Le nouvel individualisme

Brunner, Matthias; Sgier, Lea

The Securitization of Transatlantic Data Transfers

Audrey Bally

Preface - Internship Report

Introduction

A year and a half after the CJEU judgment invalidating the European Commission's Decision[1] on the adequacy of the protection provided by the EU-U.S. Privacy Shield, President Biden signed an Executive Order enhancing the safeguards of US signals intelligence activities.[2] This commitment addresses the concerns that arose in the court case Schrems II, which led to the suspension of the EU-US Privacy Shield in 2020. The commitment aims at providing adequate adhesion to the agreements' principles, which was the main concern for the decision, to accelerate and bring to an end the discussions for a new agreement and provide a new legal basis for data transfer across the Atlantic.

The EU-US Privacy Shield is a legal framework bound to regulate transatlantic exchanges of personnel data for commercial purposes. Its main purpose is to protect European citizens' privacy rights while enabling easier transfer of personnel data from EU entities to US companies. The European Union recognizes privacy as a fundamental right guaranteed by the European Union Charter of Fundamental Rights that protects individuals from corporate abusive data collection[3]. This right, under European laws, should not only be protected inside the EU borders but also when data is transferred abroad. Companies should only cooperate with countries who comply to similar rules[4]. The European Commission, thus, give guidelines on which country provide "essential equivalent" safeguards to those present under EU law[5].

In 2015, the Snowden revelations brought to light the undertakings of US surveillance programs, which led to the invalidation of the prior agreement, the Safe Harbor. The framework permitted companies to self-certify to the US Department of Commerce they abide by privacy principles when transferring data outside of the EU. After the revelations, the CJEU invalidated the Safe Harbor agreement, on the fact that under US law, US companies are bound to provide national security agencies with the withheld personal information to fall under national security, public interest and law enforcement requirements[6]. Thus, US national authorities have "privacy"

[1] (EU) 2016/1250 of 12 July 2016, https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update
[2] 14086 "Enhancing Safeguards for United States Signals Intelligence Activities" https://www.commerce.gov/news/press-releases/2022/10/statement-us-secretary-commerce-gina-raimondo-enhancing-safeguards
[3] Linn, "A Look into the Data Privacy Crystal Ball," 1317
[4] Weiss, & Archick, "U.S.-EU data privacy," 13
[5] Zalnieriute, "Data Transfers after Schrems II," 20
[6] Weiss, & Archick, "U.S.-EU data privacy," 13

over Safe Harbor principles and their actions disregard the rules laid by the agreement. Five years later, the EU-US Privacy Shield followed the same track to failure, when the CJEU courted that the US surveillance regime did not provide sufficient safeguards under the principle of proportionality, hence the United-States did not provide "essential equivalent" safeguards and the agreement can not longer sustain[7].

In 2022, after two years of discussions, European Commission President Ursula von der Leyen and President Biden have announced an agreement in principle on a new EU-US Privacy Shield. According to NOYB, the privacy NGO chaired by the lead litigant in the cases which led to both invalidation, they hear that the US does not plan to change its surveillance laws, but only foresee executive reassurances. As others, including political research figures, the NGO tend to believe that the new agreement will fail for the same reason as it has before. The past agreements have fallen short due to differences in terms of legal system, privacy definition and national security paradigms[8]. Thus, the future of the framework holds on the possibility to intertine both views of the issue.

This research aims at understanding why there has been no sufficient solution to the data flow problem. The previous agreements were invalidated for similar reasons, and many experts expect a similar loop to repeat. Thus, this paper tries through the securitization theory to point out the issue of the privacy and national security paradigm that may be one of the causes of the problem. In Europe's perspective, individuals' right to privacy is in danger in the hands of private corporations and governmental organizations across-borders. In the United-States, national security is at stake and should prevail over individual privacy. This research intends to show that the European Union and the United-States do not define the perpetrators and targets of the threats to be the same. Then, if this assumption turns out to be true, policymakers would be able to develop an agreement which links both views and therefore avoid future failure of such transatlantic treaties. Thus, without a common understanding of the targets and perpetrators of these threats, data flow agreements will keep on failing. This paper will try to answer the following research question:

How do securitisation perspectives of privacy and national security influence the conception and implementation of the transatlantic data flow agreements?

---

[7] Zalnieriute, "Data Transfers after Schrems II," 20

[8] NOYB, (2022). "Privacy Shield 2.0"? - First Reaction by Max Schrems. https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

Cross-border data exchanges have multiple implications, which will be discussed in the following section. The effect of national security perspectives on the agreements will also be discussed. This paper will start with a literature review of the concepts of privacy and national security in the two regions, before discussing the theoretical framework which will guide this research. The third section will retrace the methodology of the qualitative research that has been conducted and which findings will be analyzed in the fourth section. Last, the conclusion will highlight that ***Conclusion to summarize***.

Transatlantic Data Flow Agreements

The issue of the protection of data is not new and started with the development of the internet and new technologies. In 1995, the European Union established a region-wide framework on data privacy protection in the aim of harmonizing and facilitating data between countries. The Data Protection Directive (DPD) was thought to help strengthen the internal market and foster the development of an information based economy.[9] The framework defines guidelines on how personal information may be collected and used only for specific purposes, explicit and legitimate purposes. Exchange to non-EU countries may occur under the European Commission jurisdiction assessing the adequate level of protection provided by the given country, with particular consideration of the nature, duration and purpose of the processing of the data [10]. Thus, transfer to a third country anc only occur under strict requirements. Data Protection Authorities were created in each EU state to which databases should be registered and from which process of data should be approved.[11]

An amendment was added obligating telecommunication and internet services providers to keep for a period from 6 months to no more than 2 years information, such as traffic and location of mobile telephony, internet access and email communications.[12] Law enforcement authorities could have access to such information for the investigation, detection and prosecution

[9] Weiss, & Archick, "U.S.-EU data privacy," 2
[10] Ibid.
[11] Ibid., 3
[12] Nesterova, "Crisis of Privacy and Sacrifice," 4

of serious crime and terrorism. This amendment was invalidated by CJEU on the basis of unjustified interference with fundamental rights.

The DPD was later on invalidated on the basis that it disrupted transfer of data to the United States, thus negatively affecting businesses on both sides. It was also determined that the timeframe for the retention of data, safeguards relating to security and protection of data was insufficient, even when retained within the EU[13].

The cross-border exchange of data between the European Union and the United-States is the largest in the world and their trading relationship, the largest[14]. Thus, to avoid a trade war and allow the continuation of data transfer, the Safe Harbor principle was created in 2000. The agreement allowed US companies to meet adequate levels of protection by complying to seven principles (notice, choice, onward transfer, security, data integrity, access and enforcement)[15]. The entities had to self-regulate and self-certify to the US department of commerce.

The Snowden revelations were made public in 2013 and brought to light the US surveillance programs. It revealed that the NSA had access to emails, docs, photos and other sensible data of users from large American tech companies.[16] This led to the invalidation of the Safe Harbor after the CJEU decision on Schrems I in 2015. The judgment was held under the European law regarding legislations permitting public authorities to have general access to content of electronic communication as compromising fundamental rights to private life.[17]

The following agreement was presented in 2016 under the name EU-US Privacy Shield and with the intention to provide stronger obligations on companies.[18] The framework detailed increased guidelines on monitoring and enforcement of data privacy. A supplemental set of principles were added and US security officials had to prove their commitments in official letters[19]. Also, it allowed EU citizens to complain against misuse of their information in the US.

This new transatlantic agreement was invalidated in 2020 after the CJEU decision on Schrems II. Again, the safeguards provided in the US was insufficient to those present under EU

[13] Nesterova, “Crisis of Privacy and Sacrifice,” 6
[14] Linn, “A Look into the Data Privacy Crystal Ball,” 1315
[15] Callahan-Slaughter, “Lipstick on a Pig,” 248
[16] Zalnieriute, “Data Transfers after Schrems II,” 17
[17] Nesterova, “Crisis of Privacy and Sacrifice,” 7
[18] Callahan-Slaughter, “Lipstick on a Pig,” 249
[19] Ibid.

law and the "essential equivalent" standard provided by the European Commission to US companies was retrieved on the basis that the information provided to those entities were then transferred to national agencies without the consent of the individuals[20].

The Systematic Failure

The literature is very critical towards the implementation made between the Safe Harbor principles and the Privacy shield. For some authors, the Privacy Shield does provide an upgraded framework with improved data protection systems and increased oversight by the US government.[21] Although, for many, the new agreement was only a better coated version of the first where the safeguards required under EU laws of strict necessity and proportionality in terms of data processing are not available in the US.[22]

The data privacy NGO, NOYB, believes that the European Commision bowed to US pressures to provide a new framework as soon as possible, without correcting the fundamental flaws that exists in the system of enforcement[23]. For example, according to Vermeulen, the consideration of deemed necessity of an investigation with an individual's privacy is relative to the legitimate function governments give as purposes, like law enforcement.[24] Thus, EU citizens would receive indirect protection, just as Americans do, but their privacy relative to how it is exposed in EU law would be by passed under US law, where governmental investigation rules.

As opposed to the authors who believe that the data flow agreements have not evolved and affected the protection of individual's privacy, Shaffer accredits five factors to upgrading of US social protections in the area of data privacy.[25] As businesses want greater trade possibilities and develop elsewhere, they fall under these foreign requirements.[26] When the internal market is as large as the EU is, threats, such as restriction of data transfers to the US on account of its inadequate data privacy protections, have a strong leverage.[27] These protections are not easily met through private contact, thus individuals turn towards the government to protect their

---

[20] Zalnieriute, "Data Transfers after Schrems II," 20
[21] Linn, "A Look into the Data Privacy Crystal Ball," 1358
[22] Vermeulen, "The Paper Shield," 12
[23] NOYB, "CJEU invalidates "Privacy Shield"," https://noyb.eu/en/cjeu
[24] Vermeulen, "The Paper Shield," 11
[25] Shaffer, "Globalization and social protection," 80
[26] Ibid., 81
[27] Ibid., 82

privacy.[28] As data protection affects the privacy interests of both EU and US citizens, cross-border effects of data privacy policy can not be deflected for them to be effective[29]. Last, regulatory conflicts with significant external effects, like data exchanges, require harmonization.[30] Consequently, the EU-US data flow agreements provoked new domestic political and regulatory interactions through the impact of the European pressure backed by a strong market power.

According to Linn, the Privacy Shield, just as the Safe Harbor principles, lack protections from US surveillance. This is not only affecting these past agreements, but threatens the future framework, as it shows unperfect settlements and inefficient trade mechanisms.[31] A potent agreement would be able to operate under the different notions of privacy that apply in the EU and the US and protect personal data in divergent legal systems. Thus, the author proposes to restructure the framework into a public-private EU-US business arrangement, where a Data Privacy NGO would carry the administrative and enforcement role of US agencies.[32]

The failures of the data flow agreements are well supported across the literature on the over-reach of US surveillance programs on EU citizens, but rarely does the literature have an in-depth look into why those changes have not been led yet. The European Union and United-States diverge in their view of privacy, national security, as well, in the structure of their institutions. Thus, these multi-elements implicated in the scope of data flow make it rather difficult to dive into what may be at the heart of the problem. In such a way, this research has the purpose to determine how the securitization of the data flow issue may have been portrayed in both regions differently and how this may cause bankrupted agreements.

The securitization theory, which will be defined more closely in the following section, has been applied to different topics, such as immigration, environmental changes, to discuss how political actors may use security language to define a threat and shape their political responses to such. In terms of cyber-threats, many authors have worked on how the securitization theory can be applied to the online world. Most of which have discussed how cybersecurity has entered the US security agenda without actual threats. In his study, Eriksson argues that the "framing" of

[28] Shaffer, "Globalization and social protection," 83
[29] Ibid., 85
[30] Ibid., 86
[31] Linn, "A Look into the Data Privacy Crystal Ball," 1358
[32] Ibid.

cyber-issues surfaced from different political spheres and reached beyond traditional security discussions.[33]

Through the securitization theory, the speech act is at the heart of the study and as a result, many authors conclude that government authorities and even corporate leaders are the main voice of cybersecurity.[34] And to emulate the sense of harmful threats, the emphasis is often pin-pointed to a foreign exploitation of classified materials, precluding US citizens from being the possible perpetrator and society the target.[35] Thus, the political implications of such threats fall under national security prerogatives.[36] Howere, the importance of cyber-threats on the national security agenda seems inconsistent to the scale of events that could justify such status.

Ultimately, the literature review shows that there is an issue of security in the conception and implementation of the EU-US data flow agreements. The securitization theory has been used in different contexts and can help determine how and to what extent political actors shape an issue into a security threat. This paper, through a securitization analytical research will try to reveal how the issue of data flow has, whether, been depicted as a security issue of privacy for one of our actors, and as a national security issue for the other. This research aims at understanding how both actors define the threats created by the data transfers and explaining how it interferes with transatlantic data flow agreements. While giving such a definition, this paper will add to the literature by developing a new way to understand and maybe solve the issue of EU-US data transfer. On the other hand, this research will not have a jurisdictional and institutional perspective like other literature may provide.

With the upcoming new EU-US Privacy Shield, there is a need to better understand how the previous argument failed and how to prevent the next one from effectively failing. If this issue is not fixed, the perpetual making and invalidating loop will keep on going, with it the bypassing of European citizens' privacy rights and US national security. Whereas, if the two securitization perspectives are revealed to be existing, then policymakers and governmental officers will be able to reach common ground and find the most effective agreement to collude both perspectives.

[33] Balzacq, Léonard, & Ruzicka, "'Securitization' revisited: theory and cases," 516
[34] Nissenbaum, "Where computer security meets national security," 63
[35] Cavelty, "Cyber-terror-looming threat or Phantom menace," 24
[36] Ibid., 30

Thus, to understand how the European Union and United-States define the threats of cross-border data flow, we will start by looking at the different definitions of the terms privacy and national security given in the two regions. The theoretical framework will be built around the securitization theory and from the dual perspective of privacy, national security and national security issue of privacy of our main actors. We will also quickly look at the regulatory frameworks of the EU and US, which can not be excluded when discussing such layered topics. This section will be concluded by the description of our assumptions, to which the European Union sees corporate and governmental data processing as a threat to individual privacy, the latest being essential to protect in cross-border data flow, while the United-States views individuals' information as a threat to national security which should be reinforced through surveillance programs. Before analyzing and evaluating our findings, we will detail the methodology employed in this qualitative research. This paper will end by **Add conclusion summary.**

Securitization & Transatlantic Data Transfers

Data transfer agreements can not be understood through one glass, but should be approached through different conceptions. The long-standing issues are in terms of privacy and national security, thus the balance of individual rights for their personnel information and the one of the state to protect itself. In the following subsections, we will try to conceptualize each point and determine how they affect the decision making-process in the EU and US. This research will try to determine the securitization conception involved in both parties and before connecting it to the different elements of data flow exchange. Therefore, we will start by looking at the privacy preferences in the European Union and the United-States, then we will look at the national security narratives of the two protagonists, before underlying the arising national security issue of privacy. Last, we will have a quick glance at the regulatory framework of the two regions, which by its contrast and complexity may also impact the transatlantic data exchange agreement-making. This section will aim at identifying the different theories involved in our case studies and see how they may be relevant to the implications of the securitization theory. We will look at the differences of approaches between the two regions in terms of privacy, national

security, as well as their institutional systems to have a larger understanding of how these three may affect the construction of a transatlantic agreement.

The securitization theory studies the interactions between the so-called securitizing actor, the agent who presents an issue as a threat, and its audience, rather than the inquiry use and control of military force.[37] According to this approach, issues are fashioned to become a "security" probe through the speech act[38]. The security issue is thus seen as a result of the leader's effort to shape the world and depends on its ability to convenience its community.[39] The securitization theory looks at why and how this happens and its effects on society and the political sphere. Hence, It is fundamentally different from critical security studies and answers peculiar questions.

Securitization supports the idea that by making an issue a security problem, it enables the actors in charge to handle the situation in the way they deem the most appropriate. [40] It is a playful balance of power to socially and politically construct a threat.[41] By presenting an entity as threatened, the securitizing actor calls for extraordinary measures for the survival of the threatened object. Thus, according to the theory exposed by the Copenhague School, the issue is then moved from normal to emergency politics, allowing securitizing actors to use rules and regulations outside of the normal democracy policy making process.[42] This idea of extraordinary measure is not used as much in more recent work on securitization, where the departure between normal and exceptional politics is not established, such as in Cavelty's and Nissenbaum's works discussed previously.

This approach allows a theoretical analysis of where the issue was created. Thus, it is important to define the different elements involved in the process of securitization. First, the securitizing actor uses securitizing moves to present an issue as a threat. Then the referent subject is the threatening entity, whereas the referent object is the entity threatened. Another key element is the audience without which agreement, the status of the threat can not be granted. Last, the context and adoption of polities, whether these are exceptional or not, should reinforce

[37] Balzacq, Léonard, & Ruzicka, "'Securitization' revisited: theory and cases," 496
[38] Taureck, "Securitisation Theory and Securitisation Studies," 3
[39] Balzacq, Léonard, & Ruzicka, "'Securitization' revisited: theory and cases," 495
[40] Ibid.
[41] Taureck, "Securitisation Theory and Securitisation Studies," 3
[42] Ibid.

the securitization, desecuritization model. [43] The identification of existential threats, emergency action and the breaking free of rules effect are the important elements to clarify to prevent every issue from becoming a security inquiry.

The main critic of the securitization theory is that the analyst can never be neutral when discussing security, but the defender of this approach believes that this comment applies to all constructivist security theories.[44] The aim being to uncover the political choices of a securitizing actor, the analyst's agreement is thus irrelevant.

Using the securitization theory, this research has the ambition to establish the security character of the public problem in the European Union and the United-States, the commitments resulting from the collective acceptance of such a defined threat, and the particular policy created, in this case the EU-US Privacy Shield. To largely enlighten the different possibilities of characters given to the threat of data exchanges, the following subsection will highlight the transatlantic approaches to privacy, national security and national security of privacy.

Two Western Concepts of Privacy

Privacy has always been a political issue, well before the creation of the internet and its implication in the digital sphere. Its definition and understanding is disparate along with the different political and cultural beliefs that can be found in Europe and in North America. Along these lines, scholars have identified three concepts of privacy, the creation of knowledge, dignity and freedom[45]. The two last concepts are very relevant to the discussion of this paper and illustrate the contrast of actions held and threats felt by both the European Union and the United-States.

James Q. Whitman refers to the concepts of privacy as dignity as the continental privacy protection[46]. Europeans seem to defend the idea that privacy invasion is an offense against individual dignity.[47] Individuals living in society experience social norms as "essential

[43] Balzacq, Léonard, & Ruzicka, "'Securitization' revisited: theory and cases," 495
[44] Taureck, "Securitisation Theory and Securitisation Studies," 5
[45] Post, "Three concepts of privacy," 2088
[46] Whitman, "The two western cultures," 1161
[47] Post, "Three concepts of privacy," 2092

prerequisites" of their own identity and self-respect, therefore invading individuals' privacy, where they may not fall under those prerequisites, causes their harm[48]. This includes the right to one's image, name, reputation and self-determination[49]. Thus, by seeing their privacy as a cocoon which should be protected from the judgment of the public eye, europeans or continental privacy protectionists hold concerns and see danger about any agent gathering and diffusing information[50]. This view applies to the real and online world.

In the European Union, individual's privacy is considered a fundamental right[51]. It was incorporated into articles 7 & 8 of the 2000 charter of fundamental rights of the EU and binding all EU member states through the 2007 treaty of Lisbon. On this basis, processing of personal data is prohibited unless an explicit legal framework allows it[52] and european nations should only cooperate, thus transfer data, to countries complying to similar rules[53]. The European Union laws cover the full range of data protection rules[54], which is often portrayed as "Overreaching" by Americans scholars[55].

Contrary to the European view of privacy, Americans tend to have a presupposed set of differences, rather than mutuality[56]. Privacy as freedom or liberty define a space where social norms are suspended and not enforced[57]. It is often interpreted as liberty against the state, the right to freedom from instructions of the government[58]. In this conception, privacy is not the protection of an individual against the invasion of its dignity according to its social aspects, but of its independ and unique aspect of oneself.[59] Hence, one's individual privacy is held in its uniqueness it chooses to appear in society.

Under US laws, protection of personal information is decentralized and tailored, favoring unrestricted flow of data. The private sector is in the US, more regulated than the public sector,

[48] Ibid., 2094
[49] Whitman, "The two western cultures," 1161
[50] Ibid.
[51] Callahan-Slaughter, "Lipstick on a Pig," 243
[52] Weiss, & Archick, "U.S.-EU data privacy," 9
[53] Callahan-Slaughter, "Lipstick on a Pig," 243
[54] Zalnieriute, "Data Transfers after Schrems II," 15
[55] Callahan-Slaughter, "Lipstick on a Pig," 243
[56] Post, "Three concepts of privacy," 2095
[57] Ibid
[58] Whitman, "The two western cultures," 1162
[59] Post, "Three concepts of privacy," 2095

whereas regulation target both equally in Europe[60]. Inversely to the EU, collection and processing of data is only prohibited when it causes harm or is expressly limited by US Law[61]. In this case, rights to privacy only prevails for a citizen with a "reasonable expectation of privacy" and no longer exists when information is disclosed to a third party[62].

The continental privacy protection view supports the elimination of all differences by bringing individuals within a single normalized community, whereas privacy as freedom protects individuals autonomy by neutralizing the reach of that community[63]. When looking at US laws, there is a lack of personnel dignity norms that can be found in Europe, just as European laws do not contain many antistatic concerns that are very supported in the US[64]. Thus, the United-States, in the case of data transfers, prefers to self-regulate.[65]

The European Union and United-State do not share the same definition, view and law regarding privacy. The European Union provides a larger protection of individuals' right to privacy when it comes to data transfer within and across its borders, whereas the United-States tends to give more importance to free flow of data. This divergence must have an impact on national and international law upbringing, but may not be the only terms on which the nations do not agree upon. The following section will discuss the national security incentives across the regions.

National Security Narratives

To understand how national security impacts the view and conception of privacy in international agreement making, we must look at national security theories and incentives. States root their domestic politics from their national interests, institutions and ideas, which will thus define their international politics[66]. These may come in the form of economic interests, collective identity and culture, or the normative commitment of a nation. To limit a state's vulnerability to be attacked and to defend these interests, security policies are created and served to promote a

[60] Callahan-Slaughter, "Lipstick on a Pig," 244
[61] Weiss, & Archick, "U.S.-EU data privacy," 3
[62] Callahan-Slaughter, "Lipstick on a Pig," 244
[63] Ibid., 2099
[64] Whitman, "The two western cultures," 1163
[65] Zalnieriute, "Data Transfers after Schrems II," 15
[66] Krebs, "The politics of national security," 3

feeling of safety to the public.[67] Where the feeling of safety and the policies amended differs between regions like the European Union and the United-States, in such a way as privacy does.

National security cultures combine a mixture of the world-view of the external environment, national identity, instrumental preferences and interaction preferences[68]. To sustain the national security four types of governance policies can be implemented: assurance, as a post-conflict intervention; prevention, for pre-conflict interventions; protection, for internal security; and compellence, as military interventions.[69] And according to Kirchner and Sperling, there are three main threats to the stability for those policies, systemic on milieu goals of states, the legitimacy of state structures and national social cohesiveness and integrity.[70] The target of these menaces can be the state, directly, society or the milieu, while the protagonists can state or non-state actors. To extinguish the problem, there exists differ'ent instrument of conflicts, coercive and persuasive ones.[71]

In the case of the threat of data exchange, society is the target, as valuable information and process can be stored and distorted. Whereas the agent of the threats is the state, the United-states for the European Union which stored private information on its civilians. The instrument of conflict is in our case persuasive. Thus, the security system and threats against the state are indirect rather than direct, but the government is still trying to protect their national security by using persuasive defense through institutionalizing democratic norms.

In terms of theoretical background to apply to our region of research, we can see a dissonance of state behavior between the United-States and the European Union. The first seems to have a strong and rather older fashion way to preview the world and its threats, while the later have a more collusive protection system. Following the Westphalian state system, the United-States has a strong will to act as a gate-keeper between internal and external flows of people and information, with an avid control over its national territoriality and autonomy protected by technical and normative barriers. On the other hand, the European Union chose a Post-Westphalian state system to pursue its will for deeply-rooted relations within the region.

[67] Ibid., 6
[68] Kirchner, E. J., & Sperling, J. "National Security Cultures, " 9
[69] Ibid., 1
[70] Ibid., 5
[71] Ibid., 8

Loss of autonomy and mutual governance between states are maximized in order to meet common challenges to national welfare[72]. In these terms, the nature and volume of flows across national borders and the nature and height of the barriers to controlling those flows are commonly agreed amongst the nations.

Post-Westphalian states are incapable of meeting national security requirements alone, it is conditioned on collective goods.[73] To the contrary, westphalian states are able to reduce their security concerns by state-centric security calculus. Thus, the European Union requires a more complicated treatment of security problems, as states are, then, one agent and target of security threats.

The European Security Strategy (ESS) has the EU and its member cooperating to tackle security priorities within a multilateral institutions and the rule of law framework[74]. Efforts should be devoted though "effective multilateralism" against security threats. Poor governance, insecurity, poverty and conflict are the main barriers to achieving these goals. Thus, European states shall remain unhesitant and undivided to a stable regional security community and respond to threats by displaying a range of diplomatic, development, humanitarian and military instruments.[75]

The United-States National Security Strategy (USNSS) mentions a similar broad understanding of security problems and multilateral commitments to meeting such challenges, but to the difference that the US can act unilaterally under a concept of pre-emption with rogue states and military power.[76] The government rarely expressed a clear definition of national security but expressed the idea that it is beheld in the foreign relations to the US, the threats to the US, its people, property or interests, and any other matter bearing on US national homeland security.[77] And to maintain national defense, according to the Federal Information Security Management Act of 2002, intelligence and cryptologic activities related to national security, military forces and equipments can be operated and used to achieve such goals[78]. As Donohue explains in the *Limits of National Security,* the external components of the US national security

[72] Kirchner, E. J., & Sperling, J. "National Security Cultures, " 2
[73] Ibid., 4
[74] Quille, G. "The European Security Strategy," 422
[75] Ibid., 423-424
[76] Ibid.
[77] Donohue, L. K. "The limits of national security," 1580
[78] Ibid., 1581

are not the only element to govern decisions on such a topic. Political institutions influenced by domestic and international concerns protect the institutions' ability to act with purpose[79].

There is a clear difference in national security narratives between the two regions. The unilaterality of governmental actions in the matter of national security allows the United-States to have a grander autonomy and sovereignty compared to the multilateral framework prescribed by the European Union to defend national interests. Having clarified the diverging views of the EU and the US in terms of privacy and national security, we will look at the national security issue of privacy.

National Security Issues of Privacy

The issue of privacy in the digital world debate started long ago, at the very premise of the birth of the internet. The discussions have a long standing history, but show an evolution and split between the European Union's and the United-States' beliefs. This section looks at the concept of national security issue of privacy from the impact of the data flow agreements on the two regions to the American view on the EU decisions to invalidate the accord, while the previous two sections can be used as a knowledge spectrum of privacy and national security.

National security issues to privacy include the use of technologies to protect citizens and prevent, respond, to security threats. And its main burden is the balance between protection of individuals' privacy and state's practices to assure national security. If we look at Europe's view of privacy, then the EU governments aim at restricting the flow of information to protect their citizens' dignity from the misuse and over access of their information by government and companies. The restriction of data exchange does protect the population's privacy, but also negatively impacts the economic growth, productivity and innovation of the region.[80] Whereas large government control and retention of information access on their citizens, such as the US surveillance programs, lead to restriction and risk to individual's privacy rights.[81] Europe may withhold economic growth by protecting citizens from over-reaching their privacy, while the US may reduce individuals' right to privacy for national security purposes. Both restriction and free

[79] Ibid., 1585
[80] Aaronson, "Why Trade Agreements are not Setting Information Free," 688
[81] Aaronson, "Why Trade Agreements are not Setting Information Free," 688

flow of information seem to have downfalls, it is therefore a political national preference to choose one over the other.

The terrorist attacks of September 11, grandly impacted nations across the world in their view of national security and the use of technologies as a tool to massacre. States' economic power was now seen as a great tool to take advantage of the digital technologies' vulnerabilities and transform them into electronic surveillance tools[82]. Along with this approach, online surveillance was asserted as a way to prevent threats to their civilians[83].

Following the event, the European Data Protection Derivative (DPD), now, obliged telecommunication and internet services providers to retain traffic and location data for a period from 6 months to no more than 2 years[84]. These information should be made available upon request to law enforcement authorities for the purpose of an investigation, detection and prosecution of serious crime and terrorism. It was later invalidated by the CJEU on the basis of unjustified interferences with fundamental rights to privacy, as it was interfering beyond satisfying public security. Thus, legislation allowing access to content of electronic communication to public authorities must be regarded as compromising fundamental rights to private life and be abolished.[85]

To make it even more challenging for the European Union, national security is decided at the national level, where each state has sovereignty on their security approach, whereas data protection and human rights are both discussed at national and EU level. Other issues, such as trade are brought up at the EU level. This layering of power can cause an issue when discussing data transfer, which includes topics that are regarded by multiple parts of the institutions at different levels, making it even more difficult to develop and agree on terms.

As a way to harmonize the regulations for all EU members, the General Data Protection Regulation (GDPR) was introduced in 2018. Its aim is to protect individuals' information from being processed by the private and public sector. It also gives directives on law-enforcement and power to national data protection authorities to rule.

[82] Nesterova, "Crisis of Privacy and Sacrifice," 4
[83] Aaronson, "Why Trade Agreements are not Setting Information Free," 686
[84] Nesterova, "Crisis of Privacy and Sacrifice," 4
[85] Ibid.

On the other side of the Atlantic ocean, the United States comes to have a similar layering issue, where businesses are regulated by states and the federal government. Trade, human rights and national security are brought up by the legislative and executive branches. In a country that counts 50 jurisdictions where different regimes apply, it becomes easily difficult to regulate and watch out for the compliance to data protection standards.

The US foreign intelligence surveillance act (FISA) took action in 1978 and focuses on the ruling of government's collection of foreign intelligence information for the purpose of advancing US counterintelligence goals[86]. The National Security Strategy of the United-States of America states that cyberthreats abilities state and non-state actors to interfere in campaigns against the political, economic and security interests of the nation[87]. Priority actions such as identifying and prioritizing risks and defensible government network, improving information sharing and sensing, and deploying layered defenses should be used to counter these threats[88]. Degli Esposti et al. believe that it is the lack of public participation in the decision making process that impact the negative opinion on these practices[89]. Mass surveillance through digital technologies has become a cheap and convenient routine, whereas it was previously a consuming and expensive activity.[90] And thereby has created a stronger asymmetry of power between citizens and the state.

The European Union seems to have an evolution in terms of national security over privacy, whereas the United-states has been consistent with its strong national incentives. They also both have different and complex institutional systems that overlook the issue of data protection. The European Union sees privacy as a human right and as a consumer right which therefore should be protected by governments. Whereas online privacy only falls under consumer rights in US law and therefore should be overviewed by the Federal Trade Commission (FTC).[91] These different elements make the realization and implementation of a common data flow agreement even more challenging.

[86] Zalnieriute, “Data Transfers after Schrems II,” 18
[87] Renshaw, P. “The United States of America,” 12
[88] ibid.
[89] Degli Esposti, Pavone, & Santiago-Gómez, “Aligning security and privacy,” 74
[90] Ibid., 73
[91] Aaronson, “Why Trade Agreements are not Setting Information Free,” 682

The difference of institutional systems between the European Union and the United States can be seen as another throwback in the negotiations of transatlantic data transfers. When two entities have different regulatory mechanisms then the process to create a common accord may be long and tedious. On one hand, the multileveled European and national institutions in the EU, on the other, the US state, federal and legislative branches have to coordinate in and within the two regions to agree on such an agreement.

Zalnieriute explains well the transition from the Safe Harbor agreement, where national security was processed as an exception, to the Privacy Shield where it became the rule[92]. US laws and undertakings, as well as US national security, public interest and law enforcement requirements disregard and have priority over Safe Harbor principles[93]. In such, in the United-States, national security prevails over individuals' right to privacy as seen by the EU and could not be tolerated. The agreement was, then, invalidated.

This shift was seen as a victory by the European Parliament and Europeans, whereas in the US it was drawn as an "overreach" of the EU into US law[94]. Many scholars even declared it as hypocritical, since the Court of Justice of the European Union (CJEU) has no right to examine EU member states' national security policies, how could they declare the US national security framework as "inadequate".[95]

This discordance of approach in privacy, national security and national security of privacy have greatly impacted the making-process of the EU-US data flow agreement. Aaronson believes that EU-US policymakers did not put effort to agree on promoting free flow information while protecting digital rights and freedom.[96] At national level, coordination of trade policymakers and other policymakers did not promote privacy rights and national security, while at international level, governments did not agree on the legitimate efforts that should be conducted to restrict information flows[97]. Aaronson even believes that US policymakers have not learned from past negotiations to encourage data flow, while understanding the importance to individuals' right to privacy, in such a way that many governments have failed to respect human rights and policy priorities, by using surveillance mechanisms.[98]

[92] Zalnieriute, "Data Transfers after Schrems II," 32
[93] Weiss, & Archick, "U.S.-EU data privacy," 7
[94] Ibid., 37
[95] Ibid., 39
[96] Aaronson, "Why Trade Agreements are not Setting Information Free," 673-674
[97] Ibid.
[98] Ibid., 687

These subsections have highlighted the different privacy and national security incentives of the European Union and the United-States and try to look more in detail where they intersect in the national security issue of privacy. The complex legal frameworks involved in the regulation of the data exchanges were also involved in the aim to uncover the institutional element. Thus, from these different elements we can disting two approaches to privacy, national security and the national security issue to privacy, which are components of the securitization of the data exchange agreements. Following the study of this complex puzzle, we are able to identify two hypotheses.

First, we assume that the European Union, through its privacy as dignity belief, will define non-regulated data exchange as a threat to individuals' privacy rights. US companies and government are being depicted as the referent subject. And the policy that should be implemented is a strong, necessary data flow agreement.

> H_1: *The European Union identifies corporate and governmental data processing as a threat to individual privacy, making right to privacy a necessity to protect in cross-border flow.*

Second, we suspect the United-States to allocate foreign data, personal information of EU citizens, as a threat to national security. The entity threatening is portrayed to be the individual rather than a state, and the policies used would be unrestricted flow of data and governmental surveillance.

> H_2: *The United-States classifies individuals as a threat to national security, thus governmental processing of personal data is essential.*

This research aims at understanding how the securitization of data exchanges have led to the systematic failure of EU-US privacy agreements. We, therefore, assume that the securitizing actors, which are the states, have depicted a different portrait of the threat of data exchanges, with that peculiar entity as the perpetrator and casualty of such threat. The following sections lays out the methodology applied to this qualitative research, with the aim of verifying these above hypotheses.

Methodology

This research will be based on the case studies of discourses exchanged between the United states and the European Union on the topic of data protection and transatlantic information flow. The speeches were given by different commissioners at the Federal Trade Commission, for the United State study, whereas for the European Union, it is a collection of allocutions of high end representatives, such as vice-president of the Commission or Commissioners. All the documents were extracted from the White house and the European Commission archives and cover a decade of negotiation.

Discourse analysis was chosen as the main method for this research on the basis that "a discourse does not simply describe a reality that already exists, but constructs the representation of reality that the speaker wishes to share"[99]. The previous sections show the many differences in terms of definition and institutions between the two regions studied, as well as a long difficult history of data transfer agreement making. Analyzing speeches held in this context will allow us to better identify the place of national security in the play of these agreements making. Also, we will be on the lookout for the so-called "speech acts", that are used by political actors to promote security and assert vulnerability in security or insecurity discourses in the aim to shape the political terrain[100]. In such, the specificities of political discourse analysis is to search for and define the connection between discourse structure and political context structure[101].

There exists three types of discourses, demonstrative, exhibitory and dialogic[102]. The first is logical and contains many connecting words and reasoning procedures. Exhibitory discourses usually promote one or multiple thesis that are supported by emphasis statement, reasoning procedure and informative content. Last, dialogic speeches confront the thesis in a dialogue form. In this research, we expect the two last one to be represented in our collection of discourses, since argumentative discourses implicitly reveals the two poles of the exchange by inscribing the representation of the addresses and the speaker in its statement[103], which will help

[99] Seignour, "Méthode d'analyse des discours," 31
[100] Krebs, "The politics of national security," 6
[101] van Dijk, "What is Political Discourse Analysis," 24
[102] Seignour, "Méthode d'analyse des discours," 31
[103] Ibid.

us determine the role of each player. In such the meaning of an allocation can be analyzed in terms of the particular form of discourses within the context of the particular practices in which the discourse is produced[104].

The type of discourses is not the only important factor of a speech, the speaker is also an important element. Therefore, its intentions whether they fall under ethos, the quality of the speaker, pathos, the emotions created, or logos, the logical argumentation, addressing the reason and designed to prove, should be defined and determine the aim for which the discourse is used and in what aim[105]. Elements such as the speech structure also have meaning to which they are arranged, chronologically, by theme, oppositional,... The last factor into the speaker's work is the elocution. The discourse figure, words, thoughts, the intensity and enunciation are also used to impact the audience and should be looked into. Although, we may also believe that political discourses may be constrained to certain set of rules under which they must comply to follow "official language"[106].

The following parts of this section will discuss the methodology held in the decision of which discourses should be used, then we will look into the operationalisation of the different concepts for our analysis, before discussing the limitation of this method.

Discourses Analysis

Discourses are issued every year on multiple topics by different high placed governmental officials, therefore to have a certain consistency in the speeches chosen, we decided to use two sources, one for each region. All the documents for the European Union are extracted out of the European Commission online libraries and archives[107], while the Federal Trade Commission public statements' archives[108] were the primary sources for American speeches.

For a similar purpose of consistency over the two regions, equivalent positions were regarded for the speakers. High-end governmental officials were seen as a perfect representation

[104] Lasswe, "discourse analysis and the study," 62
[105] Ibid., 33
[106] van Dijk, "What is Political Discourse Analysis," 24
[107] https://commission.europa.eu/about-european-commission/visit-european-commission/libraries-and-archives_en
[108] https://www.ftc.gov/public-statements

of the institutions' decisions and opinions on the topic. Thus, for the European Union, commissioners and Vice-president of the European Commissionns were decided as goof perpetrators of the discourses. Similarly, commissioners and chair(wo)men were picked to represent the evolution of the discourses of the Federal Trade Commission.

The third element of consistency between the discourses of European Union and United-states were the years in which they were held. They ranged from 2012 to 2022, a decade. Having an overview of this period of time will help understanding the evolution of the narrative for the two perspectives. Also, discourses held before and after the different agreements are essential to analyze the evolution in terms of incentives that has helped shape the international decisions.

Thus, to have a larger understanding of this transformation, if there is one, we will discuss three different angles. First, a case study will be held for the particular case of the European Union views of the topic, before looking into the United-state case. For these two independent case studies, 12 speeches will be analyzed, 6 each. Last, we will discuss the implications of the EU-US relations and discussions of the data flows within the two parties. This case study will discuss 6 other discourses, half held by each party.The dissemination of analysis in these three parts will help us have a larger understanding of how the national incentives have shaped the international discussion. In such, understanding the national evolution will help to explain the international evolution.

Aftermost, the discourses were picked on the basis of topic. Thus, they discussed issues related to privacy and data protection as their main theme.

Operationalization

As discussed in the previous section, the analysis will be separated into three parts, the European view of the issue, the American side, before discussing the EU-US relationship. The three case studies will use the same baseline of analysis. This aims at having a consistency in terms of results. The analysis will be held in the form of a reading grid constructed around three main sections, context, structure and summary of terms.

To help with the analysis, reading tabs are very often used as a tool to record the different parts of the speech, its goal, its context, its construction of a representation of the real and its

persuasive target markers[109]. To understand the discourse there is a need to dissect its structure and its meaning, but to do so it is important to have an understanding of what is the aim of this speech, what is the context in which it is told, how it represents the perspective of one or multiple players and who are the targets and how are they aimed at. Thus, the methodological analysis must be based on three different steps, the enunciation system, the referential and argumentative indicators.

In this research, the context of each discourse will help define the timeline of the EU US data flow agreements within and between the case studies. The elements looked for in this section are the date of the speech, the speaker, the audience meant to be addressed to, in which step of the agreement is held (Safe Harbor, in between agreements,...) and last the goal it aims to deliver (ethos, pathos, logos). In such, we will analyze the nature of arguments. Are they part of ethos, pathos, or logos? The goal of this step is to frame particular patterns that may be found in the discourse. This first section is designed to show the relation between the speaker and its audience, as well as the context in which the discourse is held.

Second, the utterance system looks at the way the speaker and audience are shown in the discourse, through the use of personal pronouns, demonstratives, and spatio-temporal nouns, but also the degree of adhesion of the speaker, through adverbs, italic, quotation marks, the use of conditional,... The last step will be to study the verbs. Are they action verbs, or declarative, performative,...? We will also look into the referential indicators, the main semantic field. The set of words that were used to characterize a concept, an activity, a person,... Thus, this section will list the connecting and logical words, the verbs of action and the lexical field of each discourse. Looking into the wording of the speeches aims to understand the tone and goal of the speaker, whether it is to convey emotions or factual information. It is an important step to connect the context to the summary of terms and therefore show by which form the message is transmitted.

The last step of our analysis will be to describe the argumentative indicators, which look into the nature and structure of arguments. In this research, we will aim to see how the three terms, privacy, national security and national security of privacy, appear in each discourse. Privacy will then be looked for as a definition, national security as a phenomenon and the national security of privacy as the limit or success of international data flow. This section will

[109] Seignour, “Méthode d’analyse des discours,” 31

summarize and extract the information provided in the speeches and will be regarded as the opinion to be conveyed by the speaker to its audience.

Limitations

Although this research aims to be consistent in the terms defined and looked for, privacy, national security and national security of privacy, they may not appear in each speech as hoped for, as well as other terms may as well be important in the discussion but have been disregarded in this research.

Also the discourses chosen were decided, as previously described, but other speeches that could be more or as important and meaningful have not fallen into the appropriate categories and were therefore disregarded. In such, other speeches may have shown different or similar results to the one of this research.

Analysis and Evaluation

Case Study: The European Union

Case Study: The United-States

National Security & the EU-US Privacy Shield

Conclusion

References

Aaronson, S. A. (2019). What are we talking about when we talk about digital protectionism? *World Trade Review*, *18*(4), 541–577. https://doi.org/10.1017/S1474745618000198

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*, *14*(4), 671–700. https://doi.org/10.1017/S1474745615000014

Aaronson, S. A., Maxim, R., & July, I. (2013). Data Protection and Digital Trade in the Wake of the NSA Revelations. *Intereconomics*, *48*(July), 281–285.

Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2011). Privacy and National Security Issues in Social Networks : The Challenges. *International Journal of the Computer, the Internet and Management*, *19*(3), 14–20.

Aden, H. (2018). Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union. *West European Politics*, *41*(4), 981–1002. https://doi.org/10.1080/01402382.2018.1475613

Bailey, M. a, Goldstein, J., & Weingast, B. R. (2013). All use subject to JSTOR Terms and Conditions THE INSTITUTIONAL TRADE ROOTS OF POLICY Politics , Coalitions , and International Trade. *World Politics*, *49*(3), 309–338.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations*, *30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Biscop, S. (2016). The European Security Strategy. *The European Security Strategy*. https://doi.org/10.4324/9781315239835

Callahan-Slaughter, A. (2016). Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States. *Tulane Journal of International & Comparative Law*, *25*(1), 239–258. https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=120269636&site=ehost-live

Cavelty Dr., M. D. (2008). Cyber-terror-looming threat or Phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology and Politics*, *4*(1), 19–36. https://doi.org/10.1300/J516v04n01_03

Degli Esposti, S., Pavone, V., & Santiago-Gómez, E. (2017). Aligning security and privacy: The case of Deep Packet Inspection. In *Surveillance, Privacy and Security* (pp. 71-90). Routledge.

Donohue, L. K. (2011). The limits of national security. American Criminal Law Review , 48(4), 1573-1756.

Fahey, E., & Terpan, F. (2021). Torn between institutionalisation & judicialisation: The demise of the eu-us privacy shield. *Indiana Journal of Global Legal Studies*, *28*(2), 205–244. https://doi.org/10.2979/INDJGLOLEGSTU.28.2.0205

Friedewald, M., Burgess, J. P., Bellanova, R., & Peissl, W. (2017). *Surveillance , Privacy and Security*.

Gregory Voss, B. W., Kim Phan, B., & Patel U R N, R. J. (1995). *I NTERNET LAW M AY 2 0 1 6 The Future of Transatlantic Data Flows: Privacy Shield or Bust? THE FUTURE OF TRANSATLANTIC DATA FLOWS: PRIVACY SHIELD OR BUST?.. .. .. .. .1 A L O F*. http://ssrn.com/abstract=2794261

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2019). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 5027–5033. https://doi.org/10.1109/BigData.2018.8622621

Guertner, G. L. (2007). European Views of Preemption in US National Security Strategy. *The US Army War College Quarterly: Parameters*, *37*(2). https://doi.org/10.55540/0031-1723.2354

Kirchner, E. J., & Sperling, J. (2010). National Security Cultures. In *National Security Cultures*. https://doi.org/10.4324/9780203850619

Krebs, R. R. (2018). The politics of national security. *The Oxford Handbook of International Security*, *May*, 259–273. https://doi.org/10.1093/oxfordhb/9780198777854.013.42

Lasswe, Y., & Schoo, L. (n.d.). *discourse analysis and the study of policy making maarten hajer*.

Linn, E. (2017). A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement. *Vanderbilt Journal of Transnational Law*, *50*(5).

Mansfield, E. D., & Rudra, N. (2021). Embedded Liberalism in the Digital Era. *International Organization*, *75*(2), 558–585. https://doi.org/10.1017/S0020818320000569

Nesterova, I. (2016). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: the CJEU Rulings Strengthening EU Data Protection Standards. *11*, 8–10.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*(2), 61–73. https://doi.org/10.1007/s10676-005-4582-3

NOYB, (2020). CJEU invalidates “Privacy Shield” in US Surveillance case. SCCs *cannot* be used by Facebook and similar companies. CJEU Judgment. https://noyb.eu/en/cjeu

NOYB, (2022). "Privacy Shield 2.0"? - First Reaction by Max Schrems. https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

O’Rourke, C., & Kerr, A. (2017). Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers. *Westminster Papers in Communication and Culture*, *12*(3), 21–36. https://doi.org/10.16997/wpcc.264

Page, V., Virginia, B., & Fortna, P. (2015). *All use subject to JSTOR Terms and Conditions Causal Mechanisms Effects*. *56*(4), 481–519.

Post, R. C. (2001). Three concepts of privacy. Georgetown Law Journal, 89(6), 2087-2098.

Putnam, R. D. (1988). Diplomacy and domestic politics: The logic of two-level games. In *International Organization*(Vol. 42, Issue 3). https://doi.org/10.1017/S0020818300027697

Quille, G. (2004). The european security strategy: A framework for EU security interests? *International Peacekeeping*, *11*(3), 422–438. https://doi.org/10.1080/1353331042000249028

Renshaw, P. (2014). The United States of America. *The Working Class and Politics in Europe and America, 1929-1945*, 241–272. https://doi.org/10.5040/9781350221796.ch-005

Shaffer, G. (2000). Globalization and social protection: the impact of eu and international rules in the ratcheting up of u.s. privacy standards. Yale Journal of International Law, 25(1), 1-88.

Seignour, A. (2011). Méthode d’analyse des discours: L’exemple de l’allocution d’un dirigeant d’entreprise publique. *Revue Francaise de Gestion*, *211*(2), 29–45. https://doi.org/10.3166/RFG.211.29-45

Svantesson, D. J. B. (2013). A “layered approach” to the extraterritoriality of data privacy laws. *International Data Privacy Law*, *3*(4), 278–286. https://doi.org/10.1093/idpl/ipt027

Tourkochoriti, I. (2014). The transatlantic flow of data and the national security exception in the european data privacy regulation: in search for legal protection against surveillance. University of Pennsylvania Journal of International Law, 36(2), 459-524.

Tracol, X. (2016). EU–U.S. Privacy Shield: The saga continues. *Computer Law and Security Review*, *32*(5), 775–777. https://doi.org/10.1016/j.clsr.2016.07.013

van Dijk, T. A. (1997). What is Political Discourse Analysis? *Belgian Journal of Linguistics*, *11*, 11–52. https://doi.org/10.1075/bjl.11.03dij

Vermeulen, G. (2018). The Paper Shield: On the Degree of Protection of the EU–US Privacy Shield against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services. *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, *22*(2007), 127–148. https://doi.org/10.1017/9781780685786.007

Vosst, W. G. (2020). *AND DATA GOVERNANCE*.

Wæver, O. (2011). Politics, security, theory. *Security Dialogue*, *42*(4–5), 465–480. https://doi.org/10.1177/0967010611418718

Weiss, M. A., & Archick, K. (2016). U.S.-EU data privacy: From safe harbor to privacy shield. *The European Union: Challenges and Prospects*, 113–135.

Whitman, J. Q. (2004). The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*(6), 1151–1221. https://doi.org/10.2307/4135723

Wiwit, S. (2015). Metadata, citation and similar papers at core.ac.uk 4. *Донну*, *5*(December), 118–138.

Zalnieriute, M. (2022). Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security. *Alexander Trechsel VANDERBILT JOURNAL OF TRANSNATIONAL LAW*, *55*, 1041.

Data Sources & Discourses

European Commission. Libraries and Archives. https://commission.europa.eu/about-european-commission/visit-european-commission/libraries-and-archives_en

Federal Trade Commission. Public Statements. https://www.ftc.gov/public-statements

Annexes