consent of any party thereto, if such acquisition occurs in the US, but does not include the acquisition of those communications of computer trespassers that would be permissible under 18 U.S.C § 2511 (2) (i); or (3) if both the sender and all intended recipients are located within the US and the acquisition is intentional; or (b) the installation or use of an electronic, mechanical, or other surveillance device in the US for monitoring to acquire information, other than from a wire or radio communication. For (a) (1), (a) (3) and (b) it must be under circumstances in which a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes.[143]

3.2.1.6. Personal jurisdiction

Personal jurisdiction describes whether a court has the power to make a decision over a person. A person in this context means individuals as well as legal entities. On the US constitutional level, jurisdiction is defined by the Fourteenth Amendment referencing to US citizens, namely people who are "*born or naturalized in the US"*. Additionally, personal jurisdiction for other persons than US citizens is determined by US courts and requires an analysis of various factors on a case-by-case basis, where US courts determined that US personal jurisdiction also applies to non-US persons such as foreign entities with an establishment in the US or which have "minimum contacts" with the US. Some considerations are if the foreign company is selling products or services to the US, or whether the website is available in the US or if US IP addresses are blocked in the US.[144]

[142] EO 12333 Part 3 3.5 (c).
[143] 50 U.S.C. § 1801 (f).
[144] U.S. Const., amend. XIV; *Congress.gov*, Amdt14.S1.7.1.1, par 3, 7.

3.2.1.7. US and non-US persons

The differentiation between US and non-US persons is closely related to whether the US has personal jurisdiction over a specific person as described above. Where personal jurisdiction has a broader applicability and only needs to meet the minimum contact test, the definition of a US person is narrower and defined differently by statutes. A US person as defined by FISA, EO 12333, and the ECPA includes US citizens, lawful permanent residents, unincorporated associations if their members are US citizens or lawful permanent residents, or any corporation incorporated in the US. For intelligence purposes under FISA and the EO 12333, US corporations are not considered US persons if incorporated by a foreign power, which for this definition includes a foreign government, a faction of a foreign nation or an entity controlled by a foreign government.[145]

The importance of this distinguishment is based on certain privileges a US person has under the US constitution, in particular whether the Fourth Amendment protection applies. In *United States v. Verdugo-Urquidez*, the US Supreme Court declared that the Fourth Amendment does not apply to any search and seizure of property located in the US but owned by a nonresident alien located in a foreign country.[146]

3.2.1.8. The Fourth Amendment

Privacy protection on a US constitutional level is governed within the Bill of Rights by the Fourth Amendment which gives people the right *"[…] to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[147] The original intent of the Fourth Amendment was to limit the government's power from any physical invasion of premises to protect and secure the people's property from being taken away by the government. Over time, the Supreme Court changed its angle of view away from the property perspective and acknowledged that the core intent of the Fourth Amendment is the protection of people's personal privacy and

[145] 50 U.S.C. § 1801 (i) in accordance with § 1801 (a) (1), (2), (3) and 8 U.S.C. § 1101 (a) (20); EO 12333 (2008) Part 3 sec 3.5 (k); 18 U.S.C. §§ 2523 (a) (2), 2703 (h) (1) (B).
[146] *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), 264-275; in contrast for example to the Fifth Amendment (privilege against self-incrimination), which does apply to non-US persons.
[147] U.S. Const., amend. IV.

dignity from unreasonable search and seizure and not per se the protection of places or property.[148]

Fourth Amendment jurisprudence is vast. Especially over the last century, courts had difficulty determining whether electronic surveillance requires a search warrant or not and how to deal with new technology. It was long the understanding of the majority of the Supreme Court that no warrant was required if there was no actual physical invasion.[149]

In *Katz v. United States* in 1967, the Supreme Court established a two-part test, called the "Third-Party Doctrine", consisting of the subjective and the legitimate criteria to evaluate whether a person has a reasonable expectation of privacy under the Fourth Amendment. With this landmark decision, the court overruled previous jurisprudence and clarified that only in cases where a person knowingly exposes information to the public, such information is not subject to the Fourth Amendment, however, anything a person seeks to preserve as private – even in public –, is protected.[150]

The assessment whether an individual has a legitimate privacy interest in its records if it shares such information with a third party and what is a reasonable expectation of privacy, however, used to be interpreted very differently by the US courts. The majority of rulings stated that a legitimate interest of privacy does not exist in case any third party is involved. With *Carpenter v. United States* in 2018, the US Supreme Court placed substantial restrictions on the Third-Party Doctrine and determined that law enforcement must have a search warrant for certain records (e.g., cell site location information) held by third parties as such information may reveal intimate details about a person's private live. The court held that a subpoena is not sufficient for law enforcement authorities to access a person's cell phone site location for more than seven days and did not acknowledge the argument that a person lost its reasonable expectation of privacy by voluntarily disclosing such information to a third party.[151]

---

[148] *U.S. Government Publishing Office*, Fourth Amendment Search and Seizure, p 1205 et seq.; *Schwartz*, Legal Access to the Global Cloud, p 1711 et seq; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.1.

[149] See *Olmstead v. United States*, 277 U.S. 438 (1928), or *Goldman v. United States*, 316 U.S. 129 (1942), where the courts ruled that neither wiretapping nor placing a detectaphone against a wall is covered under the Fourth Amendment, as neither constitutes a physical invasion.

[150] *Katz v. United States*, 389 U.S. 347, 353 (1967); *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.1.

[151] *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.1; *Chin*, Digital Dragnets, p 3; see *United States v. Miller*, 425 U.S. 435 (1976), where there is no

Whether the Fourth Amendment also applies to data stored in the cloud – inside or outside the US – is still unanswered by the courts.[152] In my point of view, the determination where data are stored is irrelevant in light of Supreme Courts' clarification that the Fourth Amendment shall protect US-persons and not per se the information itself.

In summary, the Fourth Amendment prevents the government from any unreasonable search and seizures and requires US law enforcement to obtain a probable cause search warrant when collecting or intending to collect information for any investigation. It protects individuals who are either US citizens regardless of residency or non-US persons who reside within the US and have developed strong connections with the US. "Person" in this context is not limited to individuals but also encompasses companies or other types of associations. Consequently, the Fourth Amendment does not apply to non-permanent US residents located outside the US, such as EU citizens without a US green card, visitors of the US, visa holders, or foreign companies without a strong connection to the US, e.g., through a US parent company, subsidiary, or business engagements.[153]

3.2.1.9. Warrant

Warrants are court orders, issued by a judge which authorizes law enforcement agencies to perform an action related to the administration of justice. It requires a clear description of information and persons to be seized, probable cause that sought information will be found as described and must clearly specify which place/device will be searched. A warrant to be issued by a US governmental entity must first demonstrate probable cause that the sought data is evidence of a crime, and the person has possession, custody or control over sought data.[154] Probable cause means that law enforcement must proof that a crime has been, is or is likely to be committed. In case any evidence is gathered by law enforcement in violation

legitimate "expectation of privacy" in bank records, *Smith v Maryland*, 442 U.S. 735 (1979), where the installation and use of a pen register was no violation because the numbers would be available to and recorded by the phone company anyway; in contrast: *United States v. Jones*, 565 U.S. 400 (2012), where a warrant was needed when placing a GPS device on a car; *Riley v. California*, 573 U.S. 373 (2014), where a search warrant was needed to obtain content of a cell phone.

[152] *Schwartz*, Legal Access to the Global Cloud, p 1711.

[153] See U.S. Const. preamble *"We the People of the United States […]"*; *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), 264-275; *GPO*, Fourth Amendment Search and Seizure, p 1204 et seq; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.1.

[154] 18 U.S.C. § 2703(a) and (b) and 18 U.S.C. § 2713 in accordance with Federal Rules of Criminal Procedure or State warrant procedures; *Cornell Law School,* warrant; *Cornell Law School*, search warrant.

of the Fourth Amendment requirements, it can be eliminated from the criminal trial, under the so-called exclusionary rule.[155]

Electronic surveillance is considered as search under the Fourth Amendment and therefore subject to general warrant requirements. The Federal Rules of Criminal Procedure (Fed. R. Crim. P.) describe the general procedures for warrants seeking electronically stored information.[156]

3.2.1.10. Subpoena

Subpoenas are written orders compelling a person to testify before a court or other legal proceeding (witness subpoena or subpoena ad testificandum) or a request for documents held by the subpoenaed person (deposition subpoena or subpoena duces tecum). In regard to criminal matters, Rule 17 Fed. R. Crim. P. governs the general process of subpoenas. Subpoenas are usually issued by the court but can also be issued by an attorney.[157]

In addition, US statutes authorize specific government authorities to issue subpoenas for evidence collection in law enforcement matters. These types of subpoenas, so called administrative or governmental subpoenas, or grand jury subpoenas in case of federal criminal investigations as well as national security letters (NSL), do not have a prior judicial oversight but are judicially enforceable.[158]

NSLs are a specific form of administrative subpoenas issued by US agencies for specific foreign intelligence investigations as authorized by US statutes. NSLs can only request non-content information such as transactional records and dialed phone numbers but not the content of a communication. A prior approval from a judge is not required. NSLs usually contain confidentiality provisions which forbit the recipient to disclose the issuance, existence, and content of an NSL.[159]

[155] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch. 13.3.1.
[156] Rule 41 (e) (2) (B) Fed. R. Crim. P.; *Cornell Law School*, electronic surveillance.
[157] Rule 17 Fed. R. Crim. P.; *Cornell Law School*, subpoena; *FindLaw*, What Is a Subpoena.
[158] *Doyle*, Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations, p 2; *Schwartz*, Legal Access to the Global Cloud, p 1724.
[159] *Vladeck*, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, p 13; *Doyle*, Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations, p 19.

Prior 2001, NSLs had a comparable narrow scope of applicability and could only be used for requesting specific financial and communication records related to a foreign power[160] with each NSL requiring a firm FBI preapproval. The USA PATRIOT Act of 2001extended the NSLs issuance authority to any government agency which significantly increased the number of requests. Even though most NSL statutes do not have a judicial enforcement or penalty for non-compliance provision, a lot of criticism about the excessive use of NSLs rose which led to an adjustment of its applicability requirements. As of 2023, five statutory provisions[161] authorize US agencies to issue NSLs for foreign intelligence purposes. The indefinite disclosure requirements of NSLs are – apart from some exceptions – no longer in force. Additionally, parties receiving NSLs have the option to file a petition to court to modify or set aside the NSL and/or its confidentiality obligations.[162]

3.2.2. National security

3.2.2.1. Clear, Precise, Accessible Rules

According to the Code of Federal Regulations (CFR), *"National security refers to those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism."*.[163] The US constitution defines the president as commander-in-chief of the armed forces based on its given executive powers. Additionally, the US Supreme Court clarified that the president has plenary powers in foreign affairs, meaning that the president has complete and exclusive power without any limitations over foreign policy without the need of the US Congress to delegate such power to the executive branch.[164]

[160] 50 U.S.C. § 1801 (a): Foreign power means *"(1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; or (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction"*.
[161] 18 U.S.C. § 2709; 12 U.S.C. § 3414; 15 U.S.C. § 1681v; 15 U.S.C. § 1681u; 50 U.S.C. § 3162 (this section was formerly classified to 50 U.S.C. § 436).
[162] *Doyle*, Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations, p 19-24; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch. 13.3.5.
[163] 5 CFR § 1400.102 (a) (3).
[164] U.S Const. art II; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.4.1; *United States v. Curtiss-Wright Export Corp*., 299 U.S. 304 (1936); *Cornell Law School*, Plenary Power.

In contrast, judicial power is granted to the courts. While the US Supreme Court emphasizes the importance of judges and the accompanied requirement of a warrant pursuant to the Fourth Amendment for search and seizures, it is an ongoing debate how far reaching each, the US President's and US Supreme Court's power go. The Supreme Court criticized that the definition of national security is too vague and can therefore be easily exploited by US agencies for illegitimate warrantless surveillance measures, which supposed to be protected by the Fourth Amendment.[165]

EOs are written directives by the President of the US, published in the Federal Register[166], to manage the operations of the US federal government. While it is mostly used for administrative purposes, EOs are lately repurposed to roll out policies and programs in a much broader way than originally intended. EOs have official character, however, they can be revoked by the President at any time.[167] Presidential Policy Directives (PPD) are a specific type of EOs and mostly classified, issued by the National Security Council and signed or authorized by the President. Almost each Presidential Administration has given EOs different names.[168]

EO 12333 builds the current foundation of the current US national intelligence activities with special emphasis on detecting and countering espionage, terrorism and weapons of mass destruction. EO 12333 directs the IC, which currently consists of 18 federal intelligence agencies or parts thereof, how to obtain information regarding foreign intelligence activities in- or outside the US. Initially issued by US President Reagan in 1981, EO 12333 replaced two prior EOs regarding US intelligence activities and was amended three times in 2003, 2004 and the last major revision in 2008 by the Bush administration based on the Implementing Recommendations of the 9/11 Commission Act of 2007[169].[170]

[165] U.S Const. art III; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.4.1; *United States v. U.S. District Court for Eastern District of Michigan*, 407 U.S. 297 (1972).
[166] *National Archives*, Office of the Federal Register (OFR).
[167] *Bureau of Justice Assistance*, Executive Orders.
[168] *The Library of Congress*, Presidential Directives and Where to Find Them; e.g.: under the Trump Administration PPDs (named by the Obama Administration) are called National Security Presidential Memoranda (NSPMs), see more under <loc.gov/rr/news/directives.html> (last retrieved May 2, 2023).
[169] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110–53, 121 Stat. 266 (Aug. 3, 2007) <congress.gov/110/plaws/publ53/PLAW-110publ53.pdf> (last retrieved Aug. 13, 2023).
[170] *Bureau of Justice Assistance*, Executive Orders, in particular part I 1.1 (d); *PCLOB*, EO 12333, p 13-14.

EO 12333 grants the scope and puts limits on how to conduct intelligence activities, e.g., it limits the collection of information about US persons and sets restrictions on collection techniques and undisclosed participation in any organization inside and outside the US. EO 12333 addresses all foreign intelligence surveillance activities and is thus more far reaching than FISA as it also includes activities outside the US against non-US persons. Nothing in the EO 12333 authorizes any activity in violation of the US Constitution or statutes of the United States which means that electronic surveillance of information covered under FISA would only be disseminated pursuant to FISA and not under the EO 12333. Due to the overlap with FISA, the main applicability of EO 12333 is gathering of information outside the US against non-US persons. Any delegation of authority under the EO must be in accordance with FISA.[171]

Affected data by EO 12333 includes all intelligence gathered within or outside the US. Data sought by electronic surveillance under the EO 12333 is any nonpublic communication by electronic means in accordance with foreign intelligence and counterintelligence information.[172]

The EO 12333 targets US as well as non-US persons related to the IC's intelligence activities. Procedures against US persons, however, have stricter implementation rules and must be the least intrusive collection technique. For non-US persons no such safeguards exist in EO 12333.[173] The Presidential Policy Directive regarding Signal Intelligence Activities (PPD-28)[174] issued in 2014 set some limits to bulk collection as well as the implementation of appropriate safeguards for collected information regardless of the person's nationality or residency. PPD-28 was replaced by EO 14086 through National Security Memorandum on Partial Revocation of Presidential Policy Directive 28 (NSM-14)[175], except for section 3 and a classified annex.[176]

[171] Sec 2.3 - 2.13, 2.8, 3.7 (c) EO 12333; *Liu*, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, p 7, 10; *PCLOB*, Report on the Surveillance Program Operated Pursuant to Section 702 FISA, p 112.
[172] Sec 3.5 (a), (c), (e), (f), (i) EO 12333.
[173] Sec 2.1 – 2.4 EO 12333.
[174] Presidential Policy Directive -- Signal Intelligence Activities (Jan 17, 2014) <obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (last retrieved Aug 13, 2023).
[175] National Security Memorandum on Partial Revocation of Presidential Policy Directive 28 (Oct. 7, 2023) <whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/> (last retrieved Aug. 13, 2023).
[176] Preamble, Sec 2, 4 (a) PPD-28; Sec 5 (f) EO 14086; NSM-14; *PCLOB*, EO 12333, p 20.

In 1978, the congress enacted FISA expressly authorizing foreign intelligence surveillance as a result of investigations of Federal surveillance activities conducted in the name of national security. FISA initially only governed electronic surveillance and collection of foreign intelligence information but has been significantly extended throughout the years to the use of pen registers and trap and trace devices, physical searches, and business records.[177]

FISA was intended to balance the divergent interests between the judicial and executive branch: on the one side FISA does exclude the judicial oversight by authorizing warrantless surveillance for certain procedures, on the other side it involved the US Congress as authorization party by passing FISA as a law despite the US President's exclusive power for national security. FISA describes the procedure how the executive branch is allowed to conduct foreign intelligence surveillance – with or without a warrant.[178]

In response to the 9/11 terrorist attacks in 2001, the USA PATRIOT Act was swiftly passed by US Congress which not only modified FISA but many US electronic communications laws including the ECPA and gave US federal law enforcement the authority to an extended electronic surveillance to combat terrorism. It also targets the financial services industry to assist US law enforcement agencies to detect terrorist acts in the US and around the world and included measures to prevent, detect and prosecute international money laundering and financing of terrorism and special scrutiny of such institutions and financial transactions.[179] With the enactment of FISAAA in 2008, Title VII of FISA, including FISA 702 provision, was introduced by the Bush administration and added a new chapter for intelligence surveillance targeting persons outside the US. Since then, surveillance and searches inside the US of US and non-US persons located outside the US are covered under FISA. Prior to that, it was governed by EO 12333 which created since then an overlap between those two legal statutes. The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015)[180]

[177] *Bureau of Justice Assistance*, FISA Background.
[178] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.4.1.
[179] *Treasury Financial Crimes Enforcement Network*, USA Patriot Act.
[180] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Publ. L. 114–23, 129 Stat. 268 (June 2, 2015) <congress.gov/114/plaws/publ23/PLAW-114publ23.pdf> (last retrieved Aug. 13, 2023).

reformed and extended authorities relating to foreign intelligence gathering and for other purposes.[181]

The current FISA regulation is commonly distinguished between the so called "traditional FISA"[182] for electronic surveillance and physical search investigations targeting US and non-US persons inside the US, FISA 702[183] for targeting non-US persons outside the US, and FISA 703 and 704[184] for targeting US persons outside the US. The evidence collection itself, however, is in any of aforementioned cases within the US.[185]

For traditional FISA searches it requires a warrant issued by the FISC which is granted when the court has probable cause to believe that the target of the electronic surveillance or physical search is a foreign power and meets the formal requirements. Bulk collection is not authorized. Similarly, a court order based on Sections 703 and 704 FISA searches requires probable cause that the US person targeted is reasonably believed to be outside the US and a foreign power and the request must meet formal requirements as set out in the respective sections.[186]

One exception to a FISC order for electronic surveillance and physical searches is in case the US President authorizes the measures through the Attorney General (AG)'s certification that the acquired information is solely related to foreign powers, there is no substantial likelihood that information of a US person will be acquired, and minimization procedures outlined in FISA are respected.[187]

In contrast, FISA 702 requires the FISC to approve an annual surveillance program targeting non-US persons. FISA 702 provides the IC with a FISC approved authorization for up to one year of the targeting of persons for foreign intelligence purposes which are reasonably believed to be outside the US. The FISC issues an order approving the applied targeting procedures on the determination whether the requested targeting procedures (1) are limited to persons outside the US, (2) are in accordance with required minimization

[181] *H.R. Judiciary Committee*, USA Freedom Act; *Liu*, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, p 4; *ODNI*, Description of Civil Liberties and Privacy Protections Incorporated in the 2008 Revision of EO 12333, p 5.
[182] = 50 U.S.C. §§ 1801-1829 (subchapter I and II, also known as Title I and III FISA).
[183] = 50 U.S.C. § 1881a.
[184] = 50 U.S.C. §§ 1881b, 1881c.
[185] *ODNI*, Annual statistical transparency report CY 2022, p11.
[186] 50. U.S.C. §§ 1803-1805, 1823-1824, 1881b, 1881c; *ODNI*, Annual statistical transparency report CY 2022, p 11.
[187] 50. U.S.C. §§ 1802; 1822.

procedures, the FISA 702 limitations and the Fourth Amendment, (3) significant purpose is the acquisition of foreign intelligence information and (4) need assistance from electronic communication providers. Once the program is FISC approved, the AG and DNI may thereafter issue directives to electronic communication providers based on such FISC authorization.[188]

Which type of sought data are covered is not defined under FISA 702 and may encompass any type of data as approved by the FISC order and requested by the directive. FISA's definition of *electronic communication service provider* in Title VII encompasses a wide range of different companies and refers to other statutes with ambiguous meanings. According to *Vladeck*, whether a company acts as an electronic communications service provider is solely context dependent. Once a company meets the definition, and may it only be for a small portion of its business activities, FISA 702 requirements apply to them for the entire business and data they possess. The US government argues that most companies do not possess any data in the IC's interest and are therefore not issued with any order or directive.[189]

Title VII of FISA including Section 702 expires on December 31, 2023, unless Congress reauthorizes its provision and extends its applicability. The NSA urges for a renewal by arguing that the program saved a lot of lives. Critics inside the US including many privacy organizations and some politicians raise concerns about the program that a re-authorization without any changes poses substantial risks to US persons, as FISA 702 is being used to circumvent stricter procedures due to its lack of transparency and its backdoor to a warrantless mass surveillance of US persons. [190]

In 2022, EO 14086 was issued by US President Biden which restricted the far-reaching application of EO 12333 and FISA only to intelligence activities in pursuit of legitimate objectives. It includes the limitation of bulk collection and the retention and dissemination of collected data and addressed a redress mechanism for targeted individuals. Further, it

[188] 50 U.S.C. § 1881a, in particular (a), (b), (h), (i).
[189] 50. U.S.C. §§ 1881 (b) (4), 1881a (i) (4) (G) and (5);*Vladeck*, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, p 4-7; *DoC/DoJ/ODNI*, U.S. Privacy Safeguards Relevant after EU-US Data Transfers after Schrems II, p 2.
[190] 50 U.S.C. §§ 1881-1881g (subchapter VI); *Liu*, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, p 2; *Riley*, NSA director urges Congress to renew controversial intelligence authority; *Jayapal*, Jayapal Davidson Bipartisan Statement on Privacy Protections for Americans; *Carney*, A coalition of privacy-minded outside groups and lawmakers.

describes the process how the defined legitimate objectives and the general implementation of EO 14086 should be incorporated into the IC's priorities and policies.[191]

IC agencies must align their existing policies and procedures in consultation with the AG, the Civil Liberties Protection Officer within the Office of the Director of National Intelligence (CLPO) and PCLOB until October 7, 2023, with the new requirements and publicly release them to the maximum extent possible. On July 3, 2023, the DoC already announced that the IC has adopted its policies and procedures in accordance with EO 14086 which shall become effective upon the implementation DPF adequacy decision. Eleven IC internal policies are unclassified and available to the public.[192]

The EDPB comments on EO 14086 in its opinion on the DPF draft, that some objectives are quite general. The US President is further authorized to issue additional objectives which may not be made available to the public if deemed necessary. The public release of updated policies and procedures is also conditional based on "*the maximum extent possible"*.[193]

3.2.2.2. Necessity and proportionality

EO 14086 has introduced the principles of necessity and proportionality related to intelligence activities. It shall guarantee a balance between validated intelligence priorities and the effect on all persons' privacy and civil liberties. This is done through the National Intelligence Priorities Framework (NIPF), established by the Director of National Intelligence (DNI), assessed by the CLPO whether it meets the principles of EO 14086 and presented to the US President. NIPFs are classified and not available to the public, therefore not assessable under a TIA.[194]

3.2.2.3. Oversight

EO 12333 differs between US and non-US persons which also reflects its oversight. Any activity against a US person in- or outside the US or activities undertaken inside the US as

[191] Sec 2 (b)(i), (b) (ii), (c)(ii), (c)(iii), Sec 4 (b) EO 14086; *Liu*, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, p 10 et seq.
[192] Sec 2 (b) (iii) and (c) (B) and (C) EO 14086; *ODNI*, IC Procedures Implementing New Safeguards in EO 14086; *DoC*, Statement on the European Union-U.S. Data Privacy Framework.
[193] *EDPB*, Opinion 05/2023 Rec 115, 117, 121
[194] Sec 2 (a) (ii) (A) and (B), Sec 2 (b) (iii) (A) EO 14086; Sec 2 (c) of the National Security Memorandum on The President's Intelligence Priorities (July 12, 2022) <whitehouse.gov/briefing-room/statements-releases/2022/07/12/national-security-memorandum-on-the-presidents-intelligence-priorities/> (last retrieved Aug. 13, 2023) (NSM-12).

well as the use of gained information is limited and must be in accordance with appliable law and the US Constitution. If any activity under the EO would be considered as an ordinary law enforcement where a warrant would be required, the intelligence activity needs to be approved by the AG and may only be granted in case there is probable cause to believe that such measures are used against a foreign power or an agent thereof.[195]

EO 12333 also refers to congressional oversight in accordance with procedures outlined in the National Security Act of 1947[196]. FISA stipulates specific congressional oversight requirements per title. Furthermore, the Privacy and Civil Liberties Oversight Board (PCLOB) established in 2007 as independent agency within the executive branch has oversight power to conduct reviews and give advice. Additionally, the President's Intelligence Advisory Board, the Intelligence Oversight Board as well as several Inspectors General and privacy civil liberties officers per IC provide advice and ensure compliance.[197]

FISA introduced a special US Federal court, the US Foreign Intelligence Surveillance Court (FISC). It contains eleven district judges which have jurisdiction to hear applications and grant orders. The FISC holds its sessions nonpublic, ex-parte with the government as only party present. In case of a denial of the surveillance request, the decision can be challenged by the FISC of Review (FISCR).[198]

An electronic service provider receiving a directive under FISA 702 may challenge the directive with the FISC. The FISC may only grant such petition in case the directive doesn't meet FISA 702 requirements or is otherwise unlawful. In case the FISC confirms the directive, or the provider fails to comply with a FISA 702 directive, the provider may be punished as contempt of court, which includes escalating fines and other remedies.[199]

[195] Part I sec. 1.4, part II sec 2.3, 2.5, part III sec 3.5 (c), (h) EO 12333; *Liu*, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, p 10.
[196] National Security Act of 1947, Pub. L. 80–253, 61 Stat. 495 (July 26, 1947), as amended through Pub.L. 117–328 (Dec. 29, 2022) <govinfo.gov/content/pkg/COMPS-1493/pdf/COMPS-1493.pdf> (last retrieved Aug. 13, 2023) = 50 U.S.C. §§ 3001 et seq. (2023).
[197] Sec 3.1 EO 12333 in accordance with 50 U.S.C. §§ 3091 et seq. (= subchapter III of the National Security Act of 1947); 42 U.S.C. § 2000 ee (d) (1); 50 U.S.C. §§ 1808, 1826, 1846, 1863, 1881f.; *PCLOB*, EO 12333, p 1 Fn 1, 11, 23.
[198] 50 U.S.C. § 1803.
[199] 50. U.S.C. §§ 1881 (b) (4), 1881a (i) (4) (G) and (5); *Vladeck*, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, p 4-7.

3.2.2.4. Redress

While intelligence activities under EO 12333 are primarily the clandestine collection of foreign intelligence, affected individuals are not informed nor aware of any surveillance. As defined by EO 12333 electronic surveillance relates to the acquisition of a nonpublic communication without the consent of the targeted person. There is no direct consequence for companies not complying with EO 12333 since the EO is an implementation policy for covered IC activities in how to collect intelligence information and has therefore no direct effect on companies. Indirectly, however, through statutes such as FISA or the ECPA, EO 12333 does have noncompliance provisions against providers. The same applies to redress options, since the EO itself is not enforceable by any third party against the US.[200]

FISA provides different redress options for aggrieved persons, namely civil liability claims against the person violating the procedures, civil actions against the US for willful violations of specific FISA provisions regarding the use of information and civil actions under the Administrative Procedure Act (APA)[201].[202]

IC activities still raise a lot of concerns regarding transparency and are hard to challenge due to the secretive nature of the programs under the state's secrets privilege. Even if individuals can plausibly allege that their data was unlawfully acquired by US authorities, there is barely any chance to prove that they were targeted. The American Civil Liberties Union and Knight First Amendment Institute on behalf of the Wikimedia Foundation challenged NSA's warrantless interception of online communication data. In February 2023, the US Supreme Court declined to hear the case regarding NSA's FISA 702 surveillance "upstream" program by siding NSA's argument that a trial would reveal sensitive state secrets.[203]

EO 14086 established an entitlement and redress mechanism for individuals targeted by signal intelligence. Individuals now have the option to file qualifying complaints to the CLPO. A qualifying complaint must lay down the reasonable belief of the complainant that its data has been transferred to the US but without the need to actually demonstrate that he

[200] Sec 1,1, 3.1, 3.2, 3.5 (c), 3.5 (g), 3.7 (c) EO 12333.
[201] Administrative Procedure Act = 5 U.S.C. §§ 551-559 (2023).
[202] 18 U.S.C. § 2712 in accordance with 50 U.S.C. §§ 1806, 1825, 1845; 50 U.S.C. § 1810; 5 U.S.C. § 702.
[203] *Riley*, Wikimedia wants the Supreme Court to hear case over NSA surveillance; *Riley*, Supreme Court declines to hear Wikimedia case against NSA surveillance program; *Vladeck*, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, p 17 et seq.

or she is or was subject to intelligence activities. Additionally, EO 14086 required the AG to establish the DPRC encompassing selected data privacy and national security legal professionals to review determinations made by the CLPO on request by a complainant or the IC. Determinations made by the CLPO and the DPRC are classified. The complainant receives information about the outcome through the designated authority in the qualifying state whether the review did or did not reveal any violation or whether remediations were issued. The complainant however will not receive any information whether it has been subject to intelligence activities.[204]

3.2.3. Electronic Communications Privacy Act

3.2.3.1. Clear, precise, accessible rules

The ECPA is a main piece of US federal legislation which governs the access to electronic data and their surveillance by governmental agencies for law enforcement purposes. It also contains provisions regarding national security procedures. With the further rise of computers and cell phones in the 1980s, the US Congress passed the ECPA in 1986 to protect electronic communication from unreasonable governmental access. It also updated the Wiretap Act of 1968[205], which addressed the interception of conversations using "hard" telephone lines but did not apply to interceptions of computer and other digital and electronic communications. The ECPA was passed in 1986 after the US Supreme Court's decision that the Fourth Amendment is not applicable to pen registers and hence no search warrant is needed. The ECPA therefore lays out its own requirements for law enforcement how to obtain data, which are in some cases not as strict as a classic probable cause search warrant.[206]

Throughout the years, the ECPA has significantly been amended by several pieces of legislation such as the Communications Assistance to Law Enforcement Act in 1994 (CALEA)[207], the USA PATRIOT Act of 2001, the USA PATRIOT Act Additional

[204] Sec 3, 4 (k), 5 (h) EO 14086.
[205] Wire and Electronic Communication Interception and Interception of Oral Communications = 18 U.S.C Ch 119 §§ 2510 et seq (2023).
[206] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.2.
[207] Communications Assistance to Law Enforcement Act of 1994, Pub. L. 103–414, 108 Stat. 4279 (Oct. 25, 1994) <govinfo.gov/content/pkg/STATUTE-108/pdf/STATUTE-108-Pg4279.pdf> (last retrieved Aug. 13, 2023).

Reauthorizing Amendments Act of 2006[208], the FISAAA in 2008 and the CLOUD Act. Such statutes aimed to clarify and update the ECPA by including new technologies and methods, and to ease restrictions on law enforcement how to access stored communications.[209]

While the ECPA not only went through several legislative changes, it has also been shaped by case law due to the evolving technology and outdated language. The ECPA not only extended to some extent the Fourth Amendment rights to electronic communication, it also created ambiguity related to data accessibility when it came to cross border data sharing. One example: on the one side the SCA as part of the ECPA introduced in 1986 prohibited US companies to share data with foreign law enforcement agencies. This was a huge burden for the US government due to the vast amount of foreign data access requests received from other counties. On the other side, it wasn't clear whether the SCA applied to data stored outside the US. This ambiguity led to different judicial outcomes over the last decades.[210]

Since the 80's, the US jurisprudence uses the commonly known "*Bank of Nova Scotia doctrine*" to determine whether information stored outside the US can be produced for evidence in a US case. The doctrine is a comity analysis which analyzes competing interests in requiring and preventing the disclosure of sought information stored outside the US.[211]

US courts, however, came to different conclusions whether the SCA applied to data stored outside the US: In *Microsoft Ireland*[212] the Second Circuit Court of Appeals focused on the data location and held in 2016 that data stored outside the US do not have to be provided to the US government. In *Google Pennsylvania*[213], a US District Court determined the SCA's applicability based on where sought data is accessed (in this case US) and held in

[208] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 192 (Mar. 9, 2006) <govinfo.gov/content/pkg/STATUTE-120/pdf/STATUTE-120-Pg192.pdf> (last retrieved Aug. 13, 2023).
[209] *Bureau of Justice Assistance*, ECPA, Background.
[210] *Klumpp*, International Impact of the CLOUD Act and Suggested Amendments to Improve Foreign Relations, p 616.
[211] *Hemmings/Srinivasan/Sreenidhi/Swire*, Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act, p 638, 644 et seq; In the *Bank of Nova Scotia* case, the court had to determine whether financial documents stored in the Caribbean bank's branches must be handed over even though such disclosure would infringe bank secrecy laws, *United States v. Bank of Nova Scotia*, 740 F.2d 817 (1984).
[212] *Microsoft Corp. v. United States*, 829 F.3d 197 (2016).
[213] *Google Pennsylvania*, 232 F. Supp. 3d 708 (2017).

2017 that Google was obligated to provide the FBI with electronic evidence stored outside the US pursuant to a § 2703 SCA warrant.[214]

The US Supreme Court was supposed to determine in *Microsoft Corp. v. United States*[215] whether the SCA applied to data stored outside the US. Before the US Supreme Court, however, could resolve the question and rule on the matter, the US Congress passed the CLOUD Act in March 2018. The US Supreme Court therefore moved to vacate the judgement of the Courts of Appeals and remand the case with instructions to dismiss the case as moot. [216]

The CLOUD Act aims to clarify this ambiguity whether cloud service provider must hand over data stored abroad when receiving a warrant issued by US authorities under 18 U.S.C. § 2703. The purpose is to expedite access to electronic information held by US based global providers by providing an efficient, privacy and civil liberties-protective approach for cross-border data sharing to protect public safety and combat serious crime. and to give US companies clarity when facing potential conflicting legal obligations regarding the disclosure of such data. It provides law enforcement authorities in criminal investigations with timely access to electronic data held by communications-service providers stored in foreign countries by forcing companies falling under US jurisdiction to hand over data stored outside the US through domestic US legal processes.[217]

In exchange, the CLOUD Act authorizes the AG in concurrence with the US Secretary of State to enter into data sharing executive agreements with foreign governments for direct access requests to non-US persons data stored by companies falling under US jurisdiction. Designated authority to implement executive agreements under the CLOUD Act is the Office of International Affairs. So far, the US executed 2 CLOUD Act agreements with the United Kingdom and Australia. Canada and the US have started negotiations in March 2022.[218]

[214] *Schwartz*, Legal Access to the Global Cloud, p 1693.
[215] *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).
[216] *Id*, 1188.
[217] Sec. 102 (1) - (4) COULD Act; *DoJ*, The Purpose and Impact of the CLOUD Act, p 2; *Klumpp*, International Impact of the CLOUD Act and Suggested Amendments to Improve Foreign Relations, p 615.
[218] 18 U.S.C. § 2523 (b); *DoJ*, Regarding Cloud Act Executive Agreements; *DoJ*, Cloud Act Resources; *DoJ*, United States and Canada Welcome Negotiations of a CLOUD Act Agreement.

Due to its now clearly stated wide extraterritorial applicability it also created a conflict of laws with non-US (data privacy) regimes, in particular in relation to GDPR, and therefore received mixed international and domestic responses.[219]

Similar to the CLOUD Act, two earlier proposed bills failed to amend the ECPA: the Law Enforcement Access to Data Stored Abroad Act (LEADS Act)[220] in 2015 which was only focused on extraterritorial content of electronic communication of US persons as well as the International Communications Privacy Act (ICPA)[221] in 2017, where the ICPA already tried to extend the scope to any customer or subscribers and introduced the idea of qualifying foreign countries.[222]

The CLOUD Act amended the ECPA in following sections:

- Title I: Wire and Electronic Communication Interception and Interception of Oral Communications (Wiretap Act)[223] as amended by the CLOUD Act in 18 U.S.C. §§ 2511 (2) (j) and 2523, which governs interceptions of communications;

- Title II: Stored Wire and Electronic Communications and Transactional Records Access, commonly known as Stored Communications Act (SCA)[224] as amended by the CLOUD Act in 18 U.S.C. §§ 2702 (b) (9), 2702 (c) (7), 2703 (h), 2707 (e) (3) and 2713. The SCA governs the contents and records stored by service providers; and

- Title III: Pen Registers and Trap Trace Devices (Pen Register Act)[225] as amended by the CLOUD Act in 18 U.S.C. §§ 3121 (a), 3124 (d) and 3124 (e), which governs the use of pen registers and trap and trace devices.[226]

[219] *Klumpp*, International Impact of the CLOUD Act and Suggested Amendments to Improve Foreign Relations, p 616.
[220] Law Enforcement Access to Data Stored Abroad Act, S.512 – 114th Congress (2015-2016): A bill to amend title 18, United States Code, to safeguard data stored abroad from improper government access, and for other purposes (Feb, 12, 2015) <congress.gov/bill/114th-congress/senate-bill/512> (last retrieved Aug. 13, 2023).
[221] International Communications Privacy Act, S.1671 – 115th Congress (2017-2018): A bill to amend title 18, United States Code, to safeguard data stored abroad, and for other purposes (July 27, 2017) <congress.gov/bill/115th-congress/senate-bill/1671> (last retrieved Aug. 13, 2023).
[222] Sec 2 (4) LEADS Act; Sec 2 (4), Sec 3 (3) ICPA.
[223] = 18 U.S.C Ch 119 §§ 2510-2523 (2023).
[224] = 18 U.S.C Ch 121 §§ 2701-2713 (2023).
[225] = 18 U.S.C. Ch 206 §§ 3121-3127 (2023).
[226] *Bureau of Justice Assistance*, ECPA, Background.

The Wiretap Act

Intercepting communication is strictly regulated and includes wire communications such as phone calls or any other aural communication via a network, oral communications including hidden bugs or microphones as well as electronic communication including emails. The general rule is that any interception of aforementioned communication is prohibited unless an exception laid out in the Wiretap Act applies, including for example one party of the communication gives its consent.[227]

The Wiretap Act distinguishes between users who are authorized to use the services of a provider and computer trespassers who access the computer system without authorization and therefore have no reasonable expectation of privacy.[228]

Territorial scope of the Wiretap Act is the US. A court order authorizing wiretapping is within the territory of the court in which the judge is sitting. In case of law enforcement including special FBI investigations, a provider may intercept in case such provider has been provided with a court order or a certification that under applicable law no court order is required. Introduced with the PATRIOT Act, service providers can additionally grant law enforcement agencies voluntary access to their systems to perform interceptions of computer trespassers without the agencies needing to obtain a court order first. The CLOUD Act enabled the option for interception based on an order from a foreign government subject to an executive agreement. Interceptions conducted pursuant to FISA are specifically excluded from the coverage of the Wiretap Act.[229]

The Pen Register Act

A pen register is a device which "*records or decodes dialing, routing, addressing or signaling information*" from transmitted a wire or electronic communication, while a trap and trace device is a device capturing incoming impulses which identify the originating number or any other information likely to identify the source of a wire or electronic communication. Both definitions do not include the content of the communication.[230]

[227] 18 U.S.C. §§ 2510 (1), 2510 (2), 2510 (12), 2511.
[228] 18 U.S.C. §§ 2510 (13), 2510 (21).
[229] 18 U.S.C. § 2511 (2) (a) (ii), (2) (e), (2) (f), (2) (j); 2516, 2518 (3), (7); *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.1.2.
[230] 18 U.S.C. §§ 3127 (3) and (4).

The Pen Register Act prohibits a general installation of such devices without a court order pursuant to 18 U.S.C. § 3123 for criminal investigations, FISA for intelligence purposes or an order by a qualifying foreign country under a CLOUD Act executive agreement. Exceptions are made for service providers which use such registers and devices for testing, operating or maintaining services or protecting its property and services from unlawful use, as well as for cases where the user gave its consent.[231]

The SCA

Regarding access to electronic information stored in the cloud, the SCA is the most relevant part of the ECPA. Under the SCA, an electronic communication service or remote computing service provider must upon request of a governmental entity "*preserve backup or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody or control, regardless of whether such communication, record, or information is located within or outside the United States.*". These preservation orders require the provider to set up its technical ability for a temporary suspension of any deletion routines or data retention plans of sought data to comply with requested preservation.[232]

Affected data under the SCA are referred to either "*content*" which includes information of the substance, purport or meaning of such communication, or "*records*" which are non-content data of electronic communications such as transmissions records and account information.[233]

Persons targeted by the SCA are without being further defined customers or subscribers. The SCA does not distinguish these terms on nationality or residency. In *Suzlon Energy Ltd. v. Microsoft Corp*.[234], a US court of appeals clarified that statutory protections under the ECPA are extended to non-US citizens for data physically maintained in the US and stored in the cloud. Only in cases of CLOUD Act executive agreements, the ECPA

[231] 18 U.S.C. §§ 3121 (a) – (c); 50 U.S.C. §§ 1841 et seq (subchapter III FISA).
[232] 18 U.S.C. §§ 2703 (f), 2713 = Sec. 103 (a) (1) COULD Act; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.1.2 and 13.3.3. *Ramos/Maciejewski/Jongen*, Application of the CLOUD Act to EU Entities, p 2; *Schwartz*, Legal Access to the Global Cloud, p 1714.
[233] 18 U.S.C. §§ 2703 (a)-(c), 2711 (1) in accordance with § 2510 (8); *Kerr*, A User's Guide to the SCA, p 14, 23-25.
[234] *Suzlon Energy Ltd. v. Microsoft Corp*., 671 F.3d 726 (2011).

distinguishes between US and non-US persons and provides US person with certain privileges.[235]

It could be assumed that the terms customers or subscribers under the SCA encompass individuals as well as any corporate entities which have a contractual relationship with such provider to use the services, whether it be directly or indirectly. However, when looking at the definition of a provider of electronic communication service (ECS), "*any service which provides to users thereof the ability to send or receive wire or electronic communications*", or remote computing service (RCS) "*provision to the public of computer storage or processing services by means of electronic communications system*", it shows that while RCS are defined by providing services to the public, the ECS meaning covers "*any*" services. Providers offering such services therefore include a variety of businesses, such as internet service providers, cloud services providers, telecommunication providers, and any other company storing data on behalf of its customers or subscribers. *Vladeck* emphasizes that ECS also includes companies providing email services to its employees and refers to specific case law. *Kerr* emphasizes that provider can either be ECS and RCS or not depending on the context.[236]

The SCA does not specify whether a provider must be located in the US or not. In any case, a foreign company must have personal jurisdiction in the US to have US courts being able to rule and possession, custody or control over sought data. The terms "*possession, custody or control"* as introduced in the CLOUD Act are not defined by the act itself nor any other provision of the ECPA. Assessed by US courts on a case-by-case basis, it generally depends on several factors, established by US jurisprudence over time, with two key elements focusing on legal and day-to-day control on sought data. Additionally, courts also weight in whether the entity where data is being sought is a party or non-party to the litigation.[237]

[235] 18 U.S.C. § 2703 (h) (1) (B), 2713; 18 U.S.C. § 2523 (a) (2); *Kerr*, A User's Guide to the SCA, p 6-8; see *supra* 3.2.1.7.
[236] 18 U.S.C. §§ 2510 (1), (12), (15) and § 3117, which comprises the definition "electronic communication service" including further definitions of wire and electronic communication; 18 U.S.C. §§ 2711 (1) and (2) in accordance with §§ 2510 (1), (12), (14), (17), which comprises the definition "remote computing service" including further definitions of wire and electronic communication, electronic communications system and electronic storage; *Vladeck*, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, p 7-8; *Kerr*, A User's Guide to the SCA, p 9-12.
[237] *Hemmings/Srinivasan/Sreenidhi/Swire*, Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act, p 632, 634, 636; *Ramos/Maciejewski/Jongen*, Application of the CLOUD Act to EU Entities, p 2.

Voluntary data disclosure under the ECPA

Due to the fast technological evolution, government surveillance relies more and more on data obtained by private companies as they collect a vast amount of (personal) data from individuals. Not only businesses but also society in its entirety shifted online which results in a constant and obligatory individuals' digital footprint. One result thereof can be seen in an increase of legal requests for data held by service providers.[238]

The SCA prohibits ECS when providing its services to the public and RCS to voluntary disclose records or other information pertaining to a subscriber or customer to US governmental entities (not including the content of customer communications). This prohibition does not limit data sharing with privately held companies. That means that providers can share, sell and/or transfer collected personal data to other third parties. Those third parties are most of the time not covered under the definition of a service provider under the SCA and are therefore permitted to disclose collected data to anyone, including US governmental agencies.[239]

To circumvent the lengthy legal process to obtain data held by private companies, US government entities are using this loophole to conduct warrantless mass surveillance by seeking this less transparent and non-judicial oversight way of a voluntary disclosure and legally buy bulk data directly from private companies. So-called data brokers play a major role in this process. Those are companies which collect – mostly personal – data from various and very often indirect sources including service providers regulated under the ECPA, combine and process received data and thereafter sell it to interested parties. Affected individuals are most of the time not even aware that data brokers possess and sell their data. But not only data brokers, US agencies more and more reach out to private owners of security cameras to disclose home security footage based on a voluntary cooperation.[240]

[238] *Chin*, Digital Dragnets, p 1.
[239] 18 U.S.C. § 2702 (a) (3), § 2702 (b) (7), § 2702 (c) (6); *Kerr*, A User's Guide to the SCA, p 15-17.
[240] *Alfred NG*, The privacy loophole in your doorbell; *Shenkman/Franklin/Nojeim/Thakur*, Legal Loopholes and Data for Dollars, p 7, 9; *Chin*, Digital Dragnets, p 1 et seq; *Cameron*, The FBI Just Admitted It Bought US Location Data; *Dearen/Burke*, Senators push to reform police's cellphone tracking tools.

The in 2021 proposed Fourth Amendment Is Not for Sale Act[241] is a bill trying to counteract against these warrantless law enforcement tactics and would force US agencies to follow the legal process to access sought data.

3.2.3.2. Necessity and proportionality

US law enforcement legislation balances national interests with the privacy rights of the targeted individuals and affected third parties based on the type of criminal offense. In general, the less severe the criminal offence, the higher the burden for the law enforcement agency to access sought data and the more severe the intrusion of privacy or the more sensitive sought data is, the higher the burden for law enforcement to obtain access. The ECPA therefore provides US governmental agencies with different legal processes on how to obtain sought information depending on which type of information requested and investigated punishable offense.[242]

While law enforcement procedures withing the US do not distinguish between US and non-US persons, it makes a difference when it comes to CLOUD Act executive agreement orders of qualifying foreign countries. While US persons are protected from access requests of foreign governments, non-US persons, no matter which nationality, do not have such benefit.[243]

3.2.3.3. Oversight

The general process in US federal matters such as FISA and ECPA are codified in the Fed. R. Crim. P. Judicial oversight for specific ECPA measures, such as subpoenas, warrants or other court orders thereunder are directly described in the statute. Except for NSLs, all legal procedures require the prior involvement of a court. Examples shown below are listed from the least to the strictest access requirements.[244]

Under the SCA, the FBI is authorized to issue NSLs for international terrorism and clandestine intelligence activities. Providers receiving an NSL thereunder must provide

[241] Fourth Amendment Is Not for Sale Act, S.1265 – 117th Congress (2021-2022): A bill to amend section 2702 of title 18, United States Code, to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, and for other purposes (Apr. 21, 2021) <congress.gov/bill/117th-congress/senate-bill/1265> (last retrieved Aug. 13, 2023).
[242] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.3.
[243] 18 U.S.C. § 2523 (b) (4).
[244] See *supra* 3.2.1.10; Rule 17 (subpoena), 41 (warrant) Fed. R. Crim. P; *Kerr*, A User's Guide to the SCA, p 17-19.

subscriber information, toll billing records and transaction records to the FBI in regard to an ongoing investigation. The provider receiving an NSL may challenge its enforcement. If an NSL is made known to the affected person, the person may challenge the gained information in court if it comes to a trial.[245]

A pen register or trap and trace order for the installation and use of such device within the US for the disclosure of non-content records regarding phone numbers and emails must be issued by a court ex parte and only needs to demonstrate that sought information are likely to be obtained by such measures and are relevant for an ongoing investigation.[246]

The SCA requires law enforcement agencies to obtain either a warrant or a court order to access customer data held by an ECS or RSP. An order under the SCA, so called "§ 2703 (d) order", to access any stored content of records is a combination between a subpoena and a warrant. It requires "*specific and articulable facts showing that there are reasonable grounds*" relevant for a criminal investigation. In contrast, a traditional search warrant under Fourth Amendment requires probable cause of a crime. This is used for example as the legal standard for MLAT requests. The DoJ emphasized that the CLOUD Act does not create any new form of warrant but only clarifies already existing disclosure obligations for providers under the SCA.[247]

An order for a telephone wiretap must show probable cause that a crime has been, is, or will be committed and must meet the requirements laid out in the Wiretap Act.[248]

In addition to the above domestic legal processes, an order issued directly to a provider by a qualifying foreign country under the CLOUD Act refers to authorization and oversight mechanisms of its own domestic law. The determination or certification by the AG in assigning a qualifying foreign country has no judicial or administrative oversight within the US, but the US congress may enact a joint resolution of disapproval.[249]

---

[245] 18 U.S.C. § 2709.
[246] 18 U.S.C. § 3123(a), § 3127 (3) and (4); *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.3.4.
[247] 18 U.S.C. § 2703(d); *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.8; *Schwartz*, Legal Access to the Global Cloud, p 1683; *.DoJ*, The Purpose and Impact of the CLOUD Act, FAQ 18 p 15.
[248] 18 U.S.C. §§ 2516, 2518; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.1.2, Ch 13.3.3.
[249] 18 U.S.C. §§ 2523 (b) (4) (D) (v), (c), (d) (2) and (4); *DoJ*, The Purpose and Impact of the CLOUD Act, p 12.

3.2.3.4. Redress

The ECPA mandates providers how to provide access to information for law enforcement purposes. A provider faces legal penalties when not following the legal procedure (whether to grant access to information which shouldn't have been granted or vice versa). Provider's duties how to design their products and services to ensure cooperation and compliance with law enforcement requirements regarding the interception of communications is laid out in CALEA. A court may direct a provider to comply with CALEA and may impose a civil penalty of up to USD 10,000 per day in case a provider fails to comply with a court authorized interception, pen register or trap a trace device.[250]

If a provider receives a warrant or legal order according to the qualifying foreign government requirements, and is being required to disclose the content of a wire or electronic communication, it has the option to file a motion to modify or quash the legal process within 14 days if it reasonably believes that the customer is not an US person, does not reside in the US, and such disclosure would violate the laws of a qualifying foreign government. That means if the warrant or subpoena targets any record or other information pertaining to a customer or subscriber, or the customer or subscriber is a US citizen or the disclosure is requested for data stored in countries which do not have an executive agreement with the US in place, regardless of whether their laws would be violated or not, the provider has no option to challenge the request. [251]

Upon receipt and after response from the governmental entity which issued the legal process, the court may modify or quash the legal process if it finds that (i) the disclosure would infringe laws of a qualifying foreign government, (ii) the comity analysis determined a modification or quash of the legal process and (iii) the customer or subscriber is not a US person or resides in the US. Based on eight factors, the comity analysis in the SCA shall balance all circumstances and divergent interests of the challenged request to determine whether the foreign legal process in requesting the provider to disclose sought data is appropriate.[252]

[250] 18 U.S.C. § 2522 and 3124; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.4.
[251] 18 U.S.C. § 2703 (h) (2) (A) in accordance with 18 U.S.C. § 2523.
[252] 18 U.S.C. § 2703 (h) (2) (B) and (3).

In case no CLOUD Act executive agreement is in place, a provider can challenge a search warrant issued under SCA based on a general comity analysis pursuant to common law standards.[253]

Anyone aggrieved by a violation of the SCA may bring civil actions for appropriate relieve, actual damages with no less than USD 1,000 and reasonable litigation costs against the person which knowingly or intentionally violated the statute. If a court determines that a US agency has willfully or intentionally violated the SCA, the respective agency must initiate a proceeding for disciplinary action against the officer regarding claimed violation.[254]

A knowingly unlawful installation of a pen register or trap and trace device is fined or imprisoned for not more than one year.[255]

The Wiretap Act provides any person which communication is unlawfully intercepted, disclosed or used with the right of private action against the violating party. An unlawful interception, disclosure or use of information under the Wiretap Act may lead to a fine and/or up to five years imprisonment and additionally provides a private right of action including injunctive relief, compensatory damages, punitive damages, attorney's fees and other reasonable litigation costs.[256]

Civil actions against the US to recover actual damages not less than USD 10,000 and litigation costs may be filed by an aggrieved person due to a willful violation the SCA, Wiretap Act or under specific FISA regulations, namely in case when information acquired from an electronic surveillance, physical search or pen register or trap and trace device if used and disclosed unlawfully by a federal officer or in case of US persons if used and disclosed in non-compliance with minimization procedures. Disciplinary action may be initiated by the affected US agency against an officer in case the court determines a willful or intentional violation has been set.[257]

[253] §103 (c) CLOUD Act; *Schwartz*, Legal Access to the Global Cloud, p 1716.
[254] 18 U.S.C. § 2707.
[255] 18 U.S.C. § 3121 (d).
[256] 18 U.S.C. §§ 2511 (4) (a), 2512 (1), 2520.
[257] 18 U.S.C. § 2712 in accordance with 50 U.S.C. §§ 1806 (a), 1825 (a) and 1845 (a).

In addition to redress options stated in the ECPA, offensive monitoring may give rise to claims under state invasion of privacy or any other common-law claims.[258]

3.2.4. TIA (in)compatibility conclusion

The US as a federal, representative, democratic republic is founded on its constitution. It consists of a separation of powers as well as judicial oversight of the executive branch and national security matters. There is a common interest on EU and US side in strengthening transatlantic partnership and economy, which can also be seen in the international commitment on both sides, such as OECD guidelines adoption. The US' data protection landscape consists of sector-specific and state privacy laws and does not have an overarching regulation. The EC's DPF adequacy decision shows common ground and appropriateness of both legal regimes regarding data privacy on a political level when additional privacy principles are implemented by self-certified business.[259]

The CJEU already ruled that EO 12333 and FISA do not provide an equivalent protection due to its unrestricted mass surveillance authorization. PPD 28 limitations and safeguards were insufficient to provide an appropriate guarantee. These provisions have not changed since then. Consequently, in my view EO 12333 continues to bear risks of unproportional surveillance for data exporters, especially for personal and non-public data in transit to the US. Despite the US statement that most data are not in the interest of the US government, access based on EO 12333 while data is in transit cannot be ruled out.[260]

Under EU standards, sought data can be collected for law enforcement or national security purposes to follow a legitimate objective if the processing is necessary and proportionate. The CJEU ruled that a member state's objective of protecting national security justifies a more severe interference due to its importance, provided that the member state encounters a serious genuine and present or foreseeable threat, and the interference meets the requirements outlined in Art 52 (1) of the Charter. In *Schrems II* the CJEU clarified that any unlimited mass surveillance programs for foreign intelligence collection is unjustified and does not ensure an adequate level of protection.[261]

---

[258] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.3.
[259] *Swire*, US Surveillance Law, Safe Harbor, and Reforms Since 2013, December 2015, p.3; *H.R.,* Our American Government, sec 2.
[260] See *supra* 3.2.2.1; C-311/18 (*Schrems II*) Rec 179-185.
[261] *EDPB*, Recommendations 02/2020 Rec 34, 36; Joined cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net ao*) Rec 135-139, 177; C-311/18 (*Schrems II*) Rec 180.

The CJEU clarified that legislative measures for the purposes of safeguarding national security or combating serious crime are not precluded for the "*targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary"* subject to "*compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse"*.[262] Furthermore, Art 21 (2) of the Charter prohibits any discrimination based on nationality.[263]

As assessed above, national security regulations are not fully clear and still contain classified sections related to their applicability and enforcement which makes it impossible for a data exporter to make a hard fact assessment of the actual impact. In practice, data shown in the past must provide an estimate of future developments and potential risks. This leads to uncertainty. Until there is no clear ruling by the CJEU that US national security measures are essentially equivalent to EU standards or until US laws do not materially change by at least defining a clear scope and applicability, data exporters should in my view continue to be cautious.

Necessity and proportionality are in my view only given if US and non-US persons are treated equally. This would show that the rule of law is unbiased and would target a specific purpose and goal and not per se a person based on their nationality. There is no founded reason as to why US and non-US persons are treated differently for purposes of national security or in cases of onward transfers based on CLOUD Act executive agreements, except that the US constitution does not provide the same protection to non-US persons. Law enforcement and national security should target the objective purpose, namely combatting crime and protecting its nation. Focusing on the type of target (US or non-US person) has no objective purpose in controlling governmental agencies and their actions. Sec 1 EO 14086 states that signal intelligence should treat all persons with dignity and respect and that all persons have legitimate privacy interests. If a country sees specific governmental activities as necessary to achieve certain national security or law enforcement objectives, why is it necessary to have different programs whether the target is a US or non-US person? A threat from the inside can be as harmful and devastating, which could be

[262] C-140/20 *(G.D.)* 1st ruling.
[263] Art 21 (2) of the Charter.

witnessed with the January 6 attacks on the US capitol. Consequently, only equal treatment or justifiable unequal treatment would meet EU standards, especially the Charter.

As stated above, FISA 702 is currently in debate whether it will be extended. The wide concern inside the US for the adequate protection of US persons is an observation which should also reflect on the data handling of non-US persons by this program and whether this provision is strictly necessary and proportionate to reach intended goals. If this provision is already seen as unconstitutional within the US, a general question for its proportionality should be raised not just for US but also non-US persons. Whether EO 14086 changes FISA 702 in practice remains a challenging adequacy assessment due to many classified portions of the program.[264]

The newly enacted EO 14086 provides a number of new limitations for the IC on how to gather foreign intelligence and specifically includes non-US citizens in its safeguards. It also introduced the principles of necessity and proportionality as well as a new oversight mechanisms for non-US persons of qualifying states with a less restrictive burden for the complainant of violation and standing allegations. While redress mechanisms for individuals, especially for non-US persons have significantly improved, especially because of the elimination of standing requirements, a lot of activities and procedures authorized under EO 12333 as well as EO 14086 are still classified without disclosure to the public.[265]

These changes are a big step towards an equivalent level of EU data protection standards. The impact of and how EO 14086 will be lived in practice, however, will remain seen. So far, there is no guideline for what is necessary and proportionate. Furthermore, a lot of measures are still classified, and existing ones can be overruled by national security interests, including publicity requirements of updates or program changes. It remains in my view an approach which is built on trust that the US system is controlling itself appropriately. Appropriately in this context must, however, not just be considered from the US side but also meet an equivalent level of EU standards. Even though EO 14086 limits the access to personal data by the IC and provides data subjects with a redress mechanism, any data transfer to the US, however, is potentially still be affected by an access from US agencies.[266]

[264] See *supra* 3.2.2.1.
[265] So also, *PCLOB*, EO 12333, p 6, 7; *EDPB*, Opinion 05/2023, sec 177-179.
[266] See *supra* 3.2.2.1.

As outlined above, any company under US jurisdiction may fall under the definitions of ECPA or FISA due to its broad and ambiguous scope. In practice the number of actually affected companies may most likely be less. This can, however, only be assumed by data exporters because of restricted disclosure provisions for access requests. Regardless of the actual affected companies, in accordance with *Schrems II* and the clarification in *Google Analytics II*, the decisive factor is whether US agencies have potentially the ability to access personal data and not if US agencies may have a potential interest. That means a factual or theoretical risk is sufficient.[267]

ECPA provisions are accessible to the public and lay out their restrictions. Any access to sought data by law enforcement agencies is regulated either in the ECPA or by the overarching general rules of law (e.g., Fourth Amendment requirements). The restrictions are necessary for fulfilling the interest of public security and proportionately based on the severity of interference due to a differentiated mechanism how to obtain data (from subpoena to court order). The implementation of independent oversight and redress options are granted to affected individuals which are not distinguished by the ECPA based on nationality. The rules are not fully clear and precise regarding the ECS and RCS definition and the exact type of data which can be obtained. However, since any order under the ECPA can be challenged by the provider, it is therefore in my view that the surveillance measures laid out in the ECPA meet the requirements of a level of protection essentially equivalent to the EU.[268]

While under US law enforcement processes how to obtain data and access is in my view clear, issues arise in cases where the data importer lawfully voluntarily discloses personal data to third parties which then provide the information to the government, where the US uses its domestic laws with extraterritorial reach and in cases of onward transfers due to CLOUD Act executive agreement data sharing practices and the unequal treatment of US and non-US persons. Although US federal law has certain restrictions for governmental agencies on how to process and obtain data for law enforcement purposes, loopholes such as the voluntary disclosure provision are abused for easy access to mass surveillance. This is the result of the separation of governmental and private sector data privacy regulations,

[267] See *supra* 3.2.2.1 and 3.2.3.1; C-311/18 (*Schrems II*) 180; DSB-D155.026 (*Google Analytics II*) D.4. b).
[268] Affirmative in analogy to the DPF and the general law enforcement assessment, see *EDPB*, Opinion 05/2023 Rec 81, 89, 92, 95-96.

which bears risks and unlocks misuse of collected data as it can be seen in cases of lawful voluntary disclosure.[269]

Even though the EC approved self-certified US companies under the DPF as adequate, legislation around national security and law enforcement remains problematic based on the reasons given above. Otherwise, the EC would also extend its adequacy decision to the entire country and not only self-certified countries abiding by the DPF privacy principles.[270]

Given the (in)compatibility reasons above, it is my overall assessment that US governmental access to electronically held personal data has significantly improved by EO 14086 for intelligence purposes but still cannot be ruled out. Based on a data exporter's accountability obligation to prove its compliance related to the data processing activities, any personal data transfer to the US falls in theory under national security regulations and in most instances within the applicability of the ECPA due to these laws' broad and not well-defined scope.

This outcome requires adequate supplemental measures to justify a transfer if the transfer is based on appropriate safeguards. Even though the risk in practice can be low for data exporters, it is part of the data exporter's accountability obligation not to ignore any known (potential) risk and provide evidence for an adequate level of protection for each data transfer. Known exposures must be assessed and adequately addressed with supplementary measures to guarantee that EU standards are not undermined, otherwise the data exporter faces legal consequences and full liability for its data handling.[271]

3.3.Solution approaches on governmental side

While controllers are accountable for their data handling procedures, support from the governmental side in strengthening international business benefits the marketplace and boosts the economy. This section should give some improvement suggestions on how to overcome aforementioned incompatibilities and addresses the research question of what can be done from governmental side to provide legal certainty.

[269] See *supra* 3.2.3.1.
[270] See *supra* 2.1.
[271] Art 5 (2), 44, 46 (1), 82, 83 GDPR; *EDPB*, Recommendations 01/2020[2] Rec 50; C-311/18 (*Schrems II*) Rec 131-134.

3.3.1. International commitments

In March 2023, the EU and US continued their negotiations for an international agreement regarding the access to electronic evidence for criminal law investigation purposes. A fully recognized international treaty, such as MLAT, would provide a legal basis for processing as well as the transfer of sought data for controllers or processors to the US.[272]

There is an urgent need for reciprocity among legal authorities when it comes to the enforcement of foreign judgements. The current MLAT process is slow and based on bilateral treaties between specific states. To strengthen the international law enforcement capabilities, a harmonized approach not just among two countries but on an international basis would bring clarity. Both the US as well as EU facing issues with the current MLAT system because it is too complicated and lengthy to keep up to date with today's criminal investigation requirements.[273]

Evidence stored in another country, becomes more and more attention for law enforcement and the question under which regulation can data be obtained. *Daskal* recommends that data location shouldn't be the only factor to determine which rules apply but suggests that jurisdiction could be based on the nature of the crime and government's prosecution interests, company's headquarters, user nationality or user location. *Schwartz* points out that a key factor to determine access to cloud data is the underlying cloud model.[274]

Many privacy advocates are stressing the need for a binding global treaty which sets a legal baseline, not only for governments to access private sector data, but also how to process and manage international data handling. In contrast, *Wood* is skeptical whether a global treaty to access cloud data would benefit the international law enforcement as he refers to the comity rules which are already in place and handle such matters and a treatment would only reach the lowest common denominator.[275]

[272] *EC*, EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations; *DoJ*, Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigation.
[273] *Schaar*, EAID: E-Evidence und CLOUD Act, p. 1; *Woods*, Against Data Exceptionalism, p 786-787; Sec 102 (1) and (2) CLOUD Act.
[274] *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13.3.8; *Schwartz*, Legal Access to the Global Cloud, p 1702-1704; *Daskal*, Law Enforcement Access to Data Across Borders, p 499.
[275] *LaCasse*, In wake of global data transfer complexity, need for multilateral treaty grows; *Schwartz*, Legal Access to the Global Cloud, p 1701; *Woods*, Against Data Exceptionalism, p 788.

In my view, most international treaties fail due to the fact to press two legal systems or sometimes even more into one. Finding the lowest common denominator and starting the process could help to cover at least some aspects of international legal assistance (e.g., defining a catalogue of criminal offences which fall under the treaty). Such a list can be regularly updated and extended, but the underlying process and the collaboration remain the same.

Since it is in the interest of the business to have secure investments, it needs legal certainty. In an era where data do not follow classic borders, our legal systems have to rethink the way they operate and change the understanding of territorial sovereignty to keep up with internet-based globalization. It should not be in any country's interest to "balkanize" itself from the outer world by thinking this would give them an advantage over other countries. This would harm inventions and growth. Creating a system which works for all stakeholders should be the goal. Not perfect, but a workable and adaptable solution to meet today's needs. Invention will happen anyway, with or without governments' ability to keep up. However, if governments want to be a respected party in this equation, legislative and procedures must be in line with new technology needs and abilities. Simplification is what's needed. Only if rules and regulations are simple a broad compliance can be achieved, which eventually should be the overall interest of data privacy to protect individuals and its personal data.[276]

Based on Art 42 GDPR and the World Intellectual Property Organization (WIPO) establishment and underlying international treaties, an international organization set up as one-stop shop for registration, certification, dispute resolution as well as for search warrants/subpoenas sent by a member states institution to a member states provider based on mutual ground of its member states. Such a system could provide a transparent catalogue of legit institutions, legal requirements, official forms, etc. Such an institution could also oversee data privacy regulations and act as an escrow for requested data. Every registered company and institution would be able to securely communicate through the privacy institution which would help international companies enormously to reduce friction and create a clear path as to how to be compliant. Companies could be assured about the legality of requested warrant, the limitation of liability regarding correctness of requested warrant, and institutions could be assured of a secure and timely transmission of requested evidence.

[276] In agreement *Daskal*, Law Enforcement Access to Data Across Borders, p 501.

The certification and registration process can be overseen by an international committee rather than each government. A public register and approval authority can give individuals security that companies with whom they are sharing their personal data meet the required standards of data protection. In my opinion, such a system would certainly strengthen the trust in data privacy and hence compliance.[277]

3.3.2. US side - strengthening privacy laws

There are several areas the US could strengthen their overall privacy protection. First, governmental agencies should not be allowed to access data which companies can voluntarily disclose. The right to disclose includes the sale of such data. For any set of data, a law enforcement agency seeks access to and held by a private company, governmental agencies should follow a clearly defined legal process when and how sought data must be handed over. Making data brokers public by registering with the Federal Trade Commission (FTC) as proposed in 2021 in the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act[278] to regulate commercial data purchases and voluntary data sharing agreements e.g., with data brokers is one way to stop warrantless mass surveillance. Additionally, privacy laws in the private sector must be strengthened and aligned to ensure that private companies have appropriate boundaries regarding data collection, retention, and sharing which would ultimately decrease access of governmental entities to individuals' data.[279]

Only if data privacy is treated as an overarching goal via an omnibus law such as the introduced ADPPA or on a constitutional level regulating data protection in its entirety including the governmental as well as private sector, it can tackle the root cause of excessive data collection and sharing.

3.3.3. EU Side – clarifying transfer mechanisms

Providing a catalog of acceptable and non-acceptable transfer mechanisms, legal statutes etc. where data exporters have a reliable source of trust would enormously help data

[277] Rec 100, Art 42, GDPR, which state that establishments of certification mechanisms and data protection seals and marks should be encouraged; see also *WIPO*, Madrid System.
[278] Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, S.2499 – 117th Congress (2021-2022): A bill to establish data privacy and data security protections for consumers in the United States (July 28, 2021) <congress.gov/bill/117th-congress/senate-bill/2499> (last retrieved Aug. 13, 2023).
[279] *Chin*, Digital Dragnets, p 6 et seq.

exporters in being certain of its compliance. The EDPB provides many guidelines and recommendations, however the overall (legal) assessment is still up to the companies which leads to uncertainty. Even though data processes change rapidly companies can still be provided with a clear rulebook when data can be shared with foreign governments or not, so it is not up to companies to fight against every order they receive.

Furthermore, the EU can improve compliance and alignment with data transfer obligations in providing data exporters with more and standardized appropriate safeguard tools, such as approved code of conducts or certification mechanisms. This would not only benefit in refraining from considering derogations, but also provide an overall transparency for application procedures.

Lastly, derogations should in my point of view not be neglected and reduced to such a narrow applicability scope. If the legislation provides derogations as options for a transfer – even though as last resort – the assessment by the EDPB of those shouldn't come to the conclusion that they are in practice not usable as valid transfer mechanisms but should in contrary provide more reliable use cases when it is acceptable.

4. Supplementary Measures

Supplementary measures require additional safeguards to the general security measures under GDPR and obligations set out in Art 46 GDPR, identified on a case-by-case basis in cases where an access to transferred personal data by US agencies is inadequate and cannot be ruled out. Such measures are divided into contractual, organizational, and technical ones and must often need to be combined in order to be an effective safeguard against an undermining of privacy protection. Especially contractual measurers alone cannot guarantee an adequate protection without the additional implementation of organizational and technical measures, since they only bind the contracting parties and not US authorities or third parties, and only so long as no legal obligation contradicts the with the agreed contractual provision.[280]

The TIA assessment in previous chapter was focused on defining risk for specific data transfers due to the applicable US legal framework in relation to the intended transfer tool and its alignment with EU standards, and whether inadequate US laws impinge the (contractual) obligations outlined in the chosen transfer tool. Supplementary measures on the other side put emphasis on eliminating the identified risks to guarantee an adequate level of protection in accordance with EU standards. In accordance with *Schrems II*, only those supplementary measures which can adequately address defined risks are deemed to be effective. Based on CJEU's ruling and EDPB's clarification, the Austrian DPA – among other Union DPAs – emphasized that in regard of Chapter V GDPR, there is no risk-based approach when assessing a countries' adequacy and choosing appropriate supplementary measures. There is only compliance or non-compliance whether transfer tools including supplementary measures are deemed effective to ensure adequate level of protection, because a risk-based can neither be derived from Art 44 GDPR, *Schrems II*, the new SCCs nor EDPB's recommendations. Adequate protection in this context means that data subject's rights are appropriately respected in compliance with GDPR and the Charter. Any political or economic interests are immaterial for this assessment.[281]

[280] *EDPB*, Recommendations 01/2020[2] Rec 50-58, 99; Rec 109 GDPR; C-311/18 (*Schrems II*) Rec 131-134.
[281] *EDPB*, Recommendations 01/2020[2] Rec 50, 56. 75; C-311/18 (*Schrems II*) Rec 131-134; DSB-D155.026 (*Google Analytics II*) D.4. b); BVwG W245 2252208-1/36E (*Google Analytics*) II.3.6.2.2.3; EDPB, Report 101 Task Force Rec 7.

While the Austrian DPA presented its argumentation comprehensively, the strict conclusion of a non-risk-based approach is not fully understandable and could in my point be an issue regarding interpretation of the terminology of "risk" and "circumstances". The Austria DPA understandably emphasizes that overall, the EU standard must be ensured regardless of the type of data. However, in agreement with *Fritz/Kirchmair*, every data transfer includes different types of data, undergoes different circumstances, engages with different actors and consequently may make laws differently applicable, which eventually leads to a different risk of each transfer depending on forementioned examples. *Schrems II*, the SCCs and the EDPB refer several times to an assessment "in practice" or "practices of the country". Contractual and organizational measures, such as the disclosure of transparency reports and written declarations about whether US access requests have occurred in the past, are required parts of the overall review. It would in my opinion not make any sense to have data exporters undergo through these extra steps of an assessment "in practice" if only the sheer factual application of inappropriate US laws determines an impingement, and the sole solution (if any) can only be achieved through technical measures by ensuring no personal data are in the access spere of US agencies. Choosing an appropriate technical measure alone can already be seen as risk assessment, e.g., if data can be identified under chosen anonymization or pseudonymization tools. Furthermore, any data transfer based on Art 46 GDPR, including intracompany transfers, would be an infringement if the US data importer has potential access to any type of personal data due to the factual risk that any US company may fall under FISA. This outcome would even make EU-US business communication illegal.[282]

Regardless of the critical appraisal and in accordance with the current jurisdictional requirements, the two key questions when it comes to finding appropriate supplementary measure for securing US governmental access to personal data are: 1) Does the US have personal jurisdiction over the data importer or sought data and 2) does the US data importer have possession, custody, or control over sought data? Based on these, following supplementary measures solutions for businesses can be presented.

[282] *Fritz/Kirchmair*, Drittstaatentransfers bei Cookies, 191-192; see examples for references to "in practice" assessments: C-311/18 (*Schrems II*) Rec 126, 137, 148, 158; SCC Int transfer 2021 EC (EU) 2021/914 Rec 19, 29, Clauses 8.5, 14 including Fn 12; see *infra* 4.3.1 and 4.3.2. regarding anonymization and pseudonymization.

4.1. Contractual measures

The new SCCs provide a very robust contractual framework for international data transfers when used as instructed and can certainly also be used as a contractual starting point for the other transfer tools. Additional contractual commitments are welcomed if not in contradiction with SCCs. Data exporters must ensure to contractually bind the data importer to agreed technical measures and put conditions for noncompliance in place, such as penalties and/or immediate termination.[283]

Other additional contractual measures are firm confidentiality clauses beyond personal data, stringent disclosure and cooperation requirements, obligation to challenge any request received by public authorities and information obligations towards the data exporter, supervisory authority as well as data subjects, obtaining a written declaration of data importer that the US company nor its sub processors fall under any legal obligation under any US surveillance laws.[284]

Contractual measures as stated herein require firm management of data exporters' recipients, including audits, regular assessments and attestations. Especially in a transatlantic context, control over a business partner is in practice associated with a financial burden and time-consuming measures. It is therefore advisable to retain as much control as possible in-house, which can be achieved through organizational and technical measures. Data exporters must ensure that the data importer is not allowed to transfer any data to a third party such as data brokers which then provide data to US governmental agencies. This also includes very strict limitations on sub processors. It is recommendable to additionally restrict further usage of even anonymous data which may have been aggregated to avoid any potential de-anonymization by third parties.

4.2. Organizational measures

Organizational measures can only be seen as additional but not effective measure to prevent US access and disclosure requests. Even though these measures will not prevent any company from receiving US access requests, it lowers data exposure, raises data handling

[283] Rec 109 GDPR; *EDPB*, Recommendations 01/2020[2] Rec 103, 104.
[284] *EDPB*, Recommendations 01/2020[2] Rec 105-127.

transparency including data subject's awareness and can therefore lower the risk of civil litigations and compliance issues.[285]

4.2.1. Policy measures

The EDPB recommends ensuring additional safeguards based on state-of-the-art standards and certifications to implement internal policies on responsibilities and procedures as well as training when it comes to international data transfers. Minimum requirements to consider are questions around who is involved in the decision making, who can approve, who needs to be contacted and informed.[286]

For providers who are falling under US disclosure obligations or engaging with affected data importers, it is advisable to create an information management plan, an internal policy and external notice, which clearly lay out for employees and data subjects under which circumstances information will be retrieved and how. Additionally, companies can provide transparency reports which are anonymous statistics about litigation and law enforcement access requests, to the public to raise transparency. Big cloud service providers such as Google, AWS and Microsoft already make such reports online available to the public Furthermore, role-based access controls for everyone handling personal data should be in place and could go as far as implementing a zero-trust architecture.[287]

4.2.2. Data minimization and best practices

Prior to any transfer the data exporter must ensure that only personal data necessary will be transferred. This can be achieved by putting measures in place to follow a strict need to know principle which is monitored and appropriately enforced, linked to a role-based access model.[288]

In my opinion, one major task to achieve data minimization and lower the risk of unwanted data exposure is to adapt each processing activity and rethink the ROPA set-up by using a

[285] *EDPB*, Recommendations 01/2020[2] Rec 128.
[286] *EDPB*, Recommendations 01/2020[2] Rec 128-132, 141.
[287] *EDPB*, Recommendations 01/2020[2] Rec 133-136; *Swire/Kennedy-Mayo*, U.S. Private-Sector Privacy[3], Ch 13 introduction; examples of CLOUD Act notices and disclosure information: for *AWS* <amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF#:~:text=Amazon%20knows%20customers%20care%20deeply,legally%20valid%20and%20binding%20order>, for *Microsoft*: <microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report#:~:text=Microsoft%20requires%20official%2C%20signed%2C%20legally,(or%20its%20local%20equivalent)>, for *Google*: <policies.google.com/terms/information-requests?sjid=18036790258855842134-NA> (all last retrieved Apr. 24, 2023).
[288] *EDPB*, Recommendations 01/2020[2] Rec 137-138.

more granular approach. This can help to see whether any processing activities or subcategories thereof are standing the necessity test. For example: when HR data needs to be shared within the same group of undertakings and requires a transfer of data when processed in an international group company it should be questioned whether it is necessary and adequate to fulfil companies' interests in sharing the entire payroll information with the US affiliate. If sensitive data, such as health, insurance or bank information are extracted from the data sharing the risk for data subjects in this processing activity is much lower than if all employee related information is transferred. Names, titles, business contact information and even salary information or length of employment are justifiable sets of data to share within the same group company.

For the avoidance of doubt, the aforementioned approach does not justify a data transfer only because less sensitive data is transferred. It should allow the data exporter to assess whether under a different set of transferred data the data importer may fall or not fall under US surveillance measures. As clarified by the Austrian DPA in *Google Analytics II*, Chapter V GDPR does not know a risk-based approach, meaning the more sensitive the data the more measures must be taken. Regardless of the type of data, a data exporter must always ensure an adequate level of data protection. While it does not make much difference under FISA based on the wide application, it does make a difference when it comes to ECPA including CLOUD Act applicability due to its narrower scope.[289]

4.2.3. Insurance

Another approach for lowering financial risk is executing a cyber and privacy (liability) insurance. Even though expensive, due to an increase in privacy claims and security breaches, these insurances gain high demand. Regardless of the costs, any lawsuit may cost a company much more. Caution about the actual scope of coverage is important since in many cases only accidental access to data and related claims are covered. Additional benefit is the associated due diligence of privacy practices an insurance company does prior granting a company coverage.[290]

[289] See *supra* 3.3.2 and 3.3.3; DSB-D155.026 (*Google Analytics II*) D.4. b); also confirmed by: BVwG W245 2252208-1/36E (*Google Analytics*) II.3.6.2.2.3.
[290] *Stransky/Rex*, Unlawful data processing claims: An insurance perspective.

4.2.4. Jurisdiction & change of control

First, the question of jurisdiction should be answered by each party processing personal data. As stated in the previous chapter, except from data in transit under EO 12333, US governmental access can only be achieved when the US has jurisdiction over the person in control of the data. Working with companies located or affiliated with the US will most likely fall under such personal jurisdiction, however, there may be circumstances where personal jurisdiction and hence an access request justification does not apply. As second step, control of sought data could be cut off. This can be achieved by different measures, e.g., legal control can be shifted with data trust models, day-to day control can be manipulated through technical measures such as pseudonymization.[291]

4.3. Technical measures

4.3.1. Anonymization of data

GDPR only applies to personal data, including pseudonymized data. In contrast, anonymized data are not covered by the regulation, which means that data do not relate and cannot be made relatable to an identified or identifiable person. Technical and organizational measures must be evaluated on a case-by-case basis and need to stand an objective test that even a third party cannot (re-)connect such data to a natural person, including through malicious acts.[292]

Anonymizing data is still challenging due to the high standards set by Art 29 WP, which laid out challenges of a correct anonymization of personal data to an outcome which doesn't allow data subjects "*to be identified via "all" "likely" and "reasonable" means*". Additionally, what anonymization truly means is interpreted differently by jurisdiction and is evolving with the state-of-the-art technology which makes it difficult for data exporters to rely on it. Critique is also raised by the ambiguous use of the term which leads to further uncertainty.[293]

Based on the CJEU decision *Breyer*[294] which ruled that whether data is personal data depends on the legal means which enable a recipient to identify the data subject, the

[291] See *infra* 4.3.
[292] Rec 26, 28, 29, Art 4 (1) and (5) GDPR; *Koerner*, A trans-Atlantic comparison of a real struggle.
[293] *Art 29 WP*, WP216, p 5, 23, 27; *Burt/Stalla-Bourdillon*, The definition of 'anonymization' is changing in the EU.
[294] C-582/14 *(Breyer)*.

European General Court (EGC) recently held in 2023 that whether data is considered as anonymized or personal (pseudonymized) depends on the view of the recipient. That means data can be anonymous as well as personal depending on the recipients (non-) ability to be likely used to re-identify data. Whether this position will be confirmed by the CJEU in its pending case remains open. It would not follow Art 29 WP's interpretation of objective test. But it would align with Austrian's DPA assessment in *Google Analytics I* and *II* that considerations regarding the probability whether anyone can de-anonymize data cannot go that far that any unknown third party may have potential theoretical special knowledge how to do so, but rather, whether identifiability can be established with a justifiable and reasonable effort. In this context, this encompasses not only data importers but also US agencies. Even though GDPR has a broad applicability, this conclusion is reasonable as data exporters cannot be expected to be able to consider every even very little chance of potential de-anonymization opportunity by unknown third parties. This would otherwise subsequently mean that any type of data must be treated as personal data.[295]

If EGC's decision is upheld by the CJEU, it would change the perspective and options on international data transfers and enable data exporters to use technical and organizational measures to make sure only for the US data importer anonymous data will be transferred. Consequently, GDPR including Chapter V requirements, would then not be applicable to the data transfer at all. In any case, if a US data importer may have potential access to personal data even though such data only reside within the Union and the data exporter, e.g., via remote access, the foresaid would not uphold.[296]

4.3.2. Pseudonymization

Pseudonymization is an important security measure which reduces the likability of data to the data subject. Indirect identification to a data subject may still be possible with additional attributes to link information back to a specific data subject and therefore makes GDPR applicable to its processing. Examples of pseudonymization techniques are masking, encryption with secret key, hash and salted-hash function, key-hashed function with stored key, deterministic encryption or keyed-hash function with deletion of the key and

[295] T-557/20 *(SRB)*, Rec 96-105; DSB-D155.027 (*Google Analytics I*) D.2 d); confirmed by BVwG W245 2252208-1/36E (*Google Analytics*) II.3.6.2.1.; DSB-D155.026 (*Google Analytics II*) D.2 d); *Art 29 WP*, WP216, p 5, 23, 27; *Koerner*, A trans-Atlantic comparison of a real struggle.
[296] *EDPB*, FAQ in Case C-311/18 (Schrems II), 11; also: *EDPB*, Recommendations 01/2020[2] Rec 13; *EDPB*, Guidelines 05/2021[2] Rec 16.

tokenization, etc. Since all techniques have their pitfalls and new methods are constantly in development, a continuous risk-based approach should be followed to predict, assess and mitigate upcoming risks in light of new technological developments.[297]

Using pseudonymization in a data transfer scenario, it is important to emphasize that the key or recovery method is not made available to the US data importer by any means. The *EDPB* states that if a hosting provider in a third country stores personal data, the data must be encrypted with state-of the art methods before transmission, and the key must be retained solely under the control of the data exporter and out of reach by US agencies. In case the US data importer has access to clear data, or the encryption key and US agencies have the authority to access data in an unnecessary and unproportionate manner, the encryption is not considered as an adequate supplementary measure.[298]

The term "made available" in this context must not only be assessed by GDPR but also by US law. For the SCA, custody, possession or control over sought data is the key element. *Ramos*, *Maciejewski and Jongen*, state that "possession, custody or control" under the CLOUD Act in relation to electronic data is understood encryption neutral. But if a provider stores encrypted data but does not have possession, custody or control of the decryption key, the provider is unable to determine whether sought data are actually in his possession, custody or control and therefore the governmental entity may be unable to demonstrate probable cause that the sought data is in provider's possession.[299]

This outcome is particularly difficult to overcome for international (group) entities, where the sharing of personal data is necessary for its business operations. If the data exporter is unable to demonstrate that US agencies access does not go beyond necessity and proportionality and therefore infringes data subjects' fundamental rights a transfer even with encryption would not constitute a supplementary measure.[300]

Sharing of HR data such as employees' names, titles, business email and phone as well as communication and salary information and length of employment are unavoidable not to share within the same organization. The same applies to customer information. However,

[297] Rec 28, 29, Art 4 (5), GDPR; *Art 29 WP*, WP216, p 20 et seq; *ENISA*, Pseudonymisation techniques and best practices, p 43.
[298] *EDPB*, Recommendations 01/2020[2] Rec 84, 85, 94, 95; *EDPB*, Guidelines 05/2021[2] Rec 15-21.
[299] *Ramos/Maciejewski/Jongen*, Application of the CLOUD Act to EU Entities, p 3.
[300] *EDPB*, Recommendations 01/2020[2] Rec 96, 97.

some other and more sensitive data sets, such as bank account information, insurance, background check records as well as health related information may not need to be necessary to share. A more in-depth analysis in terms of data minimization combined with other technical measures reduces data exposure and risk while still being able to conduct company's international business administration.[301]

Another option is a technology called homomorphic encryption. It allows to work on encrypted data without sharing the secret key and would prevent any disclosure of and access to personal data by a third-party provider maintaining a company's cloud storage or computing its data.[302]

For EO 12333 and provisions where US law enforcement directly seeks access to data while in transit, the data exporter must ensure state-of-the art encryption methods which provide effective active and passive attacks.[303]

4.3.3. Data trust cloud and data escrow

Even though the US national security and law enforcement laws have an extraterritorial reach, different types of cloud models have a different legal and factual effect whether the US agencies may gain access to personal data.

One option is a data trust or data escrow model which removes direct access of a US cloud service provider to stored data in the cloud. In this case, network management, which means the provision of the platform including hard- and software components itself is separated from the ability to access data. If set up correctly, this combination of technical and organizational measures between a network management company in the US and a trustee in the EU can cut any possibility for the US law enforcement to directly request sought data from a US provider. Important is that first, the EU trustee has no personal jurisdiction in the US. And secondly, the US cloud provider who manages the platform has no possession, custody, or control over sought data. This can be achieved by technical measures such as encryption of data. The key to the data must be out of US cloud provider's reach with no legal or practical possibility of getting access. Contractually, the two companies must not

[301] In contrast *Google Analytics I* and *II* regarding non-risk based approach; see *supra* 4.
[302] *Homomorphic Encryption Standardization*, Introduction.
[303] *EDPB*, Recommendations 01/2020[2] Rec 90.

be affiliated in a way that the US company has legal control over the data in EU trustees' possession.[304]

4.4. Additional procedural measures and continuous monitoring

If effective supplementary measures are put in place to secure the appropriate level of data protection, it further must be assessed whether an authorization from a competent supervisory authority for such additional implementation is needed. Even though *Schrems II* was assessing only the validity of SCCs and not in general the appropriate safeguards under Art 46 GDPR, the decision nevertheless applies to all other transfer tools under Art 46 GDPR due to their contractual nature. Any additional safeguards to SCCs are welcomed and do not need additional approval as long as additional measures do not contradict with the SCC provisions. Any modification or contradiction, however, requires the approval of the supervisory authorities.[305]

Ongoing monitoring of made assessment is crucial for a continuous compliance and accountability obligations under GDPR. Data exporters must regularly assess data importers compliance, the effectiveness of supplemental safeguards as well as the ongoing (legal) developments in the US.[306]

Data privacy impact assessments and data lifecycle management are two key elements to achieve ongoing compliance.[307]

[304] *Schwartz*, Legal Access to the Global Cloud, p 1697, 1719; *Microsoft*, Escrow as a Service; *Rath/Spies*, CLOUD Act: Selbst für die Wolken gibt es Grenzen, sec E.
[305] *EDPB*, Recommendations 01/2020[2] Rec 59-62, 66; Rec 109, Art 46 (1) and first sentence (2) GDPR; SCC Int transfer 2021 EC (EU) 2021/914 Annex Clause 2 (a); C-311/18 (*Schrems II*) Rec 132.
[306] *EDPB*, Recommendations 01/2020[2] Rec 67-68.
[307] Art 35 GDPR.

5. Summary and conclusion

This thesis assessed on the basis of EDPB's recommendations which transfer tools and supplementary measures are appropriate and usable for data exporters transferring data to the US and the associated risk of US governmental access to personal data including its legal impacts for data exporters by answering the following research questions:

1. *Is it possible to be legally compliant with GDPR as a data exporter who is directly or indirectly through its data importer subject to US governmental access requests to electronically held personal data?*

    a. *If so, in what legal and/or technical form?*

For data exporters doing business in the US, current possible and reasonable transfer mechanisms besides the DPF are SCCs and BCRs as appropriate safeguards, a transfer based on an international treaty such as MLAT, and the derogations of explicit consent and legal claims. Other mechanism tools are either too narrow in its applicability (e.g., contract performance, vital interest, or public registers) or too time consuming to obtain (e.g., CoC, certifications or prior authorization).

The conducted TIA based on the current relevant US legal framework regarding national security and law enforcement concluded with the overall assessment that even though the US national security laws improved due to the implementation of EO 14086, access to electronically held personal data still cannot be ruled out by data exporters. Based on a data exporter's accountability obligation in being responsible for and show its compliance related to the data processing activities, any personal data transfer to the US falls in theory under US national security regulations and in most instances within the scope of the ECPA due to their broad applicability and not well-defined scope. Furthermore, the unequal treatment between US and non-US persons is not justified under laws such as FISA 702 or the CLOUD Act executive agreements and create an unproportional limitation for the freedoms of natural persons. Many classified but important information is not provided to data exporters which makes a comprehensive assessment impossible.

As this thesis demonstrated, at first it seems that governmental and private data collection make a difference, since a criminal punishment can only be enforced by the government. However, looking at the issue of governmental access to electronic data closer, a separation

between governmental and private data collection does not really matter in terms of the result since the law enforcement has options to obtain the data due to voluntarily disclosure. Data protection and the privacy of individuals can only effectively be protected if there is an overarching omnibus law in place which can tackle the root cause of abuse, namely data (mass) collection. Only if the private sector as well as governmental entities are regulated by clear, transparent and limited data collection and further usage regulations, individuals can be assured of a robust protection.

Due to this outcome, data exporters are required to adopt supplementary measures to justify a transfer. Even though the risk in practice can be low for data exporters, it is part of the data exporter's accountability obligation not to ignore any known (potential) risk and provide evidence for an adequate level of protection for each data transfer. Known exposures must be assessed and adequately addressed with supplementary measures to guarantee that EU standards are not undermined, otherwise the data exporter faces legal consequences and full liability for its data handling.

Consequently, under current US framework and its concurrent non-compliance with EU standards, it is only possible to be legally compliant with EU standards if data exporters can ensure that neither US data importers have possession, custody or control nor US agencies have potential access to personal data. This can only be achieved by implementing effective technical measures to ensure no factual access is possible. Even though contractual and organizational measures are important supplements, they, however, cannot effectively guarantee an infringement given that US law prevails.

b. *If not, what needs to be implemented by affected companies in order to obtain exemption from or mitigation of liability?*

Contractual, organizational and especially focusing on technical measures must be implemented, which are capable of closing the deficiencies of US surveillance laws and ensuring an effective level of data protection. Data exporters should consider the famous quote *"[I]n this world, with great power there must also come—great responsibility"*[308]. But the opposite is also true. GDPR gives a lot of accountability responsibility to data controllers. Data controllers, however, have therefore the power to gain control and determine its data handling and ultimately over the cloud. That includes, where feasible, to

[308] *Lee/Ditko*, Amazing Fantasy No. 15: Spider- Man, p 13.

only share anonymized or if needed pseudonymized data with data importers, extract any possession, custody or control of a data importer to personal data, including legal and day-to-day controls such as encryption, data escrow as well as change of control.

Even though it requires effort and resources to change internal procedures and data handling, it is, however, still easier to change internally than relying on compliance of a third party and controlling them. No data importer or processor can make a controller compliant. Therefore, data exporters should improve internal IT and IT security, processes, data handling and access request management. Data importers should be used smart by using role-access-based controls, encryption, masking and zero-trust architecture.

It is further advisable to have a general assessment policy in place, so each transfer assessment can be followed by the same principles to reduce time and effort. For international group companies sharing personal data on a regular basis, an internal centralized process to streamline all data access requests to the legal function sitting at the data exporters side should be set up. This achieves transparency to independently assess and decide whether access requests must be followed or fought and further controls the assessment whether at all and if so under which transfer mechanism, for example derogations, can sought data be transferred.

For outsourced services, the extraction of data importers' legal or day-to-day possession, custody or control over personal data should be achieved. If data importers still need access to personal data, data minimization principles such as pseudonymization, encryption, zero-trust architecture including role-based access models should be implemented to have a clear understanding which data may be exposed and reduce access to it.

2. *What can be done on the governmental side to provide legal certainty to affected businesses?*

Internationally, the MLAT systems and other treaties for harmonization and transparency should be enforced. The US is to be encouraged to strengthen its data protection regulations by implementing omnibus privacy laws such as the ADDP. On the EU side, more guidance and options on how to securely transfer data, e.g., with the implementation of certification mechanisms or code of conduct, should be given to data exporters.

Finding a workable and lawful solution should be the first and primer agenda point on each governmental privacy agenda. Technology is evolving so quickly that in my opinion it is impossible to keep the law and proper requirements constantly up to date. Therefore, legislators should focus on a workable rather perfect solution which includes international commitments and strengthening of internal guidelines to assist data exporters with their compliance obligations.

6. Appendix

6.1. Abstract

Abstract German

Der einfache Zugriff auf und die Speicherung von Daten von nahezu jedem Ort aus ist nicht nur bequem, sondern bringt auch eine Menge Herausforderungen für die Strafverfolgung und die nationale Sicherheit mit sich. Auch wenn die wichtigsten Anbieter von Cloud-Diensten in den USA ansässig sind, werden die Daten in den allermeisten Fällen durch verschiedene Länder transportiert, was die herkömmlichen nationalen Rechtsverfahren zur Anforderung oder Beschaffung von Daten zu Ermittlungszwecken aufgrund des internationalen Umfangs und des manchmal unklaren Standorts an ihre Grenzen bringt. Trotz der fortschreitenden Globalisierung sind die Staaten aufgrund des völkerrechtlichen Souveränitätsprinzips in der Gestaltung ihres Rechtsraums unabhängig.

Datenschutzgesetze schützen auf der einen Seite natürliche Personen und deren personenbezogene Daten und haben einen sehr breiten Anwendungsbereich mit oft extraterritorialer Anwendbarkeit. Auf der anderen Seite sind Staaten bestrebt, ihre Positionen zu stärken, indem sie einen leichteren Zugang zu gesuchten Daten für strafrechtliche und nationale Sicherheitszwecke erhalten, was wiederum zu einer weitreichenden extraterritorialen Reichweite führt. In jedem Fall führt jede extraterritoriale Anwendung einer Regelung letztlich zu einer Überschneidung der Anwendbarkeit mit den Regelungen eines ausländischen Staates und dessen Zuständigkeiten. Diese seit langem bestehende transatlantische Diskrepanz im Umgang mit und dem Zugang zu personenbezogenen Daten hat starke Auswirkungen auf die internationale Wirtschaft. Abgesehen davon, dass sowohl die EU als auch die USA bestrebt sind, eine dauerhafte und einvernehmliche Lösung auf politischer Ebene zu finden, und selbst mit dem neu in Kraft getretenen EU-US Datenschutzabkommen, bleibt die politische Unsicherheit für Unternehmen weiterhin bestehen und verlangt daher nach eigenständigen Lösungen.

Diese Masterarbeit beschreibt die Anforderungen an den Datentransfer von der EU in die USA für Unternehmen auf der Grundlage des aktuellen transatlantischen Rechtsrahmens und soll Datenexporteuren Optionen für einen legalen und sicheren Datentransfer bieten. Sie konzentriert sich auf den Zugriff der US-Regierung auf elektronisch gespeicherte personenbezogene Daten im Hinblick auf die einschlägigen US-Bundesvorschriften und soll Lösungsansätze für Unternehmen bieten, die von beiden Regelungen betroffen sind. Die Bewertung stützt sich auf die Prüfkriterien, die der Europäische Datenschutzausschuss in seinen Empfehlungen für ergänzende Übermittlungsinstrumente und die europäischen Grundgarantien für Überwachungsmaßnahmen aufgestellt hat.

Abstract English

The easy storage and access to data from almost anywhere is not only convenient but raises a lot of challenges for law enforcement and national security. Even though the many major cloud service providers reside in the US, in a vast majority of cases data travels through various countries which brings traditional national legal processes how to request or obtain data for investigation purposes to its limits due to the international scope and sometimes unclear location. Despite progressive globalization, under the international law's principle of sovereignty, countries are independent in shaping their legal sphere.

On the one side, data privacy laws protect natural persons and their personal data with a broad scope and often extraterritorial applicability. On the other side, countries are striving to strengthen their position in gaining easier access to sought data for criminal and national security purposes which again results in a far extraterritorial reach. In any case, any extraterritorial application of a regulation ultimately leads to an overlap of applicability with a foreign state's regulations and their competences. This long-lasting transatlantic discrepancy in the handling of and access to personal data has a strong impact on international business. Besides the fact that the EU as well as US are eager to find a long-lasting and amicable solution at a political level, and even with the newly enacted EU-US Data Privacy Framework now in place, uncertainty for companies remains which demands for self-independent solutions.

This master thesis describes the requirements of data transfer from the EU to the US for companies based on the current relevant transatlantic legal framework and intents to provide options for data exporters on how to legally and securely transfer data. It focuses on the US governmental access to electronically held personal data in view of relevant federal US regulations and shall provide solution approaches for businesses affected by both regimes. The assessment is based on the testing criteria provided by the European Data Protection Board in its recommendations on supplement transfer tools and the European Essential Guarantees for surveillance measures.

6.2. References

6.2.1. Bibliography and online references

Alfred NG, The privacy loophole in your doorbell, Politico (Mar. 7, 2023) <politico.com/news/2023/03/07/privacy-loophole-ring-doorbell-00084979?mkt_tok=MTM4LUVaTS0wNDIAAAGKZoWBjSup9KQD41QPxcqRPJgt3fQTuRKvUNlhRyydEsEhTzNO83lpitaIbYcqMYlitgzkUo-pZM9i1U9tJEbhTiltwYWJNol5nbktMbmABKi2> (last retrieved Aug. 16, 2023)

Anderl/Tlapak, Erleichterung für US-Datentransfer, Die Presse 2016/29/01 (July 18, 2016)

Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP 259 rev.01 (Apr. 10, 2018)

Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP238 (Apr. 13, 2016)

Article 29 Working Party, Opinion 01/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, WP15 (Jan. 26, 1999)

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216 (Apr. 10, 2014)

Article 29 Working Party, Working Document on surveillance of electronic communications for intelligence and national security purposes, WP228 (Dec. 5, 2014)

Bernsteiner, Schrems II & Privacy Shield: Auswirkungen auf internationale Datentransfers, in *Jahnel* (Hg), Datenschutzrecht. Jahrbuch 21 (2022)

Bracy, Meta fined GDPR-record 1.2 billion euros in data transfer case, IAPP (May 22, 2023) <iapp.org/news/a/meta-fined-gdpr-record-1-2-billion-euros-in-data-transfer-case/?mkt_tok=MTM4LUVaTS0wNDIAAAGL47zAZbQxSAtG_ai6jv34joBVlCcQBqfPvqpw73zqmdsJTra2ldax_p6xzfZD0tMgcx-L29-JbEeXH_pcaD1mEaR_b1Lepxrv-HjhU00Fbkxk> (last retrieved Aug. 16, 2023)

Bryant, EU-US Data Privacy Framework adopted, what now?, International Association of Privacy Professionals (July 24, 2023) <iapp.org/news/a/eu-us-data-privacy-framework-adopted-what-now/> (last retrieved Aug. 25, 2023)

Burt/Stalla-Bourdillon, The definition of 'anonymization' is changing in the EU: Here's what that means, International Association of Privacy Professionals (June 27, 2023) <iapp.org/news/a/the-definition-of-anonymization-is-changing-in-the-eu-heres-what-that-means/?mkt_tok=MTM4LUVaTS0wNDIAAAGMzYjeEWUKnZ5UWPAcZZbiBNf_ZbVt3F_XPimKIxJAm6JDDT5eVqNzW-3Lm9v7BTDI6XUmRAqMezUJZ5AKs1ypqbIibiguPv-db2z0NL6EMHUO> (last retrieved Aug. 25, 2023)

Cameron, The FBI Just Admitted It Bought US Location Data, Wired (Mar. 8, 2023) <wired.com/story/fbi-purchase-location-data-wray-senate/?mkt_tok=MTM4LUVaTS0wNDIAAAGKZoWBi_SchgdezYYh2zMnyti6G_p4uYDmTXDT_w9C_v3B0BOFGp12muRdMyvpaTX65QLlTZLbygRLqJKJIHAfsgv2IAGPSZKNeDnE2zXo7T3O> (last retrieved Aug. 16, 2023)

Carney, A coalition of privacy-minded outside groups and lawmakers are outlining sweeping changes they want to see ahead of an end-of-year surveillance deadline, Politico (Mar. 15, 2023) <politico.com/minutes/congress/03-15-2023/fisa-surveillance-privacy-hawks/> (last retrieved Aug. 16, 2023)

Centre for Information Policy Leadership, Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, Discussion Paper (Apr. 12, 2017) <informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf> (last retrieved Aug. 16, 2023)

Chin, Digital Dragnets: Examining the Government's Access to Your Personal Data, Written Testimony, House Judiciary Committee (July 19, 2022)

Committee on Civil Liberties, Justice and Home Affairs, Draft motion for a European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework 2023/2501(RSP) (Feb. 14, 2023) <europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf> (last retrieved Aug. 16, 2023)

Congress.gov, Constitution Annotated, Analysis and Interpretation of the U.S. Constitution, Amdt14.S1.7.1.1 Overview of Personal Jurisdiction and Due Process <constitution.congress.gov/browse/essay/amdt14-S1-7-1-1/ALDE_00000907/> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, electronic surveillance (Nov. 2022) <law.cornell.edu/wex/electronic_surveillance> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, electronic surveillance <law.cornell.edu/wex/electronic_surveillance> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, Plenary Power <law.cornell.edu/wex/plenary_power> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, search warrant <law.cornell.edu/wex/search_warrant> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, subpoena <law.cornell.edu/wex/subpoena> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, surveillance (Oct. 2021) <law.cornell.edu/wex/surveillance#:~:text=Individuals%20and%20law%20enforcement%20officials,can%20protect%20individuals%20against%20surveillance> (last retrieved Aug. 16, 2023)

Cornell Law School, Legal Information Institute, warrant <law.cornell.edu/wex/warrant> (last retrieved Aug. 16, 2023)

Council of Europe, Chart of signatures and ratifications of Treaty 185 <coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> (retrieved Aug. 16, 2023)

Daskal, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, Journal of National Security Law & Policy, Vol 8:473 (Sep. 6, 2016)

Dearen/Burke, Senators push to reform police's cellphone tracking tools, AP News (Sep. 27, 2022) <apnews.com/article/technology-new-york-criminal-investigations-federal-trade-commission-63451d232fb202009d71a2b59173b4c7> (last retrieved Aug. 16, 2023)

Der Bayrische Landesbeauftragte für den Datenschutz, Internationale Datentransfers Orientierungshilfe (May 1, 2023)

Desai, US State Privacy Legislation Tracker, International Association of Privacy Professionals (Aug. 4, 2023) <iapp.org/resources/article/us-state-privacy-legislation-tracker/> (last retrieved Aug. 25, 2023)

Dixon, A Brief Introduction to Fair Information Practices (originally June 5, 2006, updated Dec. 19, 2007) World Privacy Forum <worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/> (last retrieved Aug. 16, 2023)

Doyle, Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments, Congressional Research Service, The Library of Congress (Apr. 15, 2005)

Electronic Privacy Information Center, Records, Computers and the Rights of Citizens: Report of the HEW Advisory Committee on Automated Personal Data Systems (July 1973) <epic.org/documents/hew1973report/> (last retrieved Sep. 2, 2023)

Electronic Privacy Information Center, The Code of Fair Information Practices <epic.org/fair-information-practices/#:~:text=The%20Code%20of%20Fair%20Information%20Practices%20was%20the%20central%20contribution,was%20released%20in%20July%201973.> (last retrieved Sept. 2, 2023)

European Commission, Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US, Press release (Dec. 13, 2022) <ec.europa.eu/commission/presscorner/detail/en/ip_22_7631> (last retrieved Aug. 16, 2023)

European Commission, EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations (Mar. 2, 2023) <commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en> (last retrieved Aug. 16, 2023)

European Commission, Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting (June 2, 2026) <ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_2040> (last retrieved Aug. 16, 2023)

European Commission, The New Standard Contractual Clauses – Questions and Answers (May 25, 2022) <commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> (last retrieved Aug. 16, 2023)

European Commission, When does the Charter apply? <commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/when-does-charter-apply_en> (last retrieved Aug. 16, 2023)

European Data Protection Board, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence (July 10, 2019)

European Data Protection Board, Approved Binding Corporate Rules <edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=0> (last retrieved Aug. 16, 2023)

European Data Protection Board, Binding Decision 01/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR) (Apr. 13, 2023)

European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (July 23, 2020)

European Data Protection Board, Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679 (May 25, 2018)

European Data Protection Board, Guidelines 02/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Version 2 (Dec. 15, 2020)

European Data Protection Board, Guidelines 04/2021 on Codes of Conduct as tools for transfers, Version 2.0 (Feb. 22, 2022)

European Data Protection Board, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0 (Feb. 14, 2023)

European Data Protection Board, Guidelines 07/2022 on certification as a tool for transfers, Version 2.0 (Feb. 14, 2023)

European Data Protection Board, Opinion 05/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (Feb. 28, 2023)

European Data Protection Board, Pre-GDPR BCRs overview list <edpb.europa.eu/system/files/2023-03/EDPB_Information_Pre-GDPR_BCRs_Overview_en.pdf> (last retrieved Aug. 16, 2023)

European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0 (June 18, 2021)

European Data Protection Board, Recommendations 01/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) (Nov. 14, 2022)

European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (Nov. 10, 2020)

European Data Protection Board, Report of the work undertaken by the supervisory authorities within the 101 Task Force (Mar. 28. 2023)

European Union Agency for Cybersecurity, Pseudonymisation techniques and best practices (Nov. 2019)

Fazlioglu, US Federal Privacy Legislation Tracker, International Association of Privacy Professionals (May 2023) <iapp.org/resources/article/us-federal-privacy-legislation-tracker/> (last retrieved Aug. 25, 2023)

Feiler, Datenschutz: Ein Schild, der keine Deckung gibt, Die Presse 2016/11/04 (Mar. 14, 2016)

Feiler/Forgó, EU-DSGVO EU-Datenschutz-Grundverordnung (2017) Kurzkommentar, Verlag Oesterreich

FindLaw, What Is a Subpoena? <findlaw.com/litigation/going-to-court/what-is-a-subpoena.html> (last retrieved Aug. 16, 2023)

Fritz/Kirchmair, Drittstaatentransfers bei Cookies - neue Entwicklungen und Lösungswege, MR 4/2022, 190 (Sept. 23, 2022)

Gabauer/Höller, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down?, Dako 4/2020, 80 (Sep. 4, 2020)

Georgieva, EU-US-Privacy Shield - eine Gesamtbetrachtung, Jahrbuch Öffentliches Recht 2017, 193 (Jan. 9, 2017)

Guardian, Edward Snowden says surveillance technology is more intrusive than ever, The Irish Times (June 8, 2023) <irishtimes.com/world/us/2023/06/08/edward-snowden-says-surveillance-technology-is-more-intrusive-than-ever/?mkt_tok=MTM4LUVaTS0wNDIAAAGMOvOEilDDhx9BWSp5QTH84SlcPbmF9mKS2fBn3TJmGaMG9duMuhXq3SZzkPCGx7nKoYHR7DALkw_3ks76-NWFycobzdm9u-5X5Fj20fDBs1P6> (last retrieved Aug. 16, 2023)

Hamilton/Quinlan, The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe, Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, (2022) <transatlanticrelations.org/wp-content/uploads/2022/03/TE2022_report_HR.pdf> (last retrieved Aug. 16, 2023)

Hansch, Der Entwurf eines Angemessenheitsbeschlusses der Europäischen Kommission für den US-EU-Datentransfer (Jan 9, 2023) DSB 01/2023, 21

Hemmings/Srinivasan/Sreenidhi/Swire, Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act (Oct. 7, 2019), Journal of National Security Law and Policy 10, 631 (2020), Georgia Tech Scheller College of Business Research Paper No. 3469808 <ssrn.com/abstract=3469808> (last retrieved Aug. 16, 2023)

Hengesbaugh, What Privacy Shield organizations should do in the wake of 'Schrems II', IAPP (Jul. 17, 2020) <iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/> (last retrieved Aug. 16, 2023)

Homomorphic Encryption Standardization, Introduction <homomorphicencryption.org/introduction/> (last retrieved Aug. 16, 2023)

Honorable Bob Goodlatte, Digital Dragnets: Examining the Government's Access to Your Personal Data, Testimony before the Judiciary House Committee (July 19, 2022) <youtube.com/watch?v=f27nOcsenRY> (last retrieved Aug. 16, 2023)

IMY Swedish Authority for Privacy Protection, Four companies must stop using Google Analytics (July 3, 2023) <imy.se/en/news/four-companies-must-stop-using-google-analytics/?mkt_tok=MTM4LUVaTS0wNDIAAAGMzYjeEuO43WtnabLkE1F4-qw90tQrddKEYVcIx0cRILk9x6XCSyX3CfgtEz2EHjtasXIAHDUB_1A77Ya2tkHROdy6STIie61U9VkyrlQuGLCj> (last retrieved Aug. 16, 2023)

International Association of Chiefs of Police, Types of Law Enforcement Agencies <discoverpolicing.org/explore-the-field/types-of-law-enforcement-agencies/> (last retrieved Aug. 16, 2023)

ISO, Online Browsing Platform (OBP), ISO/IEC 19831:2015(en), Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol — An Interface for Managing Cloud Infrastructure <iso.org/obp/ui#iso:std:iso-iec:19831:ed-1:v1:en:term:3.3> (last retrieved Aug. 16, 2023)

Jayapal, Jayapal Davidson Bipartisan Statement on Privacy Protections for Americans (Mar. 15, 2023) <jayapal.house.gov/2023/03/15/jayapal-davidson-bipartisan-statement-on-privacy-protections-for-americans/> (last retrieved Aug. 16, 2023)

Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, George Washington Law Review, Vol 72:1701 (Aug. 2004)

Kerry, Why protecting privacy is a losing game today—and how to change the game (July 12, 2018) <brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> (retrieved Aug. 16, 2023)

Kerry, Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?, Lawfare (aug. 10, 2023) <lawfaremedia.org/article/will-the-new-eu-u.s.-data-privacy-framework-pass-cjeu-scrutiny> (last retrieved Aug. 24, 2023)

Klumpp, International Impact of the Clarifying Lawful Overseas Use od Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations, GA. J. INT'L & COMP. L, Vol. 48:613 (2020)

Knyrim, DatKomm, Manz (Jan. 2018 until 2022)

Koerner, A trans-Atlantic comparison of a real struggle: Anonymized, deidentified or aggregated?, IAPP (May 23, 2023) <iapp.org/news/a/a-transatlantic-comparison-of-a-real-struggle-anonymized-deidentified-or-aggregated/?mkt_tok=MTM4LUVaTS0wNDIAAAGMNcs9t76zBmRX6XqYvBRR7HmqbUoQSxIqJvWysChBXZ1Zi87ig83s_Sr1beRmDgkgyDYHgatQsFdZzlc5EKRcOl8v0MyFKW11YCCWd7WuwPyQ> (last retrieved Aug. 16, 2023)

Kristoferitsch/Stangl, Bruechiger Datenschild, Der Standard 2016/10/06 (Mar. 10, 2016)

LaCasse, In wake of global data transfer complexity, need for multilateral treaty grows, IAPP (Apr. 25, 2023) <iapp.org/news/a/schrems-3-transborder-data-flows-become-hot-button-topic-at-iapp-gps-2023/?mkt_tok=MTM4LUVaTS0wNDIAAAGLfGiiUDXDVrItGy5upLCvzm14_sICU4KtjOYUP-H3hL8hYqsCmlWNGPaWXknOvFnzDihZkje_JBJ-9MOBkkEx4XLAqaW69VQnqkNCmy42McrQ> (last retrieved Aug. 16, 2023)

Lee/Ditko, Amazing Fantasy No. 15: Spider- Man (Aug. 1, 1962)

Liu, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, Congressional Research Service (Mar. 17, 2023) <crsreports.congress.gov/product/pdf/R/R47477> (last retrieved Aug. 16, 2023)

Mell/Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145 (2011) <govinfo.gov/content/pkg/GOVPUB-C13-74cdc274b1109a7e1ead7185dfec2ada/pdf/GOVPUB-C13-74cdc274b1109a7e1ead7185dfec2ada.pdf> (last retrieved Aug. 16, 2023)

Microsoft, Escrow as a Service <azuremarketplace.microsoft.com/en-us/marketplace/apps/ncc.eaas?tab=overview> (last retrieved Aug. 16, 2023)

Microsoft, What is the Cloud? <azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud> (last retrieved Aug. 16, 2023)

National Archives, Office of the Federal Register (OFR) <archives.gov/federal-register/executive-orders/disposition> (last retrieved Aug. 16, 2023)

Noyb, Data Transfers <noyb.eu/en/project/eu-us-transfers> (last retrieved Aug. 16, 2023)

Noyb, New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". noyb will challenge the decision. <noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> (last retrieved Aug. 24, 2023)

Office of the Director of Intelligence, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities Calendar Year 2022 (April 2023)

Office of the Director of Intelligence, How the IC Works, Mission <intelligence.gov/mission> (last retrieved Aug. 16, 2023)

Office of the Director of Intelligence, How the IC Works, Our Organization <intelligence.gov/how-the-ic-works#our-organizations> (last retrieved Aug. 16, 2023)

Office of the Director of Intelligence, ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086 (July 3, 2023) <intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086?mkt_tok=MTM4LUVaTS0wNDIAAAGM0LMILn8N46I31KulWVaPxYwBPSRu-KJJq8gC7kZzn7WNfOjbH60nlq8sR4M-

5avNMJ2m_vSUeGqCMLahWS2svTzzq5POd0VctgWXtbZbB-Al> (last retrieved Aug. 16, 2023)

Office of the Director of National Intelligence, Civil Liberties and Privacy Information Paper: Description of Civil Liberties and Privacy Protections Incorporated in the 2008 Revision of Executive Order 12333 (2013)

Perkins Coie, Security Breach Notification Chart (revised Oct. 2022) <perkinscoie.com/images/content/2/6/v5/264631/Security-Breach-Notification-Law-Chart-October-2022.pdf> (last retrieved Aug. 16, 2023)

Piltz, Art. 49 DSGVO - Der Vakuum-Killer für Drittlandstransfers?, DSB 11/2021, 313 (Nov. 6 2021)

Privacy and Civil Liberties Oversight Board, Report on Executive Order 12333 (Apr. 2, 2021) <documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12333%20Public%20Capstone.pdf> (last retrieved Aug. 16, 2023)

Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014)

PrivacyRights.org, Data Breach Notification in the United States 2022 Report (Jan. 27, 2023) <privacyrights.org/resources/data-breach-notification-2022> (last retrieved Aug. 16, 2023)

Ramos/Maciejewski/Jongen, Memorandum to the Dutch Ministry of Justice and Security, Application of the CLOUD Act to EU Entities, GreenbergTraurig (July 26, 2022)

Rath/Spies, CLOUD Act: Selbst für die Wolken gibt es Grenzen, CCZ 2018, 229

Riley, NSA director urges Congress to renew controversial intelligence authority, Cyberscoop (Jan. 12, 2023) <cyberscoop.com/nsa-director-section-702-pclob/> (last retrieved Aug. 16, 2023)

Riley, Supreme Court declines to hear Wikimedia case against NSA surveillance program, Cyperscoop (Feb. 21, 2023) <cyberscoop.com/supreme-court-wikimedia-aclu-nsa/?mkt_tok=MTM4LUVaTS0wNDIAAAGKGUYPrI_aGbD2uHPlB0JSqJJv-dPiwn_svZn1ycdZ_1cn8Ng-J_iTv1o95NgYKXNmJN9qWISjdbrsSLnRYqP58ENgfy84xlDpNvDIHfp-6-ds> (last retrieved Aug. 16, 2023)

Riley, Wikimedia wants the Supreme Court to hear case over NSA surveillance. Here's what's at stake., Cyperscoop (Feb. 17, 2023) <cyberscoop.com/wikimedia-nsa-supreme-court-surveillance/> (last retrieved Aug. 16, 2023)

Schaar, EAID: E-Evidence und CLOUD Act - Grenzüberschreitender Direktzugriff auf Daten?, ZD-Aktuell 2019 04362

Schwartz, Legal Access to the Global Cloud, Columbia Law Review, 118 Colum. L. Rev. 1681 (Oct. 2018)

Shenkman/Franklin/Nojeim/Thakur, Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers, Center for Democracy & Technology (Dec. 2021)

Stransky/Rex, Unlawful data processing claims: An insurance perspective, International Association of Privacy Professionals (May 23, 2023) <iapp.org/news/a/unlawful-data-processing-claims-an-insurance-perspective/?mkt_tok=MTM4LUVaTS0wNDIAAAGMZI41keCB0IR3bXHx0wUDGpJNp0Cxbb-tbSkTy0bBOgQf6233rkH_XKvDfPPvJtdF-oN2Mw-vSh9nCgSseUz4qiMwpqdBcf6oM1F98A6fexWu> (last retrieved Aug. 25, 2023)

Strassemeyer, Vorhang auf für das Trans-Atlantic Data Privacy Framework - der nächste Akt ist eröffnet, DSB 7-8/2023, 186

Swire/Kennedy-Mayo, U.S. Private-Sector Privacy, 3rd Edition, International Association of Privacy Professionals (2020)

The Library of Congress, Presidential Directives and Where to Find Them (Mar. 30, 2022) <loc.gov/rr/news/directives.html> (last retrieved Aug. 16, 2023)

U.S Department of Commerce/U.S. Department of Justice, Office of the Director of Intelligence, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, White Paper (Sept. 2020)

U.S. Bureau of Justice Assistance, Electronic Communications Privacy Act of 1986 (ECPA), Background <bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#background> (last retrieved Aug. 16, 2023)

U.S. Bureau of Justice Assistance, Executive Orders <bja.ojp.gov/program/it/privacy-civil-liberties/authorities/executive-orders> (last retrieved Aug. 16, 2023)

U.S. Bureau of Justice Assistance, The Foreign Intelligence Surveillance Act of 1978 (FISA), Background <bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#background> (last retrieved Aug. 16, 2023)

U.S. Department of Commerce, Data Privacy Framework Program, FAQs - EU-U.S. Data Privacy Framework (EU-U.S. DPF) <dataprivacyframework.gov/s/article/FAQs-EU-U-S-Data-Privacy-Framework-EU-U-S-DPF-dpf> (last retrieved Aug. 24, 2023)

U.S. Department of Commerce, Data Privacy Framework Program, FAQs - General <dataprivacyframework.gov/s/article/FAQs-General-dpf> (last retrieved Aug. 24, 2023)

U.S. Department of Commerce, EU-U.S. & Swiss-U.S. Privacy Shield <privacyshield.gov/list> (last retrieved June 8, 2023)

U.S. Department of Commerce, Statement from U.S. Secretary of Commerce Gina Raimondo on the European Union-U.S. Data Privacy Framework, Press Release (July 3, 2023) <commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data?mkt_tok=MTM4LUVaTS0wNDIAAAGMu-HBPpfJ0TB8XlBBAvZhKL4uUALh8R_Zo12SGgr2qwmG0Fn9wgdaBHX3H_XI9R-qaoqyjz9ExsDowvP5n8nrgpPFjstoWqI3pRSJSIKkkrPS> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Cloud Act Resources <justice.gov/criminal-oia/cloud-act-resources> (retrieved Aug. 16, 2023)

U.S. Department of Justice, Federal Law Enforcement Officers, 2020 – Statistical Tables (Sep. 2022) <bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/fleo20st.pdf> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations (Mar. 2, 2023) <justice.gov/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086 <justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf> (last retrieved Aug. 25, 20230

U.S. Department of Justice, Mutual Legal Assistance Treaties of the United States (April 2022) <justice.gov/criminal-oia/file/1498806/download> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Overview of the Privacy Act of 1974 (Feb. 24, 2021) <justice.gov/archives/opcl/policy-objectives> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Overview of the Privacy Act: 2020 Edition, Judicial Redress Act (Oct. 4, 2022) <justice.gov/opcl/overview-privacy-act-1974-2020-edition/JRA#:~:text=The%20Judicial%20Redress%20Act%20extends%20certain%20rights%20of%20judicial%20redress,exceptions%2C%20as%20an%20individual%20may> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper (Apr. 2019) <justice.gov/criminal-oia/page/file/1153436/download> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, Regarding Cloud Act Executive Agreements <justice.gov/criminal-oia/regarding-cloud-act-executive-agreements#:~:text=By%20their%20terms%2C%20CLOUD%20Act,private%20parties%2C%20including%20criminal%20defendants.> (last retrieved Aug. 16, 2023)

U.S. Department of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement, Press Release Number 22-275 (Mar. 22, 2022) <justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement> (last retrieved Aug. 16, 2023)

U.S. Government Accountability Office, Protecting Personal Privacy Issue Summary <gao.gov/protecting-personal-privacy#:~:text=The%20federal%20government%20collects%20and,enhanced%20online%20interactions%20with%20citizens> (retrieved Aug. 16, 2023)

U.S. Government Publishing Office, Fourth Amendment Search and Seizure (1992) <govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf> (last retrieved Aug. 16, 2023)

U.S. House of Representatives Judiciary Committee, USA Freedom Act <judiciary.house.gov/usa-freedom-act> (last retrieved Aug. 16, 2023)

U.S. House of Representatives, Our American Government, Brochure 2003 revised edition, H. Con. Res. 139, 108th Congress (June 20, 2003) <govinfo.gov/content/pkg/CDOC-108hdoc94/pdf/CDOC-108hdoc94.pdf> (last retrieved Aug 16, 2023)

U.S. Treasury Financial Crimes Enforcement Network, USA Patriot Act <fincen.gov/resources/statutes-regulations/usa-patriot-act> (last retrieved Aug. 16, 2023)

Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, University of Texas School of Law (Nov. 12, 2021)

Whistic, Whats the Difference Between Privacy Shield and Safe Harbor?, Medium (Sep. 8, 2016) <blog.whistic.com/whats-the-difference-between-privacy-shield-and-safe-harbor-7c86cfa42813> (last retrieved Aug. 16, 2023)

Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Journal, Vol. 113:1151 (2004)

Woods, Against Data Exceptionalism, Stanford Law Review, Vol. 68:729 (Apr. 2016)

World Intellectual Property Organization, Madrid System – The International Trademark System <wipo.int/madrid/en/> (last retrieved Aug. 16, 2023)

6.2.2. Judicature

US Jurisdiction

US Supreme Court

Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018) <casetext.com/case/carpenter-v-united-states-67> (last retrieved Aug. 13, 2023)

Goldman v. United States, 316 U.S. 129, 62 S. Ct. 993 (1942) <casetext.com/case/goldman-v-united-states-shulman-v-same?q=Goldman%20v.%20United%20States&sort=relevance&p=1&type=case> (last retrieved Aug. 13, 2023)

Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967) <casetext.com/case/katz-v-united-states-2?sort=relevance&type=case&resultsNav=false&tab=keyword#p353> (last retrieved Aug. 13, 2023)

Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928) <casetext.com/case/olmstead-v-united-states-green-v-same-innis-v-same?> (last retrieved Aug. 13, 2023)

Riley v. California, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 24 Fla. L. Weekly Supp. 921 (2014) <casetext.com/case/riley-v-cal-united-states-1?> (last retrieved Aug. 13, 2023)

Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979) <casetext.com/case/smith-v-maryland?> (last retrieved Aug. 13, 2023)

United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936) <casetext.com/case/us-v-curtiss-wright-corp?sort=relevance&type=case&resultsNav=false&tab=keyword> (last retrieved Aug. 13, 2023)

United States v. Jones, 565 U.S. 400, 132 S. Ct. 945, 181 L. Ed. 2d 911, 23 Fla. L. Weekly Supp. 102 (2012) <casetext.com/case/united-states-v-jones-1419?sort=relevance&type=case&tab=keyword&jxs=&resultsNav=false&q=565%20U.S.%2040 0,%20134%20S.%20Ct.%20945%20(2012)&p=1> (last retrieved Aug. 13, 2023)

United States v. Microsoft Corp., 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018) <casetext.com/case/united-states-v-microsoft-corp-9?q=USA%20v.%20Microsoft,%2017-2&sort=relevance&p=1&type=case&tab=keyword&jxs=> (last retrieved Aug. 13, 2023)

United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619 (1976) <casetext.com/case/united-states-v-miller-89?sort=relevance&type=case&tab=keyword&jxs=&resultsNav=false> (last retrieved Aug. 13, 2023)

United States v. United States District Court, 407 U.S. 297, 92 S. Ct. 2125 (1972) <casetext.com/case/united-states-v-united-states-district-court?sort=relevance&type=case&tab=keyword&jxs=&resultsNav=false> (last retrieved Aug. 13, 2023)

United States v. Verdugo-Urquidez, 494 U.S. 259, 110 S. Ct. 1056 (1990) <casetext.com/case/united-states-v-verdugo-urquidez?sort=relevance&type=case&tab=keyword&jxs=&resultsNav=false> (last retrieved Aug. 13, 2023)

US Courts of Appeals

Microsoft Corp. v. United States (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) <casetext.com/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp> (last retrieved Aug. 13, 2023)

Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 11 Cal. Daily Op. Serv. 12562, 2011 Daily Journal D.A.R. 14935 (9th Cir. 2011) <casetext.com/case/suzlon-energy-ltd-v-microsoft-corporation?sort=relevance&type=case&tab=keyword&jxs=&resultsNav=false> (last retrieved Aug. 13, 2023)

United States v. Bank of Nova Scotia, 740 F.2d 817 (11th Cir. 1984) <casetext.com/case/in-re-grand-jury-proceedings-bk-nova-scotia?sort=relevance&type=case&resultsNav=false&tab=keyword> (last retrieved Aug. 13, 2023), cert. denied, 469 U.S. 1106 (1985)

US Districts Court

In re Search Warrant No. 16-1061-M to *Google*, 232 F. Supp. 3d 708 (E.D. Pa. 2017) <casetext.com/case/in-re-search-warrant-no-16-1061-m-to-google?sort=relevance&type=case&resultsNav=false&tab=keyword> (last retrieved Aug. 13, 2023)

EU Jurisdiction

European Union

CJEU Oct. 19, 2016, C-582/14, *Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779

CJEU Apr. 5, 2022, C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others*, ECLI:EU:C:2022:258

CJEU Oct. 6, 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier ministre and Others*, ECLI:EU:C:2020:791

CJEU Nov. 19, 1998, C-162/97, *Nilsson and others*, ECLI:EU:C:1998:554

CJEU Oct. 6, 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650

CJEU July 16, 2020, C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, ECLI:EU:C:2020:559

EGT Apr. 26, 2023, T-557/20, *Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS)*, ECLI:EU:T:2023:219

Member States

Data Protection Commission (Ireland) May 12, 2023, IN-20-8-1, *Meta Platforms Ireland Limited*

Bundesverwaltungsgericht (Austria) May 5, 2023, W245 2252208-1/36E W245 2252221-1/30E, *Google Analytics*

DPA (Austria) Dec. 22, 2021, DSB-D155.027, 2021-0.586.257, *Google Analytics I*

DPA (Austria) Apr. 22, 2022, DSB-D155.026, 2022-0.298.191, *Google Analytics II*