"The impact of the Schrems rulings on E.U. - U.S. data transfer relations and their relevance for the regulation of developing technologies."

Valentina Nicole Tilli

Law School and School of Economics and Global Affairs, IE University, Madrid, Spain.
Bachelor's in Laws and International Relations

E-mail: valentinanicole.tilli@gmail.com

Published January 2026

Editor: Celeste Shattuck, Georgetown University

Abstract

Developing technologies like Artificial Intelligence ("AI") involves the collection, processing, and transfer of an amount of sensitive data never seen before. This raises questions about how different countries and organisations can regulate the issue through appropriate legislation. This problem has been specifically affecting relations between countries and jurisdictions such as the United States ("U.S.") and the European Union ("EU"). The current situation is mirroring what has been happening since 2016, when the spread of the Internet and social media drastically increased the relevance of personal data. The Schrems cases tackled the difference between European and American data protection and the resulting issues. Analysing the solutions found and the regulations created is essential to understanding how to face the current situation.

Keywords: personal data, data protection, international data transfer

1. Introduction

Nowadays, the world runs on data. Information influences the way people are seen and treated, and individuals rely on it heavily in their daily lives. However, data is defined differently in every jurisdiction. According to the European Commission, personal data is "information that relates to an identified or identifiable individual".[1] The U.S. defines personal data similarly as "personally identifiable information."[2] Personal data is constantly used, collected, and processed by both individuals and organisations. Processing of information

[1] European Commission, 'Data Protection Explained' (*European Commission*2023) <https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en>.

[2] 'Data Protection Laws | International Toolkit' (world-toolkit.yale.edu) <https://world-toolkit.yale.edu/regulated-activity/data-protection-laws>.

 © IE Creative Common License

includes its use, collection, and storage. One of the most relevant uses of data processing in a globalised world is the daily transfer of data between countries. International information transfers are increasingly important due to the development of new technologies, such as AI, that rely on them. However, this creates problems because countries and jurisdictions have varying views on what data is and how it should be protected, affecting the ease of the transaction. One of the biggest discordances discussed in recent years is between the E.U. and the U.S., having higher data flows than anywhere else.[3] Yet, this fundamental process is very complicated due to their different perception of data protection. In a world where new technologies are developing at an unprecedented pace, regulators must grapple with how this divergence in data policy should be handled. Analysing how this problem has been previously addressed can offer guidance for future solutions.

2. Differences between EU and US:

2.1. The concept of data protection

In the E.U., data protection is part of the Fundamental Charter of Rights,[4] and strict protective regulations are applied to protect EU citizens. However, U.S. law deals with data protection differently. Despite the jurisdictions' similar definitions of personal data, data protection is not seen as a right, but instead, as a matter of regulation for further purposes such as commercial use and, especially, defense. For instance, the U.S.'s Foreign Intelligence Surveillance Act allows the disclosure of personal data to intelligence services.[5] In this case, data is instrumentally used as a means to enhance security. This lack of uniformity and strictness demonstrates a clear distinction from E.U. policy. This divergence in the conception of data protection can complicate the transfer of data between the EU and the U.S.

2.2. Rigour of regulations

The E.U.'s laws intend to ensure that citizens' data will not be exploited, misused, or processed in violation of their rights when transferred abroad. This is apparent in the institutions and bodies established to make sure adequacy decisions, standard contractual clauses ("SCC"), and binding corporate rules ("BCR") are respected.[6] Adequacy decisions are the method by which the E.U. ensures third countries provide adequate protection for EU citizen's data, binding upon them.. Article 45, paragraph 2 of the General Data Protection Regulation ("GDPR")[7], states that those countries have to consider "the rule of law,

[3] U.S. Chamber of Commerce, 'Transatlantic Data Flows: Moving Data with Confidence' (www.uschamber.com20 September 2021) <https://www.uschamber.com/technology/data-privacy/transatlantic-dataflows>.

[4] European Union, 'Charter of Fundamental Rights of the European Union ' (Official Journal of the European Communities 2000) <https://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[5] U.S. Congress, 'FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act' (Congress.gov2024) <https://www.congress.gov/crs-product/R48592>.

[6] European Commission, 'Data Protection' (commission.europa.eu2024) <https://commission.europa.eu/law/law-topic/data-protection_en>.

[7] Intersoft Consulting, 'Art. 45 GDPR – Transfers on the Basis of an Adequacy Decision' (General Data Protection Regulation (GDPR)2016) <https://gdpr-info.eu/art-45-gdpr/>.

respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral" when treating data coming from the E.U. In 2015, Maximillian Schrems, an Austrian lawyer and activist, initiated the establishment of clearer regulations when he took legal action regarding the improper use of his data when transferred to the U.S. Before the Schrems cases, the U.S., among other countries, did not meet E.U. standards because of its different approach to data protection.

3. The Schrem cases

3.1. From the Safe Harbor Agreement to Schrems I

The first agreement signed between the E.U. and the U.S. on the transfer of data was the Safe Harbour Agreement in 2000, also known as Decision 2000/520/EC.[8] This agreement required U.S. companies that transferred data from the E.U. to follow "adequate requirements" by certifying that they complied with seven privacy principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.[9] The authority responsible for the supervision of compliance with these rules was the U.S. Federal Trade Commission ("FTC"), which derived power from Article 5 of the FTC Act.[10] Consequences for non-compliance included complaints (from citizens), fines, and a block of the data transfer. In 2015, the lawyer and data privacy activist Maximilian Schrems pressed charges against Facebook Ireland Limited on the basis that the transfer of data to the U.S. did not respect EU citizens' rights.[11] The European Court of Justice found the Safe Harbour Agreement to violate Articles 7 and 8 of the European Charter of Human Rights, which regulate the right to privacy and the right to data protection, respectively.[12] Moreover, it infringed the fundamental laws of European data protection. One significant point of contention was that U.S. law allowed broad access to transferred data without specific limits, and E.U. citizens were not given efficient means to defend their rights in case of abuse (paragraphs 95-98 of the ruling). Lastly, the court ruled that the European Commission had not imposed a sufficient procedure to ensure that the U.S. system offered sufficient data protection.[13] This famous ruling, known as Schrems I, started a revolution in international data protection. Since then, the E.U. has adopted stricter enforcement mechanisms, including more rigorous oversight.

3.2. From the Privacy Shield to Schrems II

Because of the necessity of smooth data transfer between the U.S. and the E.U., the actors had to find a

[8] 'Decisión - 2000/520 - EN - EUR-Lex' (Europa.eu2025) <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32000D0520> accessed 13 November 2025.

[9] European Parliament, 'The EU-US Safe Harbour Agreement' (2012) <https://www.europarl.europa.eu/EPRS/120261REV1-EU-US-Safe-Harbour-Agreement-FINAL.pdf> accessed 17 November 2025.

[10] Federal Reserve, 'Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices Background' <https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf>.

[11] For more background on 'Maximilian Schrems' (*Wilson Center*24 June 2021) <https://www.wilsoncenter.org/person/maximilian-schrems> accessed 28 November 2025.

[12] Official Journal of the European Communities 2000 n(4)

[13] 'EUR-Lex - 62014CJ0362 - EN - EUR-Lex' (Europa.eu2015) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62014CJ0362> accessed 13 November 2025.

solution within a limited time. After extensive negotiations over the Safe Harbor Agreement, the jurisdictions reached a consensus, including a new framework that would impose stronger obligations on the U.S. The 'Privacy Shield Framework' was approved in 2016 and implemented by the EU Commission with Decision (EU) 2016/1250 of 12 July 2016.[14] Consequently, the U.S. Department of State regulated U.S. companies through the introduction of the Data Protection Ombudsperson, a new role with the power to investigate complaints and offer effective redress options to citizens when their rights were violated. Moreover, the Ombudsperson was given the power, by Annex III of the Decision, to access information contained in U.S. government records. This ability provided a further check on authorities to ensure they did not acquire personal information illegitimately. However, experts from the E.U. Parliament quickly began pointing out some limits of the Privacy Shield. One of the main criticisms of the Ombudsperson was its *de facto* low level of independence from the government, cited as a concern in paragraph 23 of the Parliament resolution on the adequacy of the framework.[15] Dependency on the government was a key problem for the proper functioning of the organ because it compromised its oversight function. In response, Maximilian Schrems formulated a new complaint on the basis that U.S. surveillance programs, because of their outsized influence, breached data protection.[16] As a result, the Privacy Shield Framework was also deemed invalid by the European Court of Justice, in the sentence known as Schrems II (2020). The ruling established that U.S. national security laws, such as the Foreign Intelligence Surveillance Act 1978 ("FISA") and the Executive Order 12333, gave disproportionate access to EU citizens' data.[17] [18] The problems regarding the Ombudsperson's independence were confirmed by the court, which also decided that the remedies the U.S. provided were not enough.

3.3. Relevance of Schrems cases in current legislation: Data Privacy Framework

Schrem I and Schrem II were pivotal rulings that marked the starting point of a fundamental change in the regulation of data protection. In a world where data is inevitably transferred to countries with different legal cultures, traditional legal frameworks have too many limits. To function in the modern world, jurisdictions cannot solely rely on their own legal traditions and will have to find compromises. In fact, these rulings revealed growing tensions between technological innovation and the

[14] 'Decisión de Ejecución - 2016/1250 - EN - EUR-Lex' (Europa.eu2016) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D1250> accessed 13 November 2025.

[15] Claude MORAES, 'MOTION for a RESOLUTION on the Adequacy of the Protection Afforded by the EU-US Privacy Shield | B8-0235/2017 | European Parliament' (Europa.eu2017) <https://www.europarl.europa.eu/doceo/document/B-8-2017-0235_EN.html> accessed 13 November 2025.

[16] European Parliament, 'The CJEU Judgment in the Schrems II Case' (2020) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf>.

[17] National Security Agency, 'National Security Agency/Central Security Service > Signals Intelligence > FISA' (www.nsa.gov1978) <https://www.nsa.gov/Signals-Intelligence/FISA/>.

[18] National Security Agency, 'National Security Agency/Central Security Service > Signals Intelligence > EO 12333' (www.nsa.gov1981) <https://www.nsa.gov/Signals-Intelligence/EO-12333/>.

protection of data in the digital age. The solution to these tensions must be found through negotiations that try to respect the primary needs of both jurisdictions. The U.S. responded to Schrems II through the Executive Order 14086, signed by Joe Biden on October 7, 2022,[19] a measure which reinforced surveillance of intelligence agencies. Firstly, it recognised that these agencies are necessary for the protection of the country and of its people, and highlighted the need to further develop technology in the field. However, it also aimed to protect individuals and treat them with "dignity and respect" when it comes to their data. One of the main changes brought on by this Executive Order was the introduction of the Data Protection Review Court ("DPRC"), an independent organ with binding powers to manage claims from "non-US persons" who believe their data protection rights have been violated by companies or governmental entities. With the implementation of this new legal framework, the European Commission implemented Decision EU 2023/1795 in 2023.[20] This decision recognised that the U.S. now had an adequate level of data protection under Article 45 of the GDPR regarding data transfer to companies self-registered in the new Data Privacy Framework ("DPF").[21] The DPF was the most recent agreement to regulate data transfer relations from the E.U. to the U.S.[22] It introduced similar measures contained in the Executive Order 14086 to restrain the surveillance power of American intelligence agencies, including the creation of the DPRC, and concluded that the U.S. ensures a level of protection "essentially equivalent" to the one granted to citizens in the EU. [23]

4. Data Protection and developing technologies

The Schrems rulings were merely the starting point for the reframing of data protection between international entities. These decisions serve as the conceptual foundations when facing legal challenges posed by developing technologies, such as AI. The cases discussed in this paper prove that the law is facing a new problem: keeping pace with technological development is impossible. The difficulty of regulating an area in constant development is what will undermine the protection of individuals' information in the next few years. This issue becomes even more relevant as AI technology further develops and proliferates. Personal data and sensitive information are what fuel AI machines and allow them to

[19] The White House, 'Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities | the White House' (The White House7 October 2022) <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>.

[20] 'Izvedbeni Sklep - 2023/1795 - EN - EUR-Lex' (Europa.eu2023) <https://eur-lex.europa.eu/legal-content/SL-EN/ALL/?uri=CELEX:32023D1795&from=SL> accessed 16 November 2025.

[21] Intersoft Consulting, 'Art. 45 GDPR – Transfers on the Basis of an Adequacy Decision' (General Data Protection Regulation (GDPR)2016) <https://gdpr-info.eu/art-45-gdpr/>.

[22] European Parliament and the Council, 'Implementing Decision - 2023/1795 - EN - EUR-Lex' (Europa.eu2023) <https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng>.

[23] The White House n(15)

improve.[24] This exponentially increases privacy risks, posing further legislative problems. First of all, AI is collecting an unprecedented amount of sensitive data (such as healthcare information, facial recognition, and personal finance data) without the consent or knowledge of the people involved. This processing of sensitive data is made more problematic by the fact that it can easily be exposed by hackers, who may manipulate AI using strategic prompts.

4.1. Regulations to contain the risks posed by AI

These new risks increased the existing urgency to create laws and regulations to protect individuals' data and privacy. However, it is difficult to understand how to balance this with technological evolution. AI is having an unimaginable impact on society, and both the U.S. and the E.U. have already addressed this through legislation. The E.U.'s response to technological evolution came with Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, also known as the AI Act.[25] The Act establishes harmonized rules for the development, marketing, and use of AI systems within the E.U. It adopts a risk-based approach, imposing different obligations depending on the potential danger of AI technologies.

The U.S. also implemented a legislative framework to address the issue. On October 30, 2024, President Biden signed Executive Order 14110, regulating AI in the U.S.[26] This order promotes safety, reliability, and accountability in the use of AI, establishing principles on transparency, risk management, and data protection. These regulations intersect with the regulation of personal data transfers, as the data used by AI is often sensitive and far-reaching. Its transatlantic circulation must comply with high standards to avoid risks of privacy violations and ensure compliance with the law. AI reinforces the need for robust, multinational legal frameworks such as the Data Privacy Framework, to ensure that personal data transfers are lawful, secure, and subject to effective controls, preserving both the trust of European citizens and cooperation between the U.S. and E.U.

5. Iure Condendo Expectations:

Data relations between the E.U. and the U.S. are moving towards stability; however, the situation is constantly evolving. The two jurisdictions found a balance that is now being put at stake by technological innovation. Though it seems for now that they are similarly applying limits and checks on the existing AI systems, they still view

[24] Alice Gomstyn and Alexandra Jonker, 'Exploring Privacy Issues in the Age of AI' (IBM30 September 2024) <https://www.ibm.com/think/insights/ai-privacy>.

[25] 'European Parliament P9_TA(2024)0138 Artificial Intelligence Act European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 -C9-0146/2021 -2021/0106(COD)) (Ordinary Legislative Procedure: First Reading)' (2019) <https://artificialintelligenceact.eu/wp-content/uploads/2024/04/TA-9-2024-0138_EN.pdf>.

[26] The White House, 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | the White House' (The White House30 October 2023) <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>.

technology differently. The U.S. sees AI as a driver of innovation and a positive instrument for societal development. This perspective is made apparent by 'America's Action Plan', a framework designed to accelerate innovation and build an American AI infrastructure.[27] In contrast, the E.U. perceives AI more as a threat to the safety of its citizens and a high-risk technology, as shown by the AI Act.[28] It will be necessary to further strengthen safeguards, improve the transparency of surveillance operations, and enhance the ability of data subjects to seek redress. Nevertheless, many experts believe that the law is not going to be able to regulate AI at its current pace. In response, the Future of Life Institute launched an international appeal on October 22, 2025, that, in just a few days, gathered tens of thousands of signatures from scientists, Nobel laureates, and artificial intelligence experts.[29] Experts called for a temporary moratorium on the creation of superintelligence systems until safety, transparency, and controllability can be guaranteed, to avoid an unregulated "technology race." This is an ambitious, but ultimately unrealistic initiative. Firstly, the U.S. government is now interested in developing AI competitively, seeking dominance over other countries that are also working to create their own AI infrastructures.[30] Secondly, AI development cannot realistically be stopped because it is a self-improving technology that can grow using the data it already processes. This means that AI does not need external data anymore, and can develop without exterior actors intervening.

6. Conclusions

Regulation cannot realistically stop technological progress. The only way to face the situation is to foresee the nature of future problems and begin attempting to mitigate them as soon as possible. Issues regarding AI will be similar to those jurisdictions faced in the Schrems cases. The different views of the U.S. and the E.U. on the issue will again be at the centre of the discussion. It will be necessary to consider both perspectives and find a compromise that protects citizens without interfering in the development of new technologies. This involves creating a functioning system of data surveillance to ensure AI will be used correctly. Legislators will also have to collaborate with AI developers, as the most efficient way to regulate the processing of data is to understand the direction technological development will take. Moreover, creating technological solutions that filter the amount of data AI can use will also be important for data protection. As technology continues to develop and use data differently, it will be necessary to strengthen the frameworks set after the Schrems cases by adapting them to AI specifically.

[27] AI Gov, 'AI Action Plan' (Ai.gov2025) <https://www.ai.gov/action-plan>.
[28] European Parliament n(25)
[29] Billy Perrigo and Tharin Pillay, '"Time Is Running Out": New Open Letter Calls for Ban on Superintelligent AI Development' (TIME22 October 2025) <https://time.com/7327409/ai-agi-superintelligent-open-letter/ >.
[30] AI Gov n(27)

Bibliography

AI Gov, 'AI Action Plan' (*Ai.gov*2025) <https://www.ai.gov/action-plan>

'Data Protection Laws | International Toolkit' (*world-toolkit.yale.edu*) <https://world-toolkit.yale.edu/regulated-activity/data-protection-laws>

'Decisión - 2000/520 - EN - EUR-Lex' (*Europa.eu*2025) <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32000D0520> accessed 13 November 2025

'Decisión de Ejecución - 2016/1250 - EN - EUR-Lex' (*Europa.eu*2016) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D1250> accessed 13 November 2025

'EUR-Lex - 62014CJ0362 - EN - EUR-Lex' (*Europa.eu*2015) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62014CJ0362> accessed 13 November 2025

European Commission, 'Data Protection Explained' (*European Commission*2023) <https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en>

'Data Protection' (*commission.europa.eu*2024) <https://commission.europa.eu/law/law-topic/data-protection_en>

European Parliament, 'The EU-US Safe Harbour Agreement' (2012) <https://www.europarl.europa.eu/EPRS/120261REV1-EU-US-Safe-Harbour-Agreement-FINAL.pdf> accessed 17 November 2025

'The CJEU Judgment in the Schrems II Case' (2020) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf>

European Parliament and the Council, 'Implementing Decision - 2023/1795 - EN - EUR-Lex' (*Europa.eu*2023) <https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng>

'European Parliament P9_TA(2024)0138 Artificial Intelligence Act European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 -C9-0146/2021 -2021/0106(COD)) (Ordinary Legislative Procedure: First Reading)' (2019) <https://artificialintelligenceact.eu/wp-content/uploads/2024/04/TA-9-2024-0138_EN.pdf>

European Union, 'Charter of Fundamental Rights of the European Union ' (Official Journal of the European Communities 2000) <https://www.europarl.europa.eu/charter/pdf/text_en.pdf>

Federal Reserve, 'Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices Background' <https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf>

Gomstyn A and Jonker A, 'Exploring Privacy Issues in the Age of AI' (*IBM*30 September 2024) <https://www.ibm.com/think/insights/ai-privacy>

House TW, 'Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities | the White House' (*The White House*7 October 2022) <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-en

hancing-safeguards-for-united-states-signals-intelligence-activities/>

'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | the White House' (*The White House*30 October 2023) <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

Intersoft Consulting, 'Art. 45 GDPR – Transfers on the Basis of an Adequacy Decision' (*General Data Protection Regulation (GDPR)*2016) <https://gdpr-info.eu/art-45-gdpr/>

'Izvedbeni Sklep - 2023/1795 - EN - EUR-Lex' (*Europa.eu*2023) <https://eur-lex.europa.eu/legal-content/SL-EN/ALL/?uri=CELEX:32023D1795&from=SL> accessed 16 November 2025

'Maximilian Schrems' (*Wilson Center*24 June 2021) <https://www.wilsoncenter.org/person/maximilian-schrems> accessed 28 November 2025

MORAES C, 'MOTION for a RESOLUTION on the Adequacy of the Protection Afforded by the EU-US Privacy Shield | B8-0235/2017 | European Parliament' (*Europa.eu*2017) <https://www.europarl.europa.eu/doceo/document/B-8-2017-0235_EN.html> accessed 13 November 2025

National Security Agency, 'National Security Agency/Central Security Service > Signals Intelligence > FISA' (*www.nsa.gov*1978) <https://www.nsa.gov/Signals-Intelligence/FISA/>

'National Security Agency/Central Security Service > Signals Intelligence > EO 12333' (*www.nsa.gov*1981) <https://www.nsa.gov/Signals-Intelligence/EO-12333/>

Perrigo B and Pillay T, '"Time Is Running Out": New Open Letter Calls for Ban on Superintelligent AI Development' (*TIME*22 October 2025) <https://time.com/7327409/ai-agi-superintelligent-open-letter/>

U.S. Chamber of Commerce, 'Transatlantic Data Flows: Moving Data with Confidence' (*www.uschamber.com*20 September 2021) <https://www.uschamber.com/technology/data-privacy/transatlantic-dataflows>

U.S. Congress, 'FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act' (*Congress.gov*2024) <https://www.congress.gov/crs-product/R48592>