esade

EsadeEcPol - Center
for Economic Policy

Open Internet Governance Institute

PAPER SERIES # 2

Transatlantic Data Sovereignty: How to Achieve Privacy-proof Data Flows between the EU and the US

Matthias Bauer
Senior Economist at ECIPE

MARCH, 2022

About the author

Matthias Bauer (PhD)
is Senior Economist at the European Centre
for International Political Economy (ECIPE)

Executive Summary

→ **The state of the problem.** The European Court of Justice (CJEU) ruled in July 2020 that in the US there is no sufficient level of protection for personal data of EU citizens, thus invalidating the 2016 US-EU Privacy Shield agreement that served as a basis for transatlantic data transfers. Recently, theEuropean Commission and the US government jointly announced an "agreement in principle" to produce a new framework for data f lows. However, its content, its specifics and especially its translation into enhanced changes will be key to ensure it is more sustainable than its predecessor.

→ **What's at a stake.** The ruling, along with vague and uncertain guidance given by European Data Protection Authorities and its erratic enforcement by national entities, generated considerable uncertainty for businesses (small and large), organizations and private citizens around a central aspect of global economic governance: over the past 15 years data has enabled trade in digital services between the US and Europe to double; and digital as well as less digital industries, e.g., traditional manufacturing, critically depend on data that flows between the EU and the US.

→ **Key roadblock.** The CJEU considers that US data collection powers under current surveillance laws lack effective redress options for EU citizens, allowing government agencies to collect information from foreign users outside their national territory, but without them having the same means that US citizens do have to defend their privacy through the judicial process. This prioritization of national security over (foreign citizens') privacy spurs from distinct approaches to privacy in both legal systems: In the EU, the protection of personal data is considered a fundamental right; in consequence, the European General Data Protection Regulation (GDPR) imposes mandatory rules for how organisations and companies must use personal data and gives authorities capacity to act ex officio on breaches from this basic privacy protection. In contrast, the US has no GDPR federal equivalent (nor immediate plans or credible attempts to produce one), relies on state-level regulation of different scope, substance, and procedural issues, usually placing the responsibility to correct negative externalities on private actors and their specific actions.

→ **A potential way forward.** The end goal EU & US should set themselves is "transatlantic data sovereignty", i.e. privacy-proof transfers of individuals' personal data based on the shared common goals and principles of value-based standards for international trade and technology among rights-oriented and rule of law-based market democracies. Despite these commonalities, it might be best to take a pragmatic approach acknowledging the limited scope for agreement, thus focused on adequacy, equivalence, or mutual recognition. The departing minimum for it should be mirrored EU-US conditions recognizing redress options and reining in surveillance capacities. The US government has recently signaled its willingness to implement a new framework that features both novelties.

→ **Within the US,** the main issue would be the articulation of the political process. We suggest three distinct paths:

1. The most expeditive and efficient would be an Executive Order that limits bulk collections of data by US surveillance agencies and that provides additional redress mechanisms for European citizens, such as an executive office or tribunal with the power to adjudicate complaints and issue binding decisions on US intelligence services. This seems to be the preferred approach by the current US government, which has committed to include its upcoming commitments in a new EO. The central problem of this alternative would be its long-term sustainability after the end of the current Administration.

2. The most sustainable in the long term would follow a conventional legislative path: US Congress could amend FISA to prohibit bulk intelligence collections and require court approval with respect to each target of surveillance. However, this route might prove too slow for the urgency of the matter, as well as subject to political uncertainty: the political situation in the US is challenging, characterised by a divided Senate, distinct partisanship, and upcoming midterm elections.

3. A non-statutory solution is also on the table, for instance by amending the role of the Ombudsperson to empower it to act ex officio on behalf of privacy protection. This alternative, fast and perhaps more politically feasible, bears the problem of difficult to assess whether a non-statutory option would meet substantive European requirements on redress, and whether it would lead to stable and reliable rules.

→ **Within the EU,** Member States are not subject to the same standards as foreign entities are. In fact, certain Member States (e.g. France) expressed in the past their willingness to entirely exclude their intelligence agencies from the scope of EU law. But, to make it sustainable, any US concession on the possibility of redress should be effectively mirrored by EU Member States' treatment of personal data of US citizens. This opens up a possibility for other EU Member States to advocate a mirrored EU approach to US concessions on fundamental redress rights in the context of government surveillance activities, underlining their commitment to EU fundamental rights, economic openness and meaningful Transatlantic cooperation to resolve the privacy-security dilemma.

Transatlantic Data Sovereignty: How to Achieve Privacy-proof Data Flows between the EU and the US

Personal data of European citizens cannot simply be transferred to, accessed from, and stored in the United States (US). This is, in general terms, the implication of a ruling by the European Court of Justice (CJEU) from July 2020, the socalled Schrems II ruling. The judgement found that in the US there is no level of protection for personal data of EU citizens that is essentially equivalent to protection under the EU's General Data Protection Regulation (GDPR) interpreted in light of the Charter of Fundamental Rights of the European Union.[1] The CJEU argues that US government surveillance powers are not limited as required by EU law, and objects that EU citizens do not have effective means of redress. The immediate consequence of the ruling and its implementation by European Data Protection Authorities were thousands of EU and US companies, including SMEs, that no longer could rely on the 2016 US-EU Privacy Shield agreement as a basis for transferring personal data across the Atlantic.

The Schrems II ruling also has a multilateral dimension. Currently, in addition to the US, most countries outside the EU do not have a level of equivalent data protection. As a result, data flows from the EU to these countries, including authoritarian countries like China and Russia, can be deemed illegal by EU authorities.[2] Moreover, the CJEU instructs organisations (public and private), when sending personal data under standard contractual clauses (SCCs), to assess actual protections "as regards any access by the public authorities of that third country to the personal data transferred" and "the relevant aspects of the legal system of that third country." Unless these protections are "essentially equivalent" to EU measures, companies are supposed to cease their personal data transfers.

With the invalidation of the 2016 Privacy Shield Agreement by the 2020 Schrems II decision, the regulation of cross-border data flows once again moved to the top of transatlantic dialogue.[3] Although many observers initially believed that the EU and the US would soon agree on a new mechanism transfer of personal data,

1 See case C-311/18, known as the "Schrems II" decision.

2 See European Commission (2022). Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection. Available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. As of January 2022, the European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the Law Enforcement Directive (LED), and Uruguay as providing adequate protection.

3 On October 6, 2015, the CJEU issued a judgment declaring invalid the European Commission's July 26, 2000 decision on the legal adequacy of the US-EU Safe Harbor Agreement. On July 12, 2016, the European Commission issued an adequacy decision on the EU-US Privacy Shield Framework. This new Framework, which replaces the Safe Harbor program, provides a legal mechanism for companies to transfer personal data from the EU to the United States.

and despite encouraging public statements issued by the Commission and the US since November that culminated in the March 2022 announcement of an "agreement in principle" to produce a new framework, there is no tangible outcome yet. Currently, **guidance** by the European Data Protection Board (EDPB) and national Data Protection authorities **remains rather vague and creates legal uncertainties,** which are particularly burdensome for small businesses. At the same time, **erratic enforcement decisions by national Data Protection authorities call for timely action to establish a reliable legal mechanism for privacy-proof transfer of personal data** outside of the EU.[4]

Some 20 months have now passed since the invalidation of the Privacy Shield. Beyond the "agreement in principle" public commentary suggests that the EU and US representatives still have differing views about key aspects of privacy and the protection of personal data, ranging from national security considerations to enforcement practices. Focussing on the Transatlantic political and economic relationship, the subsequent sections of this policy brief will address **critical roadblocks** impeding the quest for a more harmonised, less uncertain environment for privacy-proof data flows. It will then outline **policy options** for ensuring **"transatlantic data sovereignty",** defined here as **privacy-proof transfers of individuals' personal data between the EU and the US,** and how complementary policies could find acceptance in other parts of the world.

Policy space and impediments for transatlantic cooperation on data privacy

The free flow of data is highly important to the transatlantic economic relationship. If data transfers between the EU and the US would come to a halt, both the EU and the US would experience significant losses in trade and domestic economic activity. A recent impact assessment finds that **digital as well as less digital industries,** e.g., traditional manufacturing, **critically depend on data that flows between the EU and the US,** including various types and combinations of personal and non-personal data.[5] In addition, over the past 15 years data has enabled trade in digital services between the US and Europe to double. The free flow of data allows consumers and companies from the EU and the US to take advantage of modern services, such as e-commerce applications, cloud services, healthcare services, and a broad spectrum of digital services used to support business operations across industries.

Data is therefore often considered the lifeblood of trade and investment, supporting international production processes and research and development activities. As such the free flow of data contributes to economic resilience and "digital sovereignty" across industries, particularly those that are data intensive such as information, telecommunications, financial, and professional services.[6]

4 See, e.g., noyb (2022). Austrian DSB: EU-US data transfers to Google Analytics illegal, 13 January 2022. Also see Politico (2022). French privacy regulator rules against use of Google Analytics, 10 February 2022.

5 See ECIPE-Kearney (2021). The economic costs of restricting the cross-border flow of data. Available at: https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625067571000.

6 Notions of digital, technological or industrial sovereignty (or autonomy) remain ambiguous. A critical discussion of EU policy conceptions on the theme is provide by Bauer and Erixon (2021). Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. ECIPE Occasional Paper02/2020.

Both the EU and the US highly benefit from greater access to goods and services and jobs created by transatlantic investments and digital trade. Trade and investment statistics reveal that many EU countries are highly exposed to transatlantic commerce, which requires the free transfer of personal and other data. For example, jobs directly supported by US majority-owned affiliates in 2019 are estimated to amount to 666,000 in Germany, 506,000 in France, and 179,000 in Spain. Likewise, US jobs directly created by majority-owned companies from the EU amount to 882,000 for Germany, 799,000 for France, and 93,000 for Spain. Transatlantic services trade, which often relies on personal data, is fairly balanced and already takes a high share in EU countries' total exports to and imports with the US.[7] In 2019, US services exports to Germany amounted to USD 36.6 billion, while German services exports to the US amounted to USD 34.9 billion. US services exports to France amounted to USD 22.4 billion, while French services exports to the US amounted to USD 20.4 billion. Similarly, US services exports to Spain amounted to USD 8.7 billion, while Spanish services exports to the US amounted to USD 7.8 billion.[8]

Table 1. Estimating the size of US-linked investments in major European countries

	Spain	France	Germany
In-country jobs by US-owned companies	179,000	506,000	666,000
Service exports to US	$7.8b	$20.4b	$36.6b
Service imports from US	$8.7b	$22.4b	$34.9b

Governments are generally aware of the economic significance of data for trade and investment. **Regulations of data flows and storage requirements have thus become a critical aspect of digital economic governance across the globe.**[9] This is also true for the EU and the US. From an **economics** point of view, it would be in the **self-interest of both jurisdictions to establish a reliable and future-proof regulatory framework for the exchange of personal data and non-personal information across the Atlantic.** But there is more to build on. While there are differences in how the EU and the US approach privacy and the protection of citizens' personal data, there are important commonalities to consider in bilateral negotiations and,

7 For example, in 2019 Spain exported USD 138 billion worth of services. The top services exported were personal travel (USD 74.9 billion), business, professional, and technical services (USD 24.8 billion), transportation (USD 18.7 billion), business travel (USD 4.8 billion), and financial services (USD 3.85 billion). See Observatory of Economic Complexity (OEC). For an overview of digital modes of supply/delivery of services, see OECD (2020). Handbook on measuring Digital Trade, jointly published by the OECD, the WTO, and the IMF.

8 For an overview of trade and investment relationships in the transatlantic economy, see AmCham (2021). The Transatlantic Economy in 2021, Annual Survey of Jobs, Trade and Investment between the United States and Europe.

9 See, e.g., Svantesson, D. (2020-12-22), Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris.

potentially, multilateral fora: first, both the EU and the US have long tradition of **respect for human rights and the rule of law,** calling for legal certainty for individuals and businesses. Second, both the EU and the US consider data protection an important element of **consumer protection,** including electronic data. And third, both jurisdictions, share **similar concerns about human (or citizens') rights,** e.g., unlimited or disproportionate requirements by governments that compel access to personal data held by the private sector.[10] Finally, following the agenda of the Transatlantic Trade and Technology Council (TTC), both the EU and the US aim to jointly develop "value-based" standards for trade and technology than should be applied in likemined countries globally.[11]

The economic significance of the free flow of data, including the secure flow of personal data, together with a common understanding of human rights and the principle of the rule of law **should provide enough policy space for meaningful cooperation towards harmonised approaches or, at least, equivalence decisions** (mutual recognition) on either side. However, the devil is with the details. EU and US statutory approaches on data privacy currently differ from each other. In addition, the current US understanding of the extent of US human rights obligations differs from that of the EU, effectively limiting the policy space for meaningful outcomes. EU and US approaches to data privacy regulations are briefly outlined below.

Data privacy regulation in the EU

In 2016, the EU adopted the GDPR, which replaced the 1995 Data Protection Directive, seeking to strike a balance between the protection for the data of individuals and the free movement of personal data within the EU. The EU's statutory law on privacy – GDPR – is a consequence of EU primary law. **In the EU, the protection of personal data is considered a fundamental right.** In the Member States, national constitutions and the Charter of Fundamental Rights of the EU apply. Articles 7 and 8 of the Charter provide that "everyone has the right" to the "protection of personal data concerning him or her" and that 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."[12] Article 52 allows limitations on these rights only if they are "[s]ubject to the principle of proportionality" and must be "necessary and genuinely meet objectives of general interest of the Union or the need to protect the rights and freedom of others." Moreover, Article 47 of the Charter grant any individual who has had these rights violated to a "fair public hearing within a reasonable time by an independent and impartial tribunal previously established by law."

10 See, e.g., OECD (2021), reflecting the work of the OECD Committee on Digital Economy Policy to which the US and individual EU countries are members. It should be noted that OECD members have a long tradition of respect for human rights and the rule of law, and also share a strong commitment to protecting the fundamental right to priva-cy, when personal data is subject to access of governmental agencies.

11 See European Commission (2021). EU-US launch Trade and Technology Council to lead values-based global digital transformation, press release, 15 June 2021.

12 See Charter of Fundamental Rights of the European Union, 2012/C 326/02, Article 7 and Article 8.

The **EU's GDPR imposes mandatory rules for how organisations and companies must use personal data.**[13] In general terms, GDPR means to provide data protection for EU citizens' personal data, to reduce the severity and frequency of data breaches, and the potential for mishandling or misprocessing of personal data on the web. Accordingly, GDPR establishes several obligations for data controllers and processors and provides rights for citizens, such as consent allowing data processing for a specific purpose, transparency rights, and the right to be forgotten. GDPR applies to data controllers and processors that are established in the EU, provide goods or services to individuals in the EU, or monitor individuals' behaviour in the EU.[14]

GDPR is now recognised as law across the EU. It is an EU Regulation, which (rather than an EU Directive) was intended to be directly applicable and result in harmonisation across EU Member States. However, despite being a Regulation, GDPR does not create fully identical privacy rules across all Member States. It indeed significantly increases harmonisation, but certain aspects fall outside its scope because these areas are outside the EU's legislative competence, e.g., national security. In addition, some rules allow for policy discretion at the national level, e.g., specific rules for the processing of sensitive personal data (e.g., genetic data, healthcare data, data related to employment, criminal data), specific rules for data processing, and the imposition of additional criteria that must be satisfied to process personal data for new purposes. In addition, EU Member States follow different approaches regarding conditions that permit the processing of personal data relating to criminal convictions.[15]

GDPR, which is interpreted considering the Charter of Fundamental Rights of the EU, also regulates **the conditions under which data exporters may transfer personal data from the EU to foreign countries** (Chapter 5, Articles 44-50).[16] Data processors and controllers generally may transfer personal data to foreign countries, if the European Commission has found that the country ensures an **adequate level of protection**. In addition, data exporters can adopt certain **appropriate safeguards**: data exporters may adopt binding corporate rules (BCRs) that comply with GDPR requirements or may use standard contractual clauses (SCCs), which are specific contractual terms approved by the European Commission.[17]

13 Personal data is considered any information which, directly or indirectly, could identify a living person. Name, phone number, and address are schoolbook examples of personal data. Interests, information about past purchases, health, and online behaviour is also considered personal data as it could identify a person.

14 In GDPR a data processor is considered a person or entity who determines the "purposes and means" of processing personal data) and a processor is considered a person or entity who processes the data on behalf of a controller.

15 See, e.g., White and Case (2019). GDPR Guide to National Implementation - A practical guide to national GDPR compliance requirements across the EEA, 13 November 2019.

16 See GDPR, Chapter V.

17 On 4 June 2021, the European Commission issued modernised SCCs for data transfers from controllers or processors in the EU/EEA to controllers or processors established outside the EU/EEA (and not subject to the GDPR). It should be noted that under Article 49 GDPR the exporter may also rely on several "derogations for specific situations", e.g., the data subject gave informed consent to the transfer or where the transfer is "necessary for the performance of a contract" that is either "between the data subject and the controller" or was concluded "in the interest of the data subject."

US views on data privacy and regulation

There is no federal data privacy law like the **GDPR** in the US. However, several national laws have been put in place to regulate the use of data in specific sectors of the economy. These include:

- **1974:** The U.S. Privacy Act outlines rights and restrictions regarding data held by U.S. government agencies.[18]
- **1996:** Health Insurance Portability and Accountability Act (HIPAA) regulates privacy and security in the healthcare industry.[19]
- **1999:** Gramm-Leach-Bliley Act (GLBA) governs how consumers' non-public privacy information is collected and used in the financial industry.[20]
- **2000:** Children's Online Privacy Protection Act (COPPA) took a first step at regulating personal information collected from minors. The law prohibits online companies from asking for PII from children 12 and under unless there's provable parental permission.[21]

Beyond these legislations, **there have not been credible attempts by the US federal government to update privacy laws with the introduction of new Internet applications, ecommerce, and large online platforms.** Some proposed regulations, e.g., the "American Data Dissemination Act", the "Consumer Data Protection Act", and the "Data Care Act" did not gain sufficient support in Congress. Accordingly, the US still lacks federal regulations covering consumer privacy and data security in all industries.[22]

While the federal government has not developed a version of the EU's GDPR, **several US federal states like California and Washington have enacted similar data-protection laws.** These laws have similarities with GDPR, but they do not fully replicate it.[23] They **differ in scope, substance and procedural issues.** While the EU's GDPR protects natural persons of any nationality and establishes requirements for companies, governmental and non-profit organisations, California's CCPA is restricted to California residents and large businesses that operate in the state of California. Similarly, the Washington Privacy Act also covers only large businesses that conduct business in Washington State. GDPR and US federal laws also differ regarding the elements of obligations imposed on data collectors, such as risk assessments, data minimisation requirements, and purpose limitation. For businesses, complying with different legal requirements within the US is costly. Moreover, since there is no federal governing force protecting consumers' data and privacy

18 "Privacy Act," 5 U.S.C. § 552a (1974), https://www.justice.gov/opcl/privacy-act-1974.

19 "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," CDC, February 21, 2019, https://www.cdc.gov/phlp/publications/topic/hipaa.html.

20 "Gramm-Leach-Bliley Act," Federal Trade Commission, accessed February 8, 2022, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

21 "Children's Online Privacy Protection Rule ('COPPA')," Federal Trade Commission, July 25, 2013, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

22 "2021 Consumer Data Privacy Legislation," NCSL, accessed February 8, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx.

23 Fefer, R. F. and Archick, K. (2022). EU Data Protection Rules and U.S. Implications.

rights, US federal states that enact regulations are left to act alone in enforcement. This leads to compliance becoming confusing and inconsistent. Regarding enforcement, the **European system** is largely based on dedicated data protection agencies that act as **ex officio protectors of individual rights,** while in the **US, policymakers** at the federal level seem to **prefer a less interventionist approach aimed at balancing the interests of companies and consumers. US policymakers generally place the responsibility to correct negative externalities on private actors and their specific actions**, typically through the judicial system but also through the FTC as an enforcing agency.

In the US, the most important data protection standards for the Internet come from statutory law. They are not derived from human rights commitments. In 1992, the US indeed ratified the International Covenant on Civil and Political Rights (ICCPR), a human rights treaty that guarantees privacy rights. Article 17 protects individuals from arbitrary or unlawful interferences with their "privacy, family, home, or correspondence."[24] However, there has been no material discussion since then regarding privacy laws and their relation for "digital privacy" as a fundamental right. Contrary to the EU, US policymakers (and the US legal system respectively) do so far not accept the principle of "universality of human rights". In practice, this means that **in the US view the ICCPR applies "only to individuals who are both within the territory of a State Party and subject to its jurisdiction".**[25] In other words, the US views is that the ICCPR does not apply extraterritorially. This is a major impediment for a transatlantic agreement on cross-border flows of personal data.

In its Schrems II ruling, the CJEU invalidated the European Commission' Privacy Shield decision from 2016. Back then, the Commission concluded that transfers of personal data to the US pursuant to the agreed Privacy Shield framework provide an adequate level of protection to EU data subjects.[26] Under the agreement, US organisations had self-certify to the US Department of Commerce that they will comply with GDPR-like requirements, e.g., notice requirements, data retention limits, security requirements, and data processing purpose limitations. In 2016, the Commission also found that US government access to European citizens' personal data is effectively restricted, ensuring effective legal protection against interferences by US intelligence agencies. The European Commission acknowledged that non-US citizens have only limited redress rights, but t the same time stated that a sufficient level of protection is granted by the new ombudsperson mechanism.[27]

With the Schrems II ruling, the **CJEU annulled the European Commission's assessment** and decision respectively. It found that **US data collection powers under current surveillance laws lack effective redress options for EU citizens.** The US Foreign Intelligence Surveillance Act (FISA) in its Section 702 **allows government agencies to collect information from foreign users outside their national territory, but without them having the same means that US citizens do have to defend their privacy through the judicial process.** It is primarily this prioritization of national security over privacy and the protection of personal data that led the CJEU to invalidate the Privacy Shield.

---

24 "Human Rights and Privacy," American Civil Liberties Union, accessed February 8, 2022, https://www.aclu.org/issues/human-rights/human-rights-and-privacy.

25 See European Parliament (2021). Exchanges of Personal Data After the Schrems II Judgement. Study requested by the LIBE committee, July 2021. Also see, e.g., statement of Matthew Waxman, Principal Deputy Director for Policy Planning at the State Department, to the UN Human Rights Committee on 17 July 2006.

26 See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176).

27 See Privacy Shield agreement ANNEX A: EU-U.S. Privacy Shield Ombudsperson Mechanism.

Policy options

While there are differences in how the EU and the US approach privacy and the protection of citizens' personal data, there are important commonalities to be built on in transatlantic negotiations and multilateral fora:

1. **both the EU and the US have long tradition of respect for human rights and the rule of law,**
2. **the EU and the US consider data protection an important element of consumer protection, including electronic data,**
3. **both jurisdictions share similar concerns about unconstrained, unreasonable, or disproportionate government access to personal data held by private individuals and organisations,**
4. **several US federal states have implemented or are considering legislation like the EU's GDPR, even if they do not fully replicate it, and**
5. **both jurisdictions renewed their commitment under the TTC to work together on value-based standards for international trade and technology that are conducive to cross-border commerce.**

Despite these commonalities, **the scope for full harmonisation of privacy laws remains fairly limited.** As outlined above, GDPR itself does not fully harmonise EU Member States' data protection laws. In addition, a key difference between approaches to privacy in the US and the EU is their point of focus. US policymakers seemed in the past to be more concerned about the integrity of data as a commercial asset, while GDPR firmly puts individual rights before the interests of businesses. Moreover, the EU and the US have **different approaches to implementing new legislation,** which affects which law may pass. With GDPR, the EU relied more on a top-down approach that balances Member State and supranational policies. By contrast, the US has a bottom-up approach that reflects federal states' rights in governing and can make initiatives like privacy rights complicated legislation to pass. **Adequacy, equivalence, or mutual recognition are therefore more promising ways to arrive at a meaningful and future-proof solution** that ends legal uncertainties for transatlantic data flows. Adequacy, equivalence, or mutual recognition also trump the use of Article 49 derogations, which according to some experts might be a reliable legal basis for intra-company transfers of personal data, because these derogations potentially discriminate against organisations other than large companies or groups of companies.[28]

28 See European Parliament (2021). Exchanges of Personal Data After the Schrems II Judgement. Study requested by the LIBE committee, July 2021. Also see, e.g., statement of Matthew Waxman, Principal Deputy Director for Policy Planning at the State Department, to the UN Human Rights Committee on 17 July 2006.

A **key roadblock** to adequacy, however, is the **current US view on the application of fundamental rights to non-US citizens,** which impacts on whether and how Europeans can have effective redress in US courts. It is unlikely that the European Commission and European Data Protection authorities (which, however, do not have the power to veto a political agreement) would accept any agreement that preserves the status quo in the US and falls short of ensuring key principles such as oversight and accountability, transparency about government requests, and effective redress rights – even though in practice it might be very difficult for citizens to detect infringements. The same applies to the CJEU, which is unlikely to wave through any new agreement not meeting these bars.

It should be noted, nonetheless, that several observers pointed to a **certain disconnect between the standards to which the CJEU holds the US surveillance systems and the standards within the EU itself.** In the EU national, security is the sole responsibility of Member States. Each Member State government is free to apply its own national security policies and balance it with EU privacy obligations. "In fact, GDPR uses the threat of withdrawing access to EU personal data as a tool to seek reform of other country's security agencies to reflect the CJEU notion of proportionality, while exempting member state governments from similar expectations or threats."[29] However, EU governments are still bound by the European Convention on Human Rights (ECHR). In his opinion on Schrems II, the Advocate General argued that **even when EU law does not apply to a Member State, an adequacy assessment of a third country's surveillance laws and practices should be based on the ECHR standards** otherwise binding upon EU member states.[30]

Some EU Member States, such as France, expressed in the past their willingness to entirely exclude their intelligence agencies from the scope of EU law.[31] Accordingly, **any US concession on the possibility of redress such as the one suggested by the White House and the European Commission on its March 25 joint release should be effectively mirrored by EU Member States' treatment of personal data of US citizens** for the purpose of surveillance and national security enforcement. Considering the above, EU-US negotiations should generally build on the OECD's working group on "government access to personal data held by the private sector", and other initiatives such as the Reform Government Surveillance coalition (RGS),[32] and the Global Network Initiative (GNI)[33]. EU Member States, such as Spain, the Baltics and the Nordics, could advocate a mirrored EU approach to US concessions on fundamental redress rights in the context of government surveillance activities, underlining their commitment to EU fundamental rights, economic openness and meaningful Transatlantic cooperation to resolve the privacy-security dilemma.

---

29 Meltzer, J.P. (2020). The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security, 5 August 2020. Also see Baker, S. (2020). Cross-border data, How Can the U.S. Respond to Schrems II?, 21 July 2020.

30 See Opinion of Advocate General Saugmandsgaard, delivered on 19 December 20191 Case C-311/18

Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, interveners: The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope.

31 Lawfare (2021). How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States, 8 March 2021.

32 RGS calls on governments around the world to adhere to the following principles when conducting surveillance. Key RGS principles are outlined at https://www.reformgovernmentsurveillance.com/principles/.

33 GNI members believe that freedom of expression and privacy are critical to fostering stability, inclusiveness, and security. As such, government surveillance activities must comply with principles of rule of law and democratic governance, as well as human rights principles such as legality, necessity, and proportionality. See https://globalnetworkinitiative.org/policy-issues/surveillance/.

As regards US concessions, many US policymakers indeed share concerns about the current situation. In December 2020, the Senate Committee on Commerce, Science and Transportation held a hearing on the Invalidation of the "Privacy Shield and the Future of Transatlantic Data Flows". Concerns were expressed about the need to reform current US surveillance laws: "agreement that a privacy law alone is not enough; rather the US must also examine its approach to intelligence gathering and look towards surveillance reform, possibly to include consensus building on intelligence gathering/surveillance and data protection with other large-scale democracies".[34]

Many observers argue that there are important advantages to enacting a new legal statute in the US to provide redress, but there remain high political obstacles, including bipartisan and constitutional barriers. A non-statutory solution, which does not stand in opposition with EU law, might be an alternative. As recently argued by Christakis et al. (2021), EU law is "flexible in interpreting whether the US must adopt a new statute to meet redress requirements, especially when the question is viewed through the "essential equivalence" prism of data protection."[35] This may, for example, require amendments in the role of the Ombudsperson, as suggested by the European Data Protection Supervisor. The Ombudsperson should be able "to act independently not only from the intelligence community but also from any other authority. In practical terms, the possibility of reporting directly to Congress could be one option in this regard."[36]

US policymakers are not bound by recommendations of the CJEU, but it is difficult to assess whether a non-statutory option would meet substantive European requirements on redress, and whether it would lead to stable and reliable rules. However, to provide an adequate level of protection to EU data subjects, particularly redress rights, US policymakers could consider **two potentially more promising options (and not mutually excludable):**[37]

(1) US executive action: US President Biden could issue an **Executive Order** that **limits bulk collections of data by US surveillance agencies and that provides additional redress mechanisms for European citizens**, such as an executive office or tribunal with the power to adjudicate complaints and issue binding decisions on US intelligence services. In this regard, the White House statement following the joint announcement by the EU and the US, referring to the possibility for EU individuals to seek redress seems to go in the right direction. Furthermore, the statement also mentioned the willingness to employ an EO as a legally binding commitment device.

(2) New US legislation: **US Congress could amend FISA to prohibit bulk intelligence collections and require court approval with respect to each target of surveillance. Recent signals by the US government seem to be willing to restrict information collection "only where necessary**

34 See National Law Review (2020). Senate Commerce Committee Holds Hearing on the Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows, 21 December 2021. Testimonies can be accessed at https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows.

35 See Christakis, T, Propp, K. and Swire, P. (2021). EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution. 21 January 2021.

36 See Opinion 4/2016, Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016.

37 See, e.g., Congressional Research Services (2021). EU Data Transfer Requirements and U.S. Intelligence Laws: Un-derstanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, 17 March 2021.

to advance legitimate national interests", as stated on March 25 by the White House. New legislation could also establish the right for European citizens (or non-US citizens in general) to bring complaints before a tribunal if they assume intelligence agencies have collected or used their data in an unlawful way.

New legislative action might take time. The political situation in the US is challenging, characterised by a divided Senate, distinct partisanship, and upcoming midterm elections. In consequence, the US intention is for the Commission to use its upcoming Executive Order as a basis for its necessary adequacy decision. However, such a diplomatic solution, may be annulled by the CJEU, or criticised by the EDPB or Europe's national data protection authorities for being inconsistent with GDPR or the Charter of Fundamental Rights of the EU. Similarly, a new international treaty that would prevail over the Charter of Fundamental Rights would likely meet substantial public resistance in the EU and thus be rejected by EU Member States.

Considering privacy laws recently imposed by countries globally and recent EU adequacy decisions, e.g., decisions on essential equivalents on privacy laws of Japan, South Korea, or the UK, **any new policy for the protection of personal data in cross-border trade should include appropriate redress rights for citizens** (data subjects) **in recipient countries, limits and redress rights concerning bulk intelligence,** and independent authorities (including but not limited to tribunals) adjudicating complaints of citizens and data controllers and processors respectively. The mention to a "new multi-layer redress mechanism that includes an independent Data Protection Review Court" by the White House on March 25 seems to take this road, but this is just its beginning.

High standards for privacy-proof transfers of individuals' personal data that are shared and jointly pushed by the EU and the US could find acceptance in other parts of the world. Recognising the joint EU-US objective to uphold common values, the EU, the US and individual EU Member States could set a high global standard to contain the dissemination of rules and practices embraced by authoritarian countries, e.g., China's state-centric data sovereignty model, and heavy-handed policies such as forced data localisation requirements and authorities having unlimited access to personal information of citizens without their consent. A joint EU-US initiative in this field would contribute to meaningful consumer rights, more consistent international enforcement, and provide the certainty needed for businesses and citizens to tap into new opportunities from digital trade and cross-border commerce.

esade

EsadeEcPol - Center
for Economic Policy

Open Internet Governance Institute

The OIGI is EsadeEcPol's effort to shape debates on Internet, data & digital governance both in Spain and across the European Union, while simultaneously contributing to a better understanding of how best use new data and AI-related tools to support and improve policymaking.

We intend to contribute in a balanced and evidence-based manner, departing from the delimitation of weighed dilemmas to focus on offering viable solutions. Our ultimate goal is to help building a system of global and open internet governance, fostering the best possible digital environment among the many future worlds that open before us.

Supported by

Meta