PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 1 February 2025

Regulatory Conflict and the Struggle for Digital Sovereignty: A Critical Analysis of the EU-U.S. Data Privacy Framework

Haoyang Qin[1,2]

[1] LL.M., University of Warwick, Coventry CV4 7AL, United Kingdom
[2] Assistant Researcher, China Law Society, Beijing, China
Correspondence: Haoyang Qin, LL.M., University of Warwick, Coventry CV4 7AL, United Kingdom; Assistant Researcher, China Law Society, Beijing, China.

doi:10.56397/SLJ.2025.02.05

Abstract

After the EU-U.S. Privacy Shield was invalidated, both sides introduced the "Data Privacy Framework" in late 2022 to restore cross-border data flow order. In July 2023, the European Commission issued an adequacy decision recognizing U.S. data protection. However, the framework does not curb U.S. intelligence agencies' mass surveillance, and its redress mechanism lacks independence and effectiveness. Substantially, it offers little progress over the Privacy Shield. The EU-U.S. negotiations reflect a deeper clash between the EU's "digital sovereignty" and the U.S.'s "digital hegemony." Their competition for digital governance influence holds key lessons for developing countries in shaping their data regulation strategies.

Keywords: cross-border data flow, data governance, privacy protection, digital security

1. Introduction

Over the past two decades, the rules governing transatlantic data transfers between the United States and the European Union have undergone three major changes. Following the invalidation of the Safe Harbor and Privacy Shield Agreements by the Court of Justice of the European Union due to inadequate protection of EU citizens' data privacy, the EU and U.S. introduced the "Data Privacy Framework" in 2022. This framework includes new U.S. commitments, such as restricting intelligence agencies' access to personal data and creating legal redress mechanisms for EU citizens. However, critics argue these measures fail to resolve the fundamental regulatory conflict between the EU's emphasis on "digital sovereignty" and the U.S.'s "digital hegemony." The EU views data privacy as a fundamental right, while the U.S., shaped by capital markets and post-9/11 priorities, focuses on industrial and national security, leaving data privacy largely to market forces. This article summarizes the framework's progress, evaluates its effectiveness, and explores the root causes of EU-U.S. regulatory conflicts over data privacy.

2. Achievements of the EU-U.S. Data Privacy Framework

2.1 Executive Order 14086: Limiting Intelligence

Collection Activities

To implement U.S. commitments under the "Data Privacy Framework," President Biden signed Executive Order 14086 in October 2022. The order imposed strict limits on U.S. intelligence agencies' signal intelligence activities, highlighting the need to respect individuals' legitimate privacy interests when processing personal data.

Intelligence activities should adhere to the principles of necessity and proportionality. Such activities must be based on comprehensive and reasonable assessments to ensure they are conducted only when necessary and in a manner that aligns with "validated intelligence priorities," thus avoiding excessive infringements on individual privacy. Additionally, intelligence collection should prioritize targeted methods over bulk data collection. Bulk collection of personal information should be restricted to six specific objectives, including the prevention of terrorism, espionage, cybersecurity threats, and other narrowly defined goals. [1] When intelligence agencies handle the personal data they have collected, they must follow specific legal requirements and procedures regarding data security, access restrictions, and related safeguards.[2]

The "Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" significantly strengthens the protection of personal data privacy in U.S. signals intelligence operations, effectively reducing the likelihood of foreign citizens being subjected to unlawful surveillance by U.S. intelligence agencies. Notably, the establishment of twelve legitimate objectives not only imposes constraints on previously unregulated surveillance activities of U.S. intelligence agencies but also narrows the interpretation of "foreign intelligence" under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA). This represents a substantial advancement in the United States' efforts to protect the privacy of foreign citizens.

2.2 Two-Layer Legal Redress Mechanism in the U.S.

The third section of the "Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" establishes a two-layer redress mechanism to address complaints from foreign citizens whose rights have been infringed upon due to misconduct by U.S. intelligence agencies.

The first layer of the redress mechanism involves the Civil Liberties Protection Officer (CLPO) within the Office of the Director of National Intelligence (ODNI). This officer will investigate the complaint and take appropriate remedial measures if necessary. The second layer is the Data Protection Review Court (DPRC), established by the U.S. Department of Justice in accordance with the Executive Order. To ensure impartiality, the Attorney General is required to appoint at least six judges and two special advocates based on specific selection criteria.[3] Both the complainant and intelligence agency personnel may request a review of the CLPO's decision by the DPRC. Typically, a panel of three judges will conduct the review, with a special advocate appointed to represent the complainant's interests.[4] During the review, the court will consider the CLPO's investigative record as well as briefs submitted by the complainant, the special advocate, and the intelligence agency. The court's decisions must adhere to relevant U.S. Supreme Court precedents. Finally, the CLPO is responsible for enforcing the court's rulings.

The Executive Order enhances the independence of the first-layer redress mechanism by clearly defining the responsibilities of the Director of National Intelligence and limiting the grounds for removing the CLPO. Furthermore, by explicitly outlining the standards for the selection, appointment, and removal of judges for the DPRC, the order reduces the Attorney General's influence over the second-layer redress mechanism, thereby further ensuring its independence. [5] In this regard, the new two-layer redress mechanism represents a significant improvement over the previous Privacy Shield Ombudsperson system.

3. Controversies in the EU-U.S. Data Privacy Framework

3.1 Adequacy Decision by the European Commission

According to Article 45(1) of the EU GDPR, the European Commission must conduct a comprehensive assessment of the laws of a third country (or region) before making an adequacy

[1] The White House Sec.2(c)(ii)(B).

[2] Ibid, (n 44) Sec.2(c)(iii).

[3] Ibid, (n 44) Sec.3(d)(i)(A).

[4] Ibid, Sec.3(d)(i)(B) and Sec.3(d)(i)(C).

[5] The White House Sec.3(d)(iv).

decision.[1] In its adequacy decision regarding the United States, the European Commission explicitly stated that the "Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" provided the foundation for its adequacy decision. The Commission examined the principles of the EU-U.S. "Data Privacy Framework," the commitments and certification obligations of U.S. companies that join the framework, as well as the U.S. Department of Commerce's responsibilities for managing and enforcing the framework. The Commission concluded that the U.S. legal system, on the whole, ensures the effective implementation of these principles.[2]

The U.S. oversight and redress mechanisms are deemed sufficient to ensure that violations of data protection rules can be promptly detected and penalized in practice, and that data subjects are provided with legal remedies for accessing, correcting, and deleting their personal data. Furthermore, the Executive Order has significantly restricted U.S. intelligence agencies' ability to infringe upon the data privacy of EU citizens under the guise of national security or other public interests, confining such actions strictly to what is necessary to achieve legitimate objectives. The Order also provides effective legal protections for EU citizens against such infringements.[3]

In summary, the European Commission determined that the level of data protection in the United States has been elevated to a degree that is "essentially equivalent" to the standards of the GDPR. Consequently, the Commission decided to allow the transfer of personal data from the EU to the U.S. under the GDPR's Article 45, via the EU-U.S. Data Privacy Framework, without the need for additional authorization.

3.2 Substantive Reforms Needed in U.S. Intelligence Laws

Although the EU has adopted an adequacy decision regarding the United States, there are still legal provisions within the U.S. signals intelligence legal framework that conflict with the protection of foreign individuals' privacy data. The most notable among these are Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, titled "United States Intelligence Activities."

Section 702 of FISA allows intelligence agencies to conduct broad surveillance on any citizen of any country around the world, providing the legal basis for U.S. programs such as PRISM and UPSTREAM.[4] Executive Order 12333, on the other hand, authorizes the National Security Agency (NSA) to conduct more intrusive collection targeting non-U.S. citizens located abroad.[5] It is important to note that the "Data Privacy Framework" does not amend or impose substantive limitations on these two critical legal provisions. Instead, the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities largely replaces Presidential Policy Directive 28, some provisions of which have been rescinded.[6] Furthermore, the directive was criticized by the EU Court for being overly general in its limitations on U.S. intelligence activities, a criticism that similarly applies to the new executive order.

Firstly, the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities specifies 12 legitimate objectives. While these objectives ostensibly limit the implementation of intelligence activities, they may not effectively restrict the scope and results of surveillance in practice. In some cases, defining specific objectives does not necessarily narrow the scope of surveillance and data

[1] GDPR. (n.d.). Article 45 GDPR: Transfers on the Basis of an Adequacy Decision. GDPR-Info.eu. https://gdpr-info.eu/art-45-gdpr/ accessed 23 August 2024.

[2] European Commission. (2023). Adequacy Decision EU-US Data Privacy Framework. https://commission.europa.eu/document/download/fa09cbad-dd7d4684ae60be03fcb0fddf_enfilename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf accessed 23 August 2024, 3(7).

[3] European Commission. (2023). Commission Implementing Decision of 10.7.2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework. European Commission. https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf accessed 21 August 2024.

[4] Laura K Donohue. (2021). The Evolution and Jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. *Harv Nat'l Sec J, 12*, 198, 205.

[5] US Department of Defense. (2008). Executive Order 12333: United States Intelligence Activities. https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf accessed 24 August 2024, part 2 2.2 and 2.4.

[6] Hendrik Mildebrath. (2022). Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086. *European Parliamentary*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf accessed 24 August 2024, endnote 6.

collection. For example, one legitimate objective is "protecting against cybersecurity threats,"[1] which involves a wide range of activities. This broad goal could theoretically justify continuous monitoring of everyone's internet activities. Additionally, there are numerous detailed issues with the setting of these legitimate objectives. For instance, the executive order allows intelligence agencies to conduct surveillance for "protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person."[2] Common sense suggests that minor vandalism or petty crimes should not fall under this category, but the objective itself lacks a clear standard for severity. More worryingly, the executive order stipulates that the President can authorize updates to the list of legitimate objectives. If public disclosure of the updated list poses a national security risk, the President can choose to modify it secretly.[3] This provision effectively renders the limitation on legitimate objectives meaningless. If the content of the objective list lacks certainty and transparency, its constraints and regulations on intelligence activities are even more untenable.

Secondly, the principles of necessity and proportionality, which should guide the implementation of signals intelligence activities, are highly subjective and open to broad interpretation.[4] In practice, U.S. intelligence agencies can use any broad area related to national security, such as cyber threats or global terrorism, as a justification for the "necessity" of intelligence collection. This arbitrary interpretation renders the safeguards outlined in EO 14086 almost ineffective. Specifically, in the PRISM and Upstream programs, the NSA widely collected electronic communications from target groups, including both non-U.S. persons and U.S. citizens, which is clearly excessive. However, in theory, the NSA could still claim that it adheres to the principles of "necessity" and "proportionality" by interpreting "necessity" as collecting all possible intelligence to prevent potential threats and "proportionality" as ensuring that intelligence collection aligns with the goal of protecting national security, all of which are fully authorized by law. This means that even without a specific, real threat, the NSA can consider any action "necessary and proportionate" as long as it is possible to obtain valuable intelligence data.

In summary, the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities effectively accommodates bulk data collection. The necessity standard of the executive order mainly considers the requirements of legitimate objectives and applies to all forms of surveillance without imposing further restrictions on high-risk forms of bulk data collection. The executive order attempts to mitigate privacy violations by regulating the post-collection querying, use, dissemination, and retention of data. However, this back-end data privacy protection approach is minimally effective.[5] Intelligence collection activities under the Executive Order on United States Intelligence Activities are not subject to judicial oversight and adjudication, which likely exacerbates compliance issues. Bulk data collection inevitably leads to the collection of private communications or other data unrelated to achieving legitimate objectives, a form of arbitrary surveillance condemned by the EU Court as violating the essence of privacy rights. "In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[6]

3.3 Lack of Independence in the New Two-Layer Redress Mechanism

Although the Data Privacy Framework's two-layer redress mechanism represents an improvement over the status quo, it is still viewed as an upgraded version of the Privacy

[1] The White House (n 44) Sec.2(b)(i)(A)(8).

[2] Ibid, (n 44) Sec.2(b)(i)(A)(10).

[3] Ibid, Sec.2(b)(i)(B).

[4] Elizabeth Goitein. (2022). The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance. *Just Security*. https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/ accessed 24 August 2024.

[5] Elizabeth Goitein. (2019). The FISA Court's Section 702 Opinions, Part II: Improper Queries and Echoes of Bulk Collection. *Just Security*. https://www.justsecurity.org/66605/the-fisa-courts-section-702-opinions-part-ii-improper-queries-and-echoes-of-bulk-collection/ accessed 24 August 2024.

[6] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362 accessed 24 August 2024, para 94.

Shield ombudsman system, which was invalidated by the EU Court of Justice (CJEU) in the Schrems II case. The new redress mechanism fails to meet the standards set by Article 47 of the EU Charter of Fundamental Rights due to its lack of independence. In a 2018 ruling, the CJEU offered a clear interpretation of judicial "independence," stating that "the body concerned exercises its judicial functions wholly autonomously, without being subject to any hierarchical constraint or subordinated to any other body and without taking orders or instructions from any source whatsoever, and that it is thus protected against external interventions or pressure liable to impair the independent judgment of its members and to influence their decisions." [1] And the CJEU further emphasized that judicial independence is a fundamental requirement for providing effective judicial protection.[2] Despite measures by the Biden administration to ensure the independence of the redress mechanism, it remains part of the U.S. executive branch. The first layer, the Civil Liberties Protection Officer (CLPO), is part of the Office of the Director of National Intelligence. The second layer, the Data Protection Review Court (DPRC), is part of the Department of Justice. Both layers are essentially branches of the U.S. executive. Furthermore, the CLPO must "appropriately respect any relevant determinations made by national security officials."[3] For the DPRC, factual investigations are conducted by the Office of the Director of National Intelligence, not the court itself. Judges are selected and appointed by the Attorney General, not by a third party independent of the intelligence community, and the President has the authority to overturn the court's decisions.

These structural dependencies indicate that the DPRC does not operate with the complete autonomy required by the CJEU and is not free from hierarchical constraints. The CJEU has stressed that judges must be protected from external interventions or pressures that could impair their independent judgment and influence their decisions. It highlighted that the rules regarding judges' terms of office and dismissal must eliminate any reasonable doubts about the court's impartiality and independence.[4] However, the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities and its accompanying laws do not limit the President's power to dismiss judges. The renewal of judges' terms after their four-year tenure also depends on the executive branch. These conditions contradict the CJEU's principles of safeguarding judicial independence and autonomy, potentially leading to biased decisions.

3.4 General Assessment of the Framework

Although the European Commission has endorsed the U.S. data privacy protection status, opinions on it are mixed. The ACLU even suggest that the U.S. Congress should fundamentally reform its intelligence legal framework to meet the EU's "essential equivalence" requirements.[5] Christopher Kuner points out that the EU hopes to achieve the goal of protecting data and privacy rights in U.S. legal practice through procedural mechanisms such as the Privacy Shield Agreement, other adequacy decisions, or standard contractual clauses. He considers this an unrealistic expectation because these mechanisms cannot provide adequate protection to against U.S. intelligence collection activities and government surveillance. [6] However, considering the enormous economic benefits of reestablishing the transatlantic data transfers, such as reducing compliance costs for businesses, lowering potential risks of data transfers to the U.S., and creating a more stable business environment, some industry associations like Digital Europe and the Information Technology Industry Council highly commend the adequacy

[1] Case C-507/17 Google LLC v CNIL [2019] ECLI:EU:C:2019:772, https://curia.europa.eu/juris/document/document.jsf?docid=215341&doclang=EN accessed 24 August 2024, para 108.

[2] Theodore Konstadinides. (2019). Judicial Independence and the Rule of Law in the Context of Non-Execution of a European Arrest Warrant: LM. *Common Market Law Review, 56*(3), 743, 750.

[3] The White House (n 44) Sec.3(c)(i)(B)(ii).

[4] Case C-746/18 H.K. v Prokuratuur [2021] ECLI:EU:C:2021:153, https://curia.europa.eu/juris/document/document.jsf?text=&docid=238382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2091303 accessed 25 August 2024, para 123.

[5] ACLU. (2022). New Biden Executive Order on EU-US Data Transfers Fails to Adequately Protect Privacy. https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy accessed 25 August 2024, para 7.

[6] Christopher Kuner. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal, 18*(4), 881-918.

decision.[1]

The EU and the U.S. have different positions on cross-border data flows, making it challenging to find a suitable solution. As international digital trade continues to thrive, it can be anticipated that competition and compromise in this field will persist. Although the U.S. has not fundamentally reformed its signals intelligence legal framework in the latest Data Privacy Framework and the newly created two-layer redress mechanism has obvious independence issues, the U.S. has already made several significant concessions in this negotiation. Further negotiations to weaken its national security laws would not align with U.S. interests.[2] Some scholars believe that "the Biden administration has gone as far as it can go within the constraints of American law."[3] This is because requiring the U.S. to substantively reform its signals intelligence legal framework to more effectively limit the collection and use of signals intelligence, or enacting corresponding laws that would allow EU citizens to sue U.S. intelligence agencies in federal courts for improper surveillance, would lead to an imbalance in rights between EU citizens and U.S. citizens, as "American data was seemingly unprotected from use by European intelligence agencies."[4]

Although the current U.S. data privacy protection level may still fall short of EU expectations, considering the crucial importance of efficient cross-border data flows to the transatlantic digital economy relationship, the European Commission has still adopted the adequacy decision regarding the U.S. data protection level. This decision injects new vitality into transatlantic digital trade.

4. Underlying Causes of EU-U.S. Data Regulation Conflict

The negotiations between the EU and the U.S. over the "Data Privacy Framework" ostensibly represent a clash between two different data protection philosophies and governance models. However, at a deeper level, they reflect the EU's awakened sense of "digital sovereignty," its desire to break free from U.S. digital technology hegemony, and its strong wish to achieve true independence. Although the EU's efforts to assert its digital sovereignty have already "faced obvious challenges"[5], the conflict over cross-border data flow rules still mainly comes from the EU's goal of achieving "digital sovereignty" clashing with the U.S.'s desire to maintain its "digital hegemony." This struggle involves both sides using their strengths to compete for control over global digital governance in the era of the digital economy.

4.1 Divergent Views on Data Privacy Rights

Under EU law, "contract and consent" are the legal basis for data processing. However, the EU goes further by placing some data protection interests beyond individual control, using a collective approach that limits the use of "contract and consent."[6] Contracts must follow the principles of necessity and purpose limitation, and the consent model is also strictly regulated. Both constitutional and statutory laws support the idea of "inalienable data privacy," which restricts individuals' ability to manage their data and sets limits where neither contracts nor consent can override rights. Core data protection rules prevent individuals from selling or exchanging their data, establishing protections that cannot be waived or traded. For example, Article 8 of the Charter stipulates that "the processing of personal data must have a legitimate legal basis" and sets out a series of data processing principles. Legislation establishes clear and definitive measures to ensure that personal data interests are "essentially" protected, fundamentally preventing individuals from harming their own interests through choices such as "no privacy authorization, no service." Data subjects cannot

[1] European Parliamentary. (2022). EU-US Data Privacy Framework: Review of Recent Developments and Future Challenges. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf accessed 25 August 2024, 5-6.

[2] Oliver Patel and N Lea. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. UCL European Institute. https://ssrn.com/abstract=3618937 accessed 25 August 2024, 15.

[3] Paul Rosenzweig. (2022). The "Three Rs" of President Biden's Trans-Atlantic Privacy Outreach. Lawfare. https://www.lawfaremedia.org/article/three-rs-president-bidens-trans-atlantic-privacy-outreach accessed 25 August 2024, para 20.

[4] Ibid, para 21.

[5] Lilit Vardanyan and Hayk Kocharyan. (2022). Critical Views on the Phenomenon of EU Digital Sovereignty through the Prism of Global Data Governance Reality: Main Obstacles and Challenges. *European Studies, 9*(2) 110-132, 129.

[6] Paul M Schwartz and Karl-Nikolaus Peifer. (2017). Transatlantic Data Privacy Law. *Georgetown Law Journal*. https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf accessed 25 August 2024, 139.

agree to sell the basic rights, privacy, and fundamental interests protected by the Charter. The EU views this approach as protecting democratic self-determination, preventing individuals from becoming targets for data processors by selling their personal rights. GDPR, based on the Charter and EU legal tradition, continues to create a set of "non-waivable safeguards."

In the United States, individuals are situated within specific market relationships, such as being an individual seeking a credit card under FCRA protection, participating in financial transactions under GLBA protection, or watching videos under VPPA protection. Thus, US information privacy laws protect individual privacy rights within specific market environments and special consumer relationships. In contrast, strong constitutional protections in the US do not target individuals whose data is at risk but protect data processors. This tendency has a long history, starting from the Clinton administration's push for internet commercialization, where the primary focus was creating a regulatory environment to foster economic growth and industry self-regulation. During the Obama administration, the emphasis remained on supporting suppliers, aiming to build global leadership in consumer data privacy while promoting innovation and consumer trust. Under the Trump administration, the US and EU diverged further in privacy matters.[1] In the intense competition between individuals and data processors, US information privacy law almost exclusively considers the data processors' perspective. In the US, data processing does not need to be based on individual "consent," and statutory law adopts "opt-in" or "opt-out" consent mechanisms.[2] Daniel Solove argues that the US "privacy self-management" mechanism has structural issues. While consent is a necessary component of any regulatory regime, the tasks it requires are beyond individual capacity. Even if individuals are timely informed and deemed rational, structural issues prevent them from adequately protecting their privacy.[3]

From the EU perspective, U.S. privacy law relies on vague fair competition rules and has structural defects. [4] The American understanding of basic rights in the digital age has not evolved beyond the 1970s.[5] The basic data protection rights should not be left to the market. From the U.S. perspective, the EU's data protection is seen as trade protectionism or a way to seize commercial interests from U.S. internet companies. The U.S. believes its rules better promote the development and innovation of technology companies. The differences in rules reflect divergent definitions of personal privacy data: the EU sees personal privacy data as a human right that should be constitutionally protected, while the U.S. tends to treat personal privacy data as a conceptual commodity that should flow freely and be regulated by the market.

4.2 Digital Sovereignty vs. Digital Hegemony: The Rise of Surveillance Capitalism

The rise of U.S. internet giants is closely tied to "surveillance capitalism." [6] "Surveillance capitalism refers to new economic conditions in which online information (data) is converted into valuable commodities, and where the capture and production of these commodities (data) rely on mass surveillance over the Internet." [7] This data collection and commercialization have become the default business model for global digital enterprises. "The World's Most Valuable Resource Is No Longer Oil, but Data" [8] Personal data from communications, web browsing, shopping records, online payments, movement patterns, and even sleep quality is constantly fed back to

[1] Paul M Schwartz and Karl-Nikolaus Peifer. (2017). Transatlantic Data Privacy Law. *Georgetown Law Journal*. https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf accessed 25 August 2024, 138.

[2] Ibid, 152.

[3] Daniel J Solove. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harv L Rev*, *126*, 1880-1882.

[4] Alexander Börding. (2016). Ein neues Datenschutzschild für Europa. *Computer und Recht*, *32*(7), 431, 434.

[5] Thilo Weichert. (2014). Globaler Kampf um digitale Grundrechte. *Kritische Justiz*, *47*(2), 123, 127.

[6] Shoshana Zuboff. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs.

[7] Donell Holloway. (2019). Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children. *Media International Australia, 170*(1). https://doi.org/10.1177/1329878X19828205 accessed 26 August 2024, 27.

[8] The Economist. (2017). The World's Most Valuable Resource Is No Longer Oil, but Data. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data accessed 25 August 2024.

internet tech platforms. By collecting, storing, deeply mining, and analysing this massive data in real-time, companies can more accurately target potential consumers and develop products and services that better meet consumer needs, enhancing advertising and expanding reproduction. Extensive data collection forms the basis for advancements in big data analytics, machine learning, and artificial intelligence development. Overregulation could hinder technological progress and lead to the contraction of related industries. Fundamentally, the EU's strict personal data rights protection regime is at odds with the requirements of surveillance capitalism.

Currently, U.S. digital tech giants, leveraging their technological advantages, hold a monopoly position in the global digital value chain, lacking both strong competition and effective regulation, and are likely to "abuse their dominant position against potential rivals." [1] The large-scale surveillance activities in the U.S. are closely linked to the monopoly status of its internet giants. Although these activities are nominally aimed at maintaining national security, the intelligence data gathered can be converted into advantages in technology, economy, politics, and even military competition. The U.S. CLOUD Act established the "data controller standard"[2], extending the enforcement authority of the U.S. government to data stored abroad by American companies, providing legal protection for further expanding competitive advantages. [3] Currently, data worldwide is increasingly concentrating in the hands of U.S. digital tech giants, further squeezing the survival space of internet and digital enterprises in other countries and potentially threatening national security and independence.[4]

At the same time, the United States has leveraged its early advantages in internet and communication technologies and its rich talent pool to cultivate four major tech giants: Google, Microsoft, Facebook, and Amazon. These companies have established industry standards in the global digital field and captured substantial market shares. As digital competition between nations becomes increasingly politicized, the U.S. has employed various economic and political strategies to hinder the development of digital information technology in other countries, thereby establishing "digital hegemony" on a global scale. This hegemony gives the U.S. advantages in international economic activities and has made it easier to extract wealth in a more efficient and hidden way.

Although the EU boasts a developed manufacturing sector and advanced scientific and technological capabilities, it lacks large-scale internet technology companies. This has hindered the ability of the EU's domestic digital technology industry to fully process the vast volume of data generated within the EU, leaving it unable to compete effectively with American tech giants. The direct result is that the EU's share in the global digital economy does not align with its overall economic strength. However, the EU's data privacy protection rules and its regulatory model's method of export continue to have a unique and significant influence on international regulation. [5] Consequently, the EU has sought to leverage its robust data privacy protection framework to assert leadership in international digital governance, thereby carving out space to pursue its "digital sovereignty" strategy, which centres on enhancing technological autonomy.

To curb the unchecked expansion of American digital tech giants within its borders and to foster a growth environment for domestic internet technology firms, the EU has implemented a range of measures and enacted several data-related laws. In addition to introducing a digital services tax aimed at retaining in Europe some of the digital profits extracted by American tech giants, the EU

[1] Jean Tirole. (2023). Competition and the Industrial Challenge for the Digital Age. *Annual Review of Economics, 15*. <https://doi.org/10.1146/annurev-economics-090622-024222> accessed 26 August 2024, 573, 574.

[2] Anbound. (2018). U.S. established rules for data controller standard. http://www.anbound.com/Section/ArticleView_3691_1.htm accessed 26 August 2024.

[3] Eleni Kyriakides. (2019). The CLOUD Act, E-Evidence, and Individual Rights. *European Data Protection Law Review, 5*, 99, 101.

[4] Li Sheng. (2022). Big Tech and the Nation-State. *Big Tech Firms and International Relations*. Contributions to International Relations, Springer, Singapore. Chapter 1.1.2 https://doi.org/10.1007/978-981-19-3682-1_1 accessed 26 August 2024.

[5] Anu Bradford. (2019). The Brussels Effect in Context. *The Brussels Effect: How the European Union Rules the World*. New York, 2020; online edn, Oxford Academic, 19 December https://0-doi-org.pugwash.lib.warwick.ac.uk/10.1093/oso/9780190088583.003.0004 accessed 25 August 2024, 68.

passed the Data Governance Act, the Digital Markets Act,[1] and the Digital Services Act.[2] Following these, the EU further refined the Data Governance Act, amending it to become the Data Act.[3]

The Digital Markets Act primarily targets unfair competition practices by large internet companies that abuse their market dominance. It imposes specific positive and negative obligations on these companies, with strict penalties for non-compliance. Beyond general penalties such as fines, the Act permits the imposition of structural remedies on violators, such as mandating the divestiture of certain business units. Given that the EU identifies most large internet companies as American, this Act is also seen as an additional obligation list specifically aimed at foreign tech giants.[4] The Digital Services Act emphasizes the responsibility of internet platforms to regulate their content and requires platforms to disclose their content recommendation algorithms to European regulatory authorities, thereby enhancing the EU's ability to control content autonomously. The Data Act is designed to foster the growth of EU-based internet technology companies according to EU rules and values, stimulating the dynamism of the EU's digital economy.

In summary, the EU is attempting to create a favourable development environment for domestic internet technology companies through various policy tools, helping local businesses to compete with foreign digital tech giants and thereby asserting control over digital technological sovereignty. This effort also aims to reduce the dependency of EU member states on foreign tech companies. At the same time, the EU is committed to expanding its digital economy market and refining data governance rules, using the dual strategies of market scale and regulatory modelling to enhance its influence in the global arena of privacy data transfers.

Faced with the EU's regulatory challenges, the U.S. leverages its digital technology advantages and the international monopoly position of its tech giants to promote relevant international standards and rules. The U.S. has also accelerated the process of comprehensive domestic data privacy legislation. In June 2022, both chambers of the U.S. Congress have jointly released the draft of the "American Data Privacy and Protection Act" (ADPPA), making it the first attempt to propose such legislation at the federal level instead of on a state-by-state basis.[5]

4.3 Competing for Global Digital Governance

Both the EU and the U.S. are striving to promote their respective data governance philosophies and models as global standards, each aiming to build alliances that align with their own interests. The EU leverages the size of its data market and its advanced regulatory frameworks, while the U.S. relies on its traditional international hegemonic position. Both major global data market players are continuously seeking to strengthen their influence in global digital governance.

The EU, capitalizing on its early lead in data privacy legislation, uses its comprehensive legal framework and stringent regulation to attract other countries to adopt similar standards when crafting their own data protection laws.[6] Specifically, on one hand, the EU has unified the standards for data transfers among its member states through the GDPR, creating an integrated data market within the EU. On the other hand, it has established a whitelist for the free flow of data across borders based on the "adequacy" mechanism under the GDPR, which allows it to attract more countries to join this whitelist by leveraging the EU's large data market. To expand digital trade and economic cooperation with the EU, some countries have even raised their own data protection standards by using the

[1] European Commission. (n.d.). Digital Markets Act. https://digital-markets-act.ec.europa.eu/index_en accessed 26 August 2024.

[2] European Commission. (n.d.). Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en accessed 26 August 2024.

[3] European Commission. (n.d.). Data Act. https://digital-strategy.ec.europa.eu/en/policies/data-act accessed 26 August 2024.

[4] Andrea Willige. (2023). What is the EU Digital Markets Act and How Will It Impact Big Tech?. *World Economic Forum*. https://www.weforum.org/agenda/2023/09/eu-digital-markets-act-big-tech/ accessed 25 August 2024.

[5] Lauren A Di Lella. (2023). Accept All Cookies: Opting-in to a Comprehensive Federal Data Privacy Framework and Opting-out of a Disparate State Regulatory Regime. *Vill L Rev, 68*, 511, 515.

[6] Anu Bradford. (2020). The Brussels Effect in Context. *The Brussels Effect: How the European Union Rules the World*. New York, online edn, Oxford Academic. https://0-doi-org.pugwash.lib.warwick.ac.uk/10.1093/oso/9780190088583.003.0004 accessed 25 August 2024, 31.

EU's framework as a reference.[1]

The United States, meanwhile, primarily utilizes its dominance in digital technology to reinforce its control over international rules through multilateral and bilateral agreements. Firstly, the U.S. has promoted the concept of completely free cross-border data flows. "Specifically, US-led trade agreements generally focus on two issues: the emphasis is on the freedom of choice of individuals (consumers) in digital products and services and the restriction of the state's control over the flows of data."[2] Additionally, the U.S. expanded its influence in the Asia-Pacific region's data transfer domain through the CBPR System established under APEC. The U.S. seeks to globally advance a legally binding framework for cross-border data flows that aligns with American principles, aiming to secure a systemic competitive edge and maintain technological hegemony.

5. Conclusion

From the Safe Harbor Agreement to the Privacy Shield Agreement and the 2022 Data Privacy Framework, the EU and the U.S. have engaged in numerous rounds of negotiations over their cross-border data flow arrangements for more than two decades. The invalidation of the Privacy Shield Agreement essentially represents the EU's counteraction against the U.S. by leveraging its data privacy regulatory discourse power under its "digital sovereignty" strategy. The Data Privacy Framework, on the other hand, reflects the EU's compromise, Data Privacy Framework was still approved despite the fact that the improvements made by the United States have not fully met the European privacy protection standards. The changes in policies and laws regarding transatlantic data transfers between Europe and the United States illustrate that coordinating different data privacy protection regimes is not merely a legal or technical issue, but rather reflects the challenge of balancing national security, economic needs, and the protection of individual privacy rights. The global political landscape must find ways to engage in mutually respectful, cooperative, and inclusive competition within the digital network space. Promoting global digital technological advancements and maintaining order in digital spaces through multilateral efforts are new challenges facing global digital governance.

[1] Ius Laboris. (2019). The Impact of the GDPR Outside the EU. https://iuslaboris.com/insights/the-impact-of-the-gdpr-outside-the-eu/ accessed 26 August 2024.

[2] Yueh C. Chin and J Zhao. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws, 11*(4), 63, 66. https://doi.org/10.3390/laws11040063.

References

Books

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

Journal Articles

Aaronson, S. (2015). Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security. *World Trade Review*, *1*.

Ahmed, U., & Chander, A. (2015). Information goes global: Protecting privacy, security, and the new economy in a world of cross-border data flows. *The E15 Initiative, International Centre for Trade and Sustainable Development.*

Bamberger, K. A., & Mulligan, D. K. (2013). Privacy in Europe: Initial data on governance choices and corporate practices. *George Washington Law Review, 81*, 1529-1530.

Barrett, L. (2019). Confiding in con men: US privacy law, the GDPR, and information fiduciaries. *Seattle University Law Review, 42*(3), 1057-1058.

Bignami, F., & Resta, G. (2015). Transatlantic privacy regulation: Conflict and cooperation. *Law and Contemporary Problems, 78*(4), 231.

Boyne, S. M. (2018). Data protection in the United States. *American Journal of Comparative Law, 66*(Suppl.), 343.

Bruin, R. de. (2022). A comparative analysis of the EU and US data privacy regimes and the potential for convergence. *Hastings Science & Technology Law Journal, 13*, 127-166, 152.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law, 26*(3), 213.

Callo-Müller, M. V. (2018). GDPR and CBPR: Reconciling personal data protection and trade. *APEC Policy Support Unit Policy Brief, 23*, 8.

Carolan, E., & Castillo-Mayen, M. R. (2015). Why more user control does not mean more user privacy: An empirical (and counter-intuitive) assessment of European e-privacy laws. *Virginia Journal of Law & Technology, 19*(2), 325-326.

Chander, A., & Le, U. P. (2015). Data nationalism. *Emory Law Journal, 64*, 677.

Chin, Y. C., & Zhao, J. (2022). Governing cross-border data flows: International trade agreements and their limits. *Laws, 11*(4), 63-66. https://doi.org/10.3390/laws11040063

Cole, D., & Fabbrini, F. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. *International Journal of Constitutional Law, 14*(1), 236.

Fabbrini, F. (2015). Human rights in the digital age: The European Court of Justice ruling in the data retention case and its lessons for privacy and surveillance in the United States. *Harvard Human Rights Journal, 28*, 65-66.

Goitein, E. (2019). The FISA court's Section 702 opinions, Part II: Improper queries and echoes of bulk collection. *Just Security.* https://www.justsecurity.org/66605/the-fisa-courts-section-702-opinions-part-ii-improper-queries-and-echoes-of-bulk-collection/ accessed 24 August 2024.

Goitein, E. (2022). The Biden administration's SIGINT executive order, Part I: New rules leave door open to bulk surveillance. *Just Security.* https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/ accessed 24 August 2024.

Hatfield, P. T. (2015). The great divide: Recent trends could help bridge the US/EU data privacy gap. *Seattle Journal for Social Justice, 14*(1), 307-308.

Hoang, C. (2012). In the middle: Creating a middle road between US and EU data protection policies. *Journal of the National Association of Administrative Law Judiciary, 32*(2), 854.

Jamison, S. G. (2019). Creating a national data privacy law for the United States. *Cybaris Intellectual Property Law Review, 10*(1), 40.

Joel, A. (2023). Necessity, proportionality, and Executive Order 14086. *Joint PIJIP/TLS Research Paper Series, American University Washington College of Law, 12.*

Kuner, C. (2011). Regulation of transborder data flows under data protection and privacy law: Past, present, and future. *OECD Digital Economy Papers, 187*, 39.

Kuner, C. (2017). Reality and illusion in EU data transfer regulation post-Schrems. *German Law Journal, 18*(4), 881-918.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: The US-EU Safe Harbor compromise. *Journal of European Public Policy, 9*(3), 325-344.

Mildebrath, H. (2022). Reaching the EU-US data privacy framework: First reactions to Executive Order 14086. *European Parliamentary*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf accessed 24 August 2024, endnote 6.

Mitchell, A. D., & Mishra, N. (2018). Data at the docks: Modernizing international trade law for the digital economy. *Vanderbilt Journal of Entertainment and Technology Law*, *20*(4), 79.

Pardau, S. L. (2018). The California Consumer Privacy Act: Towards a European-style privacy regime in the United States. *Journal of Technology Law & Policy, 23*(1), 114.

Patel, O., & Lea, N. (2020). EU-US privacy shield, Brexit, and the future of transatlantic data flows. *UCL European Institute*. Retrieved from https://ssrn.com/abstract=3618937 accessed 25 August 2024, 15.

Pendaroska, L. (2022). International transfer of personal data between the EU and countries outside the EU. *Iustinianus Primus Law Review, 13*, 5.

Roth, P. (2017). Adequate level of data protection in third countries post-Schrems and under the General Data Protection Regulation. *Journal of Law, Information & Science, 25*(1), 49.

Rubinstein, I. S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal, 28*(2), 1333-1414.

Schwartz, P. M. (2019). Global data privacy: The EU way. *New York University Law Review,*

94(4), 771.

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. *Georgetown Law Journal, 106*(1), 115.

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*, 1880-1882.

Soma, J. T., Rynerson, S. D., & Beall-Eder, B. D. (2004). An analysis of the use of bilateral agreements between transnational trading groups: The US/EU e-commerce privacy safe harbor. *Texas International Law Journal, 39*, 171-214, 203.

Svantesson, D. J. B. (2010). A legal method for solving issues of internet regulation: Applied to the regulation of cross-border privacy issues. *European University Press Working Paper, 1.*

Svantesson, D. J. B. (2011). The regulation of cross-border data flows. *International Data Privacy Law, 1*(3), 180.

Tene, O. (2013). Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws. *Ohio State Law Journal, 74*(6), 1217.

Vardanyan, L., & Kocharyan, H. (2022). Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: Main obstacles and challenges. *European Studies, 9*(2), 110-132.

Vasquez Callo-Müller, M. (2018). GDPR and CBPR: Reconciling personal data protection and trade. *APEC Policy Support Unit Policy Brief, 23*, 8.

Voss, W. G. (2016–2017). European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting. *Business Lawyer, 72*, 233.

Wallace, S. L. (2016). Rethinking data security: The differences between the European Union and the United States' approach to data security and building transnational standards with transparency and uniformity. *Wisconsin International Law Journal, 34*(2), 447.

Yakovleva, S., & Irion, K. (2016). The best of both worlds? Free trade in services and EU law on privacy and data protection. *European Data Protection Law Review, 2*, 191-195.

Policy Reports

Article 29 Data Protection Working Party. (2016, April 13). *Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision — WP238.* European Commission. https://ec.europa.eu/newsroom/article29/items/640157 Accessed 22 August 2024

Donohue, L. K. (2021). The evolution and jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. *Harvard National Security Journal, 12*, 198-205.

European Commission. (2013). Proposal for a regulation of the European Parliament and of the Council laying down rules on the protection of personal data in the European Union (COM (2013) 847 final). https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_en.pdf. Accessed 21 August 2024.

European Commission. (2022, March 25). Questions and answers: EU-U.S. Data Privacy Framework. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045. Accessed 22 August 2024.

European Commission. (2023). Adequacy decision EU-US Data Privacy Framework. https://commission.europa.eu/document/download/fa09cbad-dd7d4684ae60be03fcb0fddf_enfilename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. Accessed 23 August 2024.

European Commission. (2023, July 10). 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-U.S. Data Privacy Framework. https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. Accessed 21 August 2024.

European Parliament. (2015, May). The U.S. legal system on data protection in the field of law enforcement: Safeguards, rights, and remedies for EU citizens (pp. 10–13).

European Parliamentary Research Service. (2022). EU-U.S. Data Privacy Framework: Review of recent developments and future challenges.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf. Accessed 25 August 2024.

Holloway, D. (2019). Surveillance capitalism and children's data: The Internet of toys and things for children. *Media International Australia, 170*(1), 27. https://doi.org/10.1177/1329878X19828205. Accessed 26 August 2024.

Mildebrath, H. (2022). Reaching the EU-U.S. Data Privacy Framework: First reactions to Executive Order 14086. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf. Accessed 24 August 2024.

Office of the Director of National Intelligence. (2022, October 7). ODNI releases IC procedures implementing new safeguards in Executive Order 14086. https://www.intelligence.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086. Accessed 23 August 2024.

Rosenzweig, P. (2022, October 21). The "three Rs" of President Biden's transatlantic privacy outreach. *Lawfare.* https://www.lawfaremedia.org/article/three-rs-president-bidens-trans-atlantic-privacy-outreach. Accessed 25 August 2024.

Rubinstein, I. S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal, 28*(2), 1333-1414.

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. *Georgetown Law Journal.* https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf. Accessed 25 August 2024.

Svantesson, D. J. B. (2010). A legal method for solving issues of internet regulation: Applied to the regulation of cross-border privacy issues. *European University Press Working Paper, 1.*

Svantesson, D. J. B. (2011). The regulation of cross-border data flows. *International Data Privacy Law, 1*(3), 180.

Tene, O. (2013). Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws. *Ohio State Law Journal, 74*(6), 1217.

Tirole, J. (2023). Competition and the industrial challenge for the digital age. *Annual Review of Economics, 15*, 573-574. https://doi.org/10.1146/annurev-economics-090622-024222. Accessed 26 August 2024.

Voss, W. G. (2016–2017). European Union data privacy law reform: General Data Protection Regulation, Privacy Shield, and the right to delisting. *Business Lawyer, 72*, 233.

Wallace, S. L. (2016). Rethinking data security: The differences between the European Union and the United States' approach to data security and building transnational standards with transparency and uniformity. *Wisconsin International Law Journal, 34*(2), 447.

Weichert, T. (2014). Globaler Kampf um digitale Grundrechte. *Kritische Justiz, 47*(2), 123, 127.

Cases

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.

Case C-507/17 *Google LLC v CNIL* [2019] ECLI:EU:C:2019:772.

Case C-746/18 *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:153.

Legislation

GDPR-Info.eu. (n.d.). *Article 45 GDPR: Transfers on the basis of an adequacy decision.* https://gdpr-info.eu/art-45-gdpr/. Accessed 23 August 2024.

The White House. (2022, October 7). *Executive Order on enhancing safeguards for United States signals intelligence activities.* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/. Accessed 23 August 2024.

U.S. Department of Defense. (2008). *Executive Order 12333: United States Intelligence Activities.* https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf. Accessed 24

August 2024.

U.S. Department of Justice. (2019). *Clarifying Lawful Overseas Use of Data (CLOUD) Act.* https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf. Accessed 24 August 2024.

Websites

American Civil Liberties Union (ACLU). (2022, October 7). *New Biden executive order on EU-U.S. data transfers fails to adequately protect privacy.* https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy. Accessed 25 August 2024.

Anbound. (2018). *U.S. established rules for data controller standard.* http://www.anbound.com/Section/ArticleView_3691_1.htm. Accessed 26 August 2024.

Bradford, A. (2020). *The Brussels effect in context.* In *The Brussels effect: How the European Union rules the world* (Online ed.). Oxford Academic. https://0-doi-org.pugwash.lib.warwick.ac.uk/10.1093/oso/9780190088583.003.0004. Accessed 25 August 2024.

European Commission. (n.d.). *Data Act.* https://digital-strategy.ec.europa.eu/en/policies/data-act. Accessed 26 August 2024.

European Commission. (n.d.). *Digital Markets Act.* https://digital-markets-act.ec.europa.eu/index_en. Accessed 26 August 2024.

European Commission. (n.d.). *Digital Services Act.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en. Accessed 26 August 2024.

Ius Laboris. (2019). *The impact of the GDPR outside the EU.* https://iuslaboris.com/insights/the-impact-of-the-gdpr-outside-the-eu/. Accessed 26 August 2024.

The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data.* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Accessed 25 August 2024.

Willige, A. (2023, September 12). *What is the EU Digital Markets Act and how will it impact big tech?* World Economic Forum. https://www.weforum.org/agenda/2023/09/eu-digital-markets-act-big-tech/. Accessed 25 August 2024.