Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions

Xinchuchu Gao
University of Lincoln
xingao@lincoln.ac.uk

Xuechen Chen
Northeastern University London
xuechen.chen@nulondon.ac.uk

ABSTRACT

Transatlantic data flows are critical to the European Union–United States (US–EU) economic relationship. In a digitalised world, data are not only an economic resource but also important for protecting personal privacy, human rights, and national security interests. Nevertheless, the current transatlantic data privacy regimes are somewhat fragmented, and there is a lack of a coherent regulatory approach to data collection, storage, and transfer. In 2020, the Court of Justice of the European Union (CJEU) found that the US and EU data transfer accords failed to meet EU data protection standards and breached the US–EU Privacy Shield framework. The CJEU's 2020 invalidation of the Privacy Shield has limited transatlantic data flows and led to a lengthy period of persistent uncertainty for EU and US businesses. On July 10, 2023, the European Union adopted its adequacy decision for the EU-US Data Privacy Framework (DPF), which seeks to facilitate cross-border transfers of personal data in compliance with EU law. Against this backdrop, this research seeks to unpack and explain the turbulent process of institutionalisation of US-EU engagement in data privacy. By adopting an interests, ideas, and institutions (3I) approach, this article examines the key differences between the EU and US approaches to data governance as well as explains the facilitating and constraining factors underlying the EU–US relationship in terms of data flow and privacy regulation.

CCS CONCEPTS

• **Social and professional topics** → Computing / technology policy; Privacy policies.

KEYWORDS

European Union, United States, Data, Privacy

ACM Reference Format:
Xinchuchu Gao and Xuechen Chen. 2024. Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions. In *European Interdisciplinary Cybersecurity Conference (EICC 2024), June 05, 06, 2024, Xanthi, Greece*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3655693.3655720

EICC 2024, June 05, 06, 2024, Xanthi, Greece

ACM ISBN 979-8-4007-1651-5/24/06
https://doi.org/10.1145/3655693.3655720

1 INTRODUCTION

Transatlantic data flows are critical to the European Union–United States (US–EU) economic relationship. In a digitalised environment, data are not only an economic resource but also important for protecting personal privacy, human rights, and national security interests. Nevertheless, the current transatlantic data privacy regimes are somewhat fragmented, and there is a lack of a coherent regulatory approach to data collection, storage, and transfer. This fragmentation has disrupted US–EU data flows, posing challenges to US–EU economic and security relations. In 2013, widespread reports of US National Security Agency (NSA) surveillance programmes contributed to European concerns about US government access to EU citizens' personal data and about possible violations of EU citizens' privacy [1]. In 2020, the Court of Justice of the European Union (CJEU) found that the US and EU data transfer accords failed to meet EU data protection standards and breached the US–EU Privacy Shield framework. The Court of Justice of the European Union (CJEU)'s 2020 invalidation of the Privacy Shield has limited transatlantic data flows and led to a lengthy period of persistent uncertainty for EU and US businesses [2]. On July 10, 2023, the European Union adopted its adequacy decision for the EU-US Data Privacy Framework (DPF), which seeks to facilitate cross-border transfers of personal data in compliance with EU law. Against this backdrop, this article seeks to shed light on the relatively underexplored scholarly debate on the evolving US-EU transatlantic data privacy regime. Much of the scholarly literature focuses on the very visible contest between the US's and China's respective regulatory models of governing data. Nevertheless, the US-China contest is not the only determinant of the global digital order. The EU-US regulatory battles over data governance, although less visible and direct, can be consequential.

The article seeks to reflect on the following questions: To what extent does the EU's approach to data privacy differ from that of the US? How can the longstanding institutionalisation of transatlantic data privacy be explained? What are the key driving factors and obstacles underpinning the institutionalisation of the US–EU data privacy regime between the Safe Harbor agreement and the new EU-US DPF? This article argues that the EU-US engagement in data privacy has continued to be institutionalised over the past two decades, despite disruptions and obstacles deriving primarily from the two parties' divergent normative considerations on data privacy. The EU's data governance approach differs greatly from that of the US in terms of the conceptualisation of individual rights and the level of government involvement. Despite these normative differences, the EU and the US have gradually institutionalised transatlantic data privacy regimes to coordinate their actions and safeguard their shared commitment to the principle of free data flows and common economic interests. However, although the

EU and the US have made great efforts to sustain an institutional space in which they can maximise their economic gains and address disputes arising from divergent normative considerations, the institutionalisation of the transatlantic data privacy regime remains modest. While it is unlikely that such an institutionalisation process will progress substantially in the short term, the EU has managed to incrementally leverage its normative and regulatory impact on the US, which may result in greater convergence in data privacy governance between the EU and the US in the long term.

In this research, to explain the respective EU and US approaches to data governance and the evolution of the US–EU engagement in data privacy, we draw on conceptual tools derived from the scholarly literature on institutional and policy change. Specifically, we adopted an interests, ideas, and institutions (3I) approach to explain the facilitating and constraining factors underlying the EU-US relationship in terms of data flow and privacy regulation. Scholars in political science and policy studies generally agree that these three major elements—interests, ideas, and institutions—play a pivotal role in explaining institutional and policy changes [3]. The 3I approach has been widely adopted in empirical research. For example, some scholars used this framework to examine the UK's and the Netherlands' policies for promoting system innovations towards sustainability [4]. Building on these existing works, our paper draws theoretical insights from the 3I approach to operationalise the empirical research on the transatlantic data privacy regime.

Regarding methodology and data sources, we employed qualitative text analysis, underpinned by an interpretivist perspective, that involved the review and analysis of a wide range of primary and secondary materials. The data sources encompassed EU and US official documents, media coverage, policy reports, and scholarly works concerning transatlantic data privacy regimes. In addition, we used a process tracing technique to trace the process of institutionalisation of US–EU data privacy cooperation over time. Process tracing allowed us to examine the driving factors and obstacles, as well as the casual processes, underpinning the evolution of transatlantic data privacy regimes in different time periods [5]. In terms of the unit of analysis, this article limits the discussion of the US and the EU's respective data privacy regimes to the national level of the US and the supranational level of the EU.

Beyond the introduction, the remainder of this article is structured as follows: the next section examines the different EU and US approaches to data privacy governance, accounting for their considerations of interests and ideas. The following section traces the institutionalisation of the transatlantic data privacy regime over time and explores how this institutionalisation has interacted with the interests and ideas driving the respective EU and US data governance approaches. The final section offers some insights into policy implications, along with concluding remarks.

2 COMPARING EU AND US APPROACHES TO DATA GOVERNANCE: INTERESTS AND IDEAS

The EU's data governance approach differs normatively from that of the US in terms of its conceptualisation of individual rights and the level of government involvement. Moreover, the EU and the US approaches to data privacy reflect their respective economic interests, which mostly converge, and security interests, which often clash. Despite its acknowledgement of the importance of free data flows, the EU has exercised caution regarding the inclusion of free data flow provisions in trade agreements [6]. It was not until the 2018 Economic Partnership Agreement with Japan that the EU included provisions on cross-border data flows in bilateral trade agreements, but these provisions only committed 'the two sides [to] agree to "reassess" the need to incorporate free data flow clauses into the agreement within three years of the agreement's entry into force' [7]. The EU's more cautious approach to free data flows reflected its wish to couple the issue of data flows with high data protection standards. As the President of the European Commission, Ursula von der Leyen, stated in her political guidelines for the 2019–2024 Commission, Europe must 'balance the flow and use of data while preserving high privacy, security, safety and ethical standards' [8]. Based on the principle of prioritising privacy and data protection, which will be discussed in detail later, the EU has adopted a conditional approach to governing data flows between EU and non-EU countries. This means that only when such countries meet the EU's data protection requirements are cross-border data flows allowed.

Despite their shared commitment to the principle of free data flows, there is a 'conceptual gulf' between the EU and the US with respect to data governance [9]. This gap primarily derives from the different EU and US conceptualisations of individual rights and data privacy. In the EU, data privacy is a fundamental right protected at the highest constitutional level, as in Articles 7 and 8 of the EU's Charter of Fundamental Rights [10]. This demonstrates that the EU's approach to data governance places significant weight on the individual rights of its data subjects [11]. Thus, the EU views data privacy as part of its legal culture of fundamental rights. The safeguarding of privacy and data protection is also driven by the EU's overall aim of creating a sense of European citizenship and promoting democratic values. In particular, the protection of personal information depends on 'the preservation of democratic self-rule, the protection of autonomy, preventing the erosion of the capability of self-determination and avoiding a negative collective impact', which is the main rationale behind the creation of the EU [11]. According to this line of reasoning, adequate protection of data and privacy legitimises the EU's existence.

In contrast, the US Constitution provides no right to data privacy equivalent to that in the EU. The US data privacy law is underpinned by the 'marketplace' discourse, which views data as a commodity that can be used by business actors with few restrictions [12]. This underlying rationale is clearly demonstrated in the 2012 report Consumer Data Privacy in a Network World [13]. This report views personal data as a catalyst for the advertising marketplace, which in turn 'brings many online services and sources of content to consumers for free' [13]. Thus, it sees personal data in the marketplace as contributing to human flourishing, enabling individuals to choose their preferred use of personal data. It follows that the US's approach to data governance leaves significant areas of personal data use free from legal constraints.

The conceptual gap between the EU and the US in terms of data governance also derives from their different understandings of the

relationship between the market and the state. The EU has historically been somewhat suspicious of the market's capability to self-regulate and, therefore, more comfortable with government involvement [12]. The US's attitudes towards government involvement in data governance differ from those of the EU. Following marketplace logic, the thinking of US policymakers focuses on proper functioning of the market. Consequently, the US approach to data governance is primarily driven by the desire to boost the technology sector's growth. Regulators have therefore relied on market self-regulation and adopted a 'hands-off-the-internet' approach, with limited government intervention. In recent decades, however, the US has increasingly pursued a more balanced relationship between the promotion of innovation and the protection of privacy, hoping to establish a 'more flexible, innovation-enhancing privacy model' [13]. Nevertheless, with constitutional protection granted to data processing organisations, it remains unclear whether privacy, as opposed to innovation, will win the upper hand in the short term [11].

Despite their normative differences in data governance, the EU and the US share common interests in promoting the data economy. They both acknowledge the significance of data-driven technical innovation and economic growth. Beyond safeguarding individual data privacy, the EU has become aware of the necessity of participating in the global information economy and garnering its enormous economic benefits [9]. In A European Strategy for Data, the European Commission explicitly pointed out that while respecting the fundamental values that are the foundation of European societies, Europe aims to capture the benefits of better data usage, including greater productivity and competitiveness [14]. More recently, the EU's Data Act has aimed to make Europe a global leader in the data-agile economy [15]. In the US, the data economy has long been among the fastest growing and most innovative economic sectors. The EU and the US's shared interest in accelerating the free flow of data and the development of data-related economy is illustrated by negotiations within the WTO Joint Initiative on Electronic Commerce. The EU proposes to include a privacy and personal data protection exception while the US supports limiting exceptions to cross-border data flows to legitimate public policy objectives. Promoting data-driven technical innovation and economic growth therefore serves as a common ground towards the EU and the US's approaches to cross-border data flows [1].

In short, the EU and US approaches to data governance are underpinned by different conceptualisations of individual rights and levels of government involvement. The EU emphasises data privacy as a fundamental right protected at the constitutional level, whereas the US grants individuals the freedom to trade personal data. Regarding government involvement, the EU relies on government regulation, whereas the US adopts a market self-regulation approach. These normative differences have posed challenges to transatlantic data privacy cooperation. Beyond these normative differences, the EU and the US's approaches converge on common interests in pursuit of the economic benefits of the data economy. Nevertheless, when it comes to the level of openness of data economy, the EU's approach tends to be more protectionist. In addition, the EU and the US disagree on how to balance data privacy with national security. The following section explores how ideas, interests and institutions interact with each other in the development of the transatlantic data privacy regime.

3 THE INSTITUTIONALIZATION OF TRANSATLANTIC DATA GOVERNANCE REGIMES: DRIVING FORCES AND OBSTACLES

The transatlantic relationship concerning data flows and privacy is a significant example of US–EU relations and represents a shift towards innovative forms of governance [16]. However, the institutionalisation of US–EU data privacy has been far from a smooth linear process. Instead, institution building in terms of transatlantic engagement in data flows and privacy over the past three decades has been characterised by dynamic setbacks, adaptations, and innovations.

3.1 Phase 1: The safe harbor agreement and its invalidation (1990s-2015)

Notably, data flows and privacy have long been a sticking point and source of tension in transatlantic economic and security relations. Early attempts to strengthen US–EU institutional relationships over the issue of data privacy, going back to the late 1990s, subsequently resulted in the adoption of the 2000 Safe Harbor agreement. The negotiations over the Safe Harbor agreement can be regarded as direct responses to the EU's internal institutional development in terms of data governance, as evidenced by the adoption of the 1995 Data Protection Directive, which constituted the foundation of the EU's data privacy regime [1]. The EU's 1995 Data Protection Directive specified a set of conditions under which personal data could be transferred to non-EU countries. Specifically, this directive not only sought to harmonise personal data protection within the EU, but also required non-EU countries to meet the same adequate level of privacy protection before personal data could be transferred and used. The 'extra-jurisdictional effect' [17] of the EU's Data Protection Directive had a far-reaching impact on the US, primarily because, at that point, the US failed to meet the EU's criteria for adequate data privacy protection due to the absence of an overarching data privacy law [18]. As discussed earlier, in the EU, privacy is a fundamental individual right protected by law and government regulations. In the US, however, the priority is to maximise individuals' preferred uses of personal data in the marketplace. Accordingly, the US approach relies on market self-regulation rather than law and government oversight. The EU was therefore concerned that the 'patchwork of narrowly focused sectoral laws and voluntary self-regulation' adopted by the US could not provide sufficient protection of data originating in the EU [19]. However, the US insisted on the principle of self-regulation in data governance. Despite significant differences emerging from diverse normative considerations, the EU and the US generally accepted that transatlantic data flows should continue because both parties were aware of the economic losses that would result from the disruption of transatlantic data flows. The EU and the US were each other's largest trading partners. Moreover, the EU was the site of most US foreign investment; therefore, US-controlled affiliates in

Europe relied heavily on transatlantic data flows for their routine business activities [17].

Due to their divergent normative principles and shared economic interests, the EU and the US made it a priority to find a solution to the data privacy controversy. The US's initial strategy to respond to this challenge was twofold. Firstly, the US sought to provide further explanation to the EU to justify the reasonableness of its sectoral approach to data privacy. Secondly, companies in the US private sector were encouraged to develop a functional equivalent of the EU's Data Privacy Directive. However, the US was reluctant to introduce any fundamental changes in its own self-regulation data privacy approach [18]. The US Department of Commerce International Trade Administration therefore proposed establishing a self-regulatory mechanism that would shelter US companies from sanctions under the EU Data Privacy Directive.

Initially, officials from the European Commission were wary of the US proposal, partly due to concerns that allowing a self-regulated exception under the Data Protection Directive for the US could weaken the effectiveness of that directive. Despite these concerns, since there were limited options available for preventing trade conflict with the US, the European Commission agreed to consider the idea of a Safe Harbor agreement [20]. In 1998, based on an initial outline produced by the US Department of Commerce, Safe Harbor Principles were further developed in consultation with EU officials and US industry, leading to the officially adopted 2000 framework [20]. Notably, the US–EU Safe Harbor framework is not a treaty or international agreement, but instead consists of two separate dimensions of actions. The first is the release by the US Department of Commerce of Safe Harbor Principles and a list of frequently asked questions. The second is the European Commission's adoption of a decision regarding the adequacy of these principles [1].

It is widely argued that Safe Harbor agreement was a negotiated compromise to avoid a transatlantic trade war over data privacy issues. However, the 'safe harbor' primarily reflected the preferences and interests of US industry [1]. Regarding enforcement mechanisms, the US–EU Safe Harbor agreement was a hybrid of government enforcement and self-regulation, allowing firms to use personal data more flexibly than the EU Data Protection Directive permitted. This meant that the Safe Harbor did not address fundamental normative differences between the EU and US approaches to data privacy. From the viewpoint of the US, the Safe Harbor agreement responded to the EU's concerns about data privacy without changing its own privacy regime.

For 15 years, the Safe Harbor agreement provided a foundation for transatlantic flows of personal data for commercial purposes, despite ongoing controversy within the EU regarding the adequacy of data privacy protection under this mechanism [21]. The first major turning point for the US–EU institutional relationship concerning data privacy came with the 2013 Snowden whistleblowing event, which revealed mass surveillance by the US National Security Agency. This event generated deep concerns over the effectiveness of the Safe Harbor agreement. Against this backdrop, the European Commission and the US Department of Commerce began discussions in January 2014 to formulate a new framework for transatlantic data flows [1]. For the European Commission, strengthening the existing Safe Harbor framework was preferable because its 'revocation would adversely affect the interests of member companies in the EU and in the US' [22]. In contrast to the Commission's emphasis on economic interests, the European Parliament raised concerns over the violation of EU fundamental rights and data protection standards [23]. The European Commission's and the European Parliament's attitudes towards the Safe Harbor agreement reflected tension within the EU regarding the balance of economic interests and normative considerations.

A ruling by the CJEU then sealed the fate of the Safe Habor agreement. In October 2015, following the Schrems I case, the CJEU declared that the European Commission's adequacy decision on the Safe Habor agreement was invalid. The CJEU's ruling again reflected the tension between the EU and US approaches to data privacy. The CJEU found that the US's national security, public interest, and law enforcement principles prevailed over the protection of privacy. Hence, the CJEU ruled that US public authorities failed to provide adequate levels of protection for data privacy as required by EU law, and it therefore invalidated the Safe Harbor agreement.

The preceding explanation demonstrates that the Safe Habor agreement emerged from EU and US efforts to address normative differences and allow continued transatlantic data flows to maximise their common interests. Both parties benefitted economically from this arrangement. Nevertheless, the institutionalisation of the US–EU data privacy regime introduced by the Safe Harbor agreement is arguably limited because the arrangement did not require the US to introduce formal legislation or set a precedent for future changes in the US privacy regime. Consequently, the CJEU's ruling was that the Safe Harbor agreement failed to provide sufficient protection of EU citizens' personal data. Although the Safe Harbor agreement marked a significant institutional innovation, the modest level of institutionalisation turned out to be ineffective to address the deep-rooted divergence between the EU and US approaches to data privacy as well as challenges resulted from exogenous shocks.

3.2 Phase II: The Privacy Shield agreement and its failure (2016–2020)

Nevertheless, the CJEU's ruling did not mark the end of the institutionalisation process for US–EU data flows. The EU and the US started negotiations immediately after the CJEU's decision, motivated by a sense of urgency generated by pressing demands from business and technology companies [1]. At the time of the CJEU's decision, approximately 4,500 companies were supporting Safe Habor provisions, and there were widespread concerns that the ruling would disrupt transatlantic data flows. Many business and industry leaders expressed hope that the EU's trust in US data protection standards could be restored [24]. Driven by the urgent need to rebuild the framework for governing continued flows of data across the Atlantic, a successor agreement to Safe Harbor agreement needed to be concluded promptly. In February 2016, the European Commission and the US's Department of Commerce jointly announced that they had reached an agreement in principle to replace the Safe Harbor agreement with the Privacy Shield principles. This new framework would enable companies to continue transferring personal data between the EU and the US [25]. The Privacy Shield principles largely mirrored the self-certification

approach of the Safe Harbor agreement and functioned based on unilateral actions by the EU and the US [16]. Nevertheless, despite its institutionalised dimensions remaining weak, the Privacy Shield principles allowed for more institutional cooperation between the EU and the US regarding data governance. For instance, the Privacy Shield principles followed the European Commission's call for increased transparency and included a significantly longer list of notice requirements. Additionally, they embodied more stringent requirements for onward transfers and provided more detailed provisions on recourse, enforcement, and liability [1]. In addition, the US government agreed to establish an annual review system that would allow EU officials to monitor the operation of the Privacy Shield, including its restrictions and safeguards related to national security access. Moreover, the US agreed to establish a new Privacy Shield Ombudsman to enable individuals to submit enquiries regarding US intelligence practices within the State Department. For the first time, the US government, through letters from the Office of the Director of National Intelligence and the Department of Justice, gave the EU written assurance that access to data by public authorities for national security and law enforcement purposes would be subject to limitations, safeguards, and monitoring mechanisms [16].

Therefore, like the Safe Harbor agreement, the Privacy Shield principles did not require the US to introduce new, formal legislation or change its privacy regime [1]. Despite the lack of amended US laws, the US responded to the EU's concerns about the undermining effects of the US's use of data with a 'written assurance'. This shows that, through the Privacy Shield principles, the US–EU data flows and data privacy achieved a certain level of institutionalisation. Four years after the implementation of the Privacy Shield principles, another major shock to the US–EU data privacy institutionalisation occurred. In July 2020, the CJEU ruled on the Schrems II case, once again declaring that the transfer of personal data according to the Privacy Shield principles was illegal and did not offer the necessary level of protection to comply with EU standards after the introduction of the General Data Protection Regulation (GDPR). This ruling was prompted by extensive US data collection through government surveillance and the lack of options for EU citizens to seek redress. Although the Privacy Shield principles attempted to address the concerns prompted by the Schrems I case, which invalidated the Safe Harbor agreement, they were regarded as insufficient to meet the requirements of the CJEU after the implementation of the GDPR [6]. Similar to the Schrems I judgement, the Schrems II ruling reflected the EU's persistent concerns over the US lack of data protection caused by their divergent normative considerations, different conceptualisations of individual rights, and varying levels of government involvement [27]. For instance, regarding a 2018 resolution on the use of Facebook users' data and its impact on data protection, the European Parliament criticised the protection afforded by the US–EU Privacy Shield principles and urged the US authorities responsible for enforcing them to act [28].. The US reaction mostly reflected its economic considerations. The US Secretary of Commerce, Wilbur Ross, and the US Secretary of State, Mike Pompeo, expressed their deep disappointment with CJEU's 2020 ruling, but stated that they were in close contact with the EU on this matter and hoped to limit the adverse effects on the US$7.1 trillion transatlantic economic relationship [27].

Meanwhile, within the EU, there were increasing concerns over the economic costs of invalidated Privacy Shield principles. Observers pointed out that transatlantic data flows were in crisis, and a pragmatic US–EU digital alliance would be beneficial for both sides [29]. European businesses, therefore, called for the reestablishment of a framework for governing transatlantic data flows [30]. The European Commission echoed this interest in collaborating to ensure transatlantic data flows. In a conference held shortly after the CJEU's ruling, Vice-President of the European Commission Jourová made it clear that both sides would continue working to ensure the continuity of safe data flows [31]. In short, the Schrems II judgement again reflected the long-lasting tension between the different data governance approaches of the EU and the US, given their respective normative considerations. Nevertheless, both sides remain aware of the economic significance of data flows between the EU and the US and the urgent need for the restoration of transatlantic data privacy regimes.

3.3 Phase III: Towards a new transatlantic data privacy framework (TADP) (2021–present)

Similarly, instead of demolishing the institution-building efforts, the CJEU's decision on the Schrems II case marked the beginning of more rounds of intense negotiations between the two sides. Following more than two year of detailed EU–US negotiations led by Secretary of Commerce Gina Raimondo and Commissioner for Justice Didier Reynders, in July 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework that would continue to foster transatlantic data transfers and tackle the concerns raised by the CJEU in the Schrems II ruling. As part of the framework, the US has agreed to implement reforms that will ensure that signal surveillance activities are necessary and proportional to achieving specified national security objectives. This includes the creation of a two-tier independent redress mechanism to enforce corrective actions as well as the establishment of robust and multi-layered oversight of signal intelligence activities to guarantee compliance with surveillance limitations [32].

In addition, recent dynamics in the US–EU relationship offer hope for positive developments that, in the long term, may result in a higher degree of normative convergence between the EU and the US. Specifically, during the US–EU Summit in 2021, a new institutional mechanism—the US–EU Trade and Technology Council—was created to serve as a non-binding institutional platform for both parties to coordinate actions and approaches to global trade and economic and technology issues and to strengthen transatlantic economic relations based on their shared interests and values, such as human rights and democracy [33]. The council meets periodically at the ministerial level to steer cooperation. In the meantime, the Council has established 10 working groups led by relevant departments, services, or agencies to facilitate the operationalisation of political decisions and the coordination of technical developments. An appropriate data governance and technology platform is one of the key themes for the working groups [33]. The creation of these non-binding institutional mechanisms indicates the US's strong intention to deepen political engagement and dialogue with the EU regarding general data governance and technology issues.

Moreover, another recent development in the US—the proposal to establish the ADPPA—has received tremendous attention in policy circles and has been regarded as a positive signal of the future trajectory of transatlantic data privacy cooperation [34]. The ADPPA—the first federal privacy bill with bipartisan support in over a decade—was proposed on 3 June 2022. The bill passed a committee vote in July 2021 and has now made its way to the house floor, making it one of the best attempts at establishing a national privacy framework in the US. Although there are still several obstacles to overcome before the ADPPA can be considered a serious contender as a new law, organisations should remain abreast of its provisions. The ADPPA aims to safeguard the personal information of US citizens through a wide range of measures, many of which are similar to those found in the GDPR. These measures include compliance mechanisms, such as data minimisation, privacy by design (PbD), and conditions for consent. It is interesting to note that the ADPPA shares many similarities with the EU's GDPR. Notably, at a high level, the GDPR principles of transparency, data minimisation, necessity, and purpose are reflected in the proposed ADPPA. This can be seen as good evidence of the EU's 'Brussels effect'—the phenomenon whereby EU regulations and standards have an impact beyond the EU's borders [12]—incrementally altering or shaping the US's normative and legal structure in terms of data privacy.

The preceding discussions demonstrate two interesting trends in US-EU data privacy cooperation. First, although the evolution of the transatlantic relationship has been characterised by a turbulent and delicate process constantly failing to fundamentally address the normative and conceptual gulf between the EU and US approaches to data privacy, the institutionalisation of transatlantic data privacy regimes is arguably resilient. Specifically, from the Safe Harbor agreement to the latest EU-US Data Privacy Framework, new institutional mechanisms have been agreed and created to address the EU's concerns, which indicates the US's willingness to incrementally strengthen the level of institutionalisation in transatlantic data privacy. Throughout this process, it can be argued that common interests outweigh normative divergence and serve as the most important motivation driving the institutionalisation in US-EU data privacy cooperation forward. Second, whilst the normative divergence between the EU and the US is unlikely to be overcome in the short term, normative convergence may occur progressively in the longer term if the EU manages to leverage greater regulatory impact on the US data governance approach. Biden's executive order and the proposal to establish the ADPPA have already shown positive signals of the US's political and normative adjustment in terms of data privacy not only in transatlantic relationship but also at domestic level.

4 CONCLUSION

To provide a reflection on the institutionalisation of the US–EU data privacy regime and explore obstacles to further institutionalisation, this article draws on the 3I approach to develop an empirically grounded analysis of the US–EU relationship regarding data privacy by considering their respective ideas and interests. The article provides evidence that despite facing obstacles and disruptions resulting from their divergent normative considerations, the US and EU have institutionalised their engagement in data privacy over the past two decades. Whilst the conceptual and normative gulf constituted the key constraining and disruptive factor in this institutionalisation process, transatlantic engagement in data privacy remains resilient. Common interests, particularly economic considerations, play the most pivotal role in driving transatlantic engagement in data privacy forward as well as in incentivising new policy and institutional initiatives throughout this turbulent process. The evolution from the Safe Harbor agreement to the newly EU-US Data Privacy Framework witnessed an incremental yet increasing degree of institutionalisation with the development of new institutional and policy mechanisms to address the concerns resulted from the CJEU's rulings. This research also shows that the EU has managed to gradually leverage its normative and regulatory impact on the US, which may ultimately lead to greater normative and regulatory convergence in data privacy governance between the two entities in the long term.

REFERENCES

[1] Suda, Yuko. 2017. The politics of data transfer: transatlantic conflict and cooperation over data privacy. Routledge, New York, NY.

[2] Obendiek, Anke Sophia. 2023. Data Governance: Value Orders and Jurisdictional Conflicts. Oxford University Press, Oxford.

[3] Hay, Colin. 2004. Ideas, interests and institutions in the comparative political economy of great transformations. Review of International Political Economy Vol. 11, No. 1 (Feb, 2004), pp. 204-226. https://www.jstor.org/stable/4177494

[4] Kern, Florian. 2011. Ideas, Institutions, and Interests: Explaining Policy Divergence in Fostering 'System Innovations' towards Sustainability. Environment and Planning C: Government and Policy, 29(6), 1116-1134. https://doi.org/10.1068/c1142

[5] George, Alexander L., and Andrew Bennett. 2005. Case studies and theory development in the social sciences. MIT Press, Massachusetts.

[6] Yakovleva, Svetlana. 2018. Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?. World Trade Review 17, no. 3 (July, 2018): 477-508. https://doi.org/10.1017/S1474745617000453

[7] European Commission. 2018. Agreement between the European Union and Japan for An Economic Partnership. https://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf

[8] European Union. 2019. Political Guidelines for the Next European Commission 2019-2024. https://op.europa.eu/en/publication-detail/-/publication/62e534f4-62c1-11ea-b735-01aa75ed71a1

[9] Schwartz, Paul M. and Peifer, Karl-Nikolaus. 2017. Transatlantic Data Privacy. Georgetown Law Journal 115 (November, 2017), UC Berkeley Public Law Research Paper. https://ssrn.com/abstract$=$3066971

[10] Official Journal of the European Communities. 2000. Charter of Fundamental Rights of the European Union. https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[11] De Bruin, Ruben. 2022. A Comparative Analysis of the EU and US Data Privacy Regimes and the Potential for Convergences. Hastings Sci. & Tech. LJ 13 (2022): 127. https://dx.doi.org/10.2139/ssrn.4251540

[12] Bradford, Anu. 2023. Digital empires: The global battle to regulate technology. Oxford University Press, Oxford.

[13] White House. 2012. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

[14] European Commission. 2020a. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri$=$CELEX:52020DC0066&from$=$EN

[15] European Parliament and the Council. 2022. Regulations (EU)2022/868 of the European Parliament and of the Council of 20 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri$=$CELEX:32022R0868&from$=$EN

[16] Fahey, Elaine. 2018. Introduction: Institutionalisation beyond the nation state: new paradigms? in Fahey, Elaine (eds) Transatlantic relations: data, privacy and trade law (pp. 1-27). Springer International Publishing, Cham.

[17] Shaffer, Gregory. 2000. Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. Yale Journal of International Law 25(1):1-44. http://hdl.handle.net/20.500.13051/6405

[18] Long, William J., and Marc Pang Quek. 2022. Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. Journal of European

Public Policy 9, no. 3 (2002): 325-344. https://doi.org/10.1080/13501760210138778
[19] European Commission. 1999. Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp19_en.pdf
[20] Heisenberg, Dorothee. 2005. Negotiating Privacy: the European Union, the United States, and Personal Data Protection. Lynne Reinner, London.
[21] Kobrin, Stephen J. 2004. Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance." Review of International Studies 30, no. 1 (2004): 111-131. https://www.jstor.org/stable/20097901
[22] European Commission. 2013. Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri$=$CELEX%3A52013DC0847.
[23] European Parliament. 2014. European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri$=$CELEX:52014IP0230&from$=$EN
[24] Congressional Research Service. 2021. U.S.-EU Privacy Shield and Transatlantic Data Flows. https://crsreports.congress.gov/product/pdf/R/R46917
[25] European Commission. 2016. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216
[26] Benson, Emily and Duncan, Elizabeth. 2022. Temporarily shielded? Executive Action and the Transatlantic Data Privacy Framework. CSIS. https://www.csis.org/analysis/temporarily-shielded-executive-action-and-transatlantic-data-privacy-framework
[27] European Parliament. 2020. The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
[28] European Parliament. 2018. European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_EN.html
[29] Cory, Nigel and Dick, Ellysse. 2021. How to Build Back Better the Transatlantic Data Relationship." ITIF. https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship/
[30] Cory, Nigel. 2021. How Schreme II Has Accelerated Europe's Slide Toward a De Facto Data Localisation Regime. ITIF. https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data/
[31] European Commission. 2020b. Opening remarks by Vic-President Jourová and Commissioner Reynders at the press point following the judgement in case C-311/18 Facebook Ireland and Schrems. https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366
[32] European Commission. 2022. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087
[33] European Commission. 2023. EU-US Trade and Technology Council. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en
[34] Propp, Kenneth. 2023. "Biden's call to modernize US tech policy would pay transatlantic dividends"Atlantic Council, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/bidens-call-to-modernize-us-tech-tpolicy-would-pay-transatlantic-dividends/