TORN BETWEEN INSTITUTIONALISATION AND JUDICIALISATION: THE DEMISE OF THE EU-US PRIVACY SHIELD

Working Paper: *Forthcoming in the Indiana Journal of Global Legal Studies 2021*

Elaine Fahey[*] *& Fabien Terpan*[**]

A. Introduction

In July 2016, the EU-US Privacy Shield came into force replacing the Safe Harbour "agreement", to address the concerns around data collection and privacy that arose in the case of *Schrems v. European Data Commissioner* (C-362/14) after Edward Snowden's revelations on the NSA's surveillance programs.[1] The latter have spurred the development of several instruments and enforcement regimes, such as the General Data Protection Regulation (GDPR)[2] adopted in April 2016, and the EU-US Umbrella Agreement on the "protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences" [3], concluded in December 2016. These two acts, as well as the Privacy Shield, were significant global data transfer instruments on account of their enormous regulatory reach across the Atlantic at least until July 2020 when the Privacy Shield was struck down. Most commentators agreed that the implementation of the EU-US Privacy Shield raised serious legal concerns in terms of rights and obligations. Not surprisingly, actions for annulment were brought before the General Court of the CJEU against the EU-US Privacy Shield (T-670/16 and T-738/16, pending), and preliminary references were initiated culminating in a recent CJEU judgment (C-311/18) invalidating it.

This article analyses the implementation and eventual demise of the Privacy Shield from the perspective of EU law based on a framework combining the dynamic between two concepts at the heart of the evolution of the EU legal order: 'institutionalisation' and 'judicialisation'. This conceptual framework allows us to capture the relationship between EU and US legal orders and better understand why it is sometimes harmonious, sometimes disharmonious.

Institutionalisation is defined here as the process by which an organisation becomes increasingly subject to rules, procedures and stable practices. [4] Informal institutionalisation is based on practices and other informal mechanisms while formal institutionalisation is based on law and other formal rules and norms. From a legal perspective, we argue institutionalisation is weak when only based on informal and imprecise rules and stronger when it includes formal and precise rules. Judicialisation is understood here as focusing on the more and more central role played by courts in political systems, in particular as to the EU.[5] The more the involvement and impact of courts and tribunals, the more the judicialisation. Applied to the legal relationship between legal orders, judicialisation can be *positive* when it guarantees the correct functioning of an existing system of relationship : courts, then, ensure that common rules are correctly implemented by every actor. Judicialisation can also be *negative* when it challenges the system itself through conflicts of law, extra-territorial judgements or invalidation of legal commitments. We do not argue that either positive or negative judicialisation is bad per se or undesirable since both perform valuable roles. Rather, we indentify the interaction between institutionalisation and judicialisation as a causal dynamic, where one may result in the other and be accordingly of significance more broadly for understanding legal frameworks.

We argue thus that the link between institutionalisation and judicialisation is well suited to explaining the consequences of EU international relations (IR) powers, in an area like data protection and privacy where the

[*] Jean Monnet Chair in Law & Transatlantic Relations, Institute for the Study of European Law, City Law School, City, University of London
[**] Jean Monnet Chair in EU Law & Politics, University Grenoble Alpes, Sciences Po Grenoble, CESICE.
We would like to thank Paul James Cardwell, Isabella Mancini, Pola Cebulak, Florian Trauner and Jed Odermatt, for their valuable comments at the conference organized by the Council of European Studies, Madrid 2019 and Ivanka Karaivanova for research assistance.
[1] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.
[2] Regulation 2016/679 of the European Parliament and the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU).
[3] Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016 O.J. (L 336) 3.
[4] See ELAINE FAHEY, INSTITUTIONALISATION BEYOND THE STATE, Ch. 1 (2017); JOSÉ E ALVAREZ, THE IMPACT OF INTERNATIONAL ORGANIZATIONS ON INTERNATIONAL LAW (2016); Fabien Terpan, *Soft Law in the European Union-The Changing Nature of EU Law*, 21 EUROPEAN L.J. 68 (2014).
[5] E.g. Ninke Mussche & Dries Lens, *The ECJ's Construction of an EU Mobility Regime-Judicialisation and the Posting of Third-country Nationals,* 57 J. COMM. MKT. STUD. 1247 (2019).

degree of protection afforded by the US and the EU is very different, with EU law being far more protective than US law. Within the framework of EU international relations in the field of data transfer, our hypothesis is that because institutionalisation is weak or informal, negative judicialisation is more likely, with courts and tribunals of the most protective legal order –in the end the CJEU- are prone to make their own rules prevail. A lack of a robust framework is thus highly consequential. In turn, positive judicialisation is more likely when the institutionalisation is strong, or strongly formalised, because risks of conflicts between legal orders are reduced and common rules guarantee a harmonious relationship between legal orders: which courts and tribunals then do not challenge these rules but rather ensure that they are correctly implemented. The EU and third states commit themselves both through formal agreements and soft law arrangements. The latter are potentially weak forms of institutionalisation due to the lack of clarity and serious commitments. These weaknesses must be strongly alleviated if the soft law arrangement is to escape negative judicialisation. The former are more formalised forms of institutionalisation. However, formal agreements can also suffer from weak institutionalisation for various reasons such as the incompetence of the concluding institution, an incorrect legal basis or substantial deficiencies. In many cases, EU IR agreements are subjected to positive rather than negative judicialisation but the 'invalidation' of an IR agreement is possible when its weak institutionalisation is challenged before the Court. We are not thus concerned with judicalisation per se to be problematic but rather with the broader framework within which rules are embedded, namely institutionalisation, and its judicial construction and analysis through judicial review.

Following from this, using the casestudy of the Privacy Shield and its evolution from Safe Harbour, we argue that the Safe Harbour agreement was poorly institutionalised, and suffered legal weaknesses that led to its inevitable invalidation by the CJEU.[6] Negative judicialisation has then triggered the adoption of the Privacy Shield, which was presented as a strengthened and more institutionalised version of the Safe Harbour but which was in reality mostly weakly institutionalised masked by new terminology, some enhanced governance but little else.[7] We will show how after three years of annual reviews and governance, weak institutionalisation was particularly apparent. Key forms of institutional actors evolve late in the process, certain key actors lack complete independence and 'guarantees' provided appear vague and declaratory, rendering the overall institutional framework less than robust. The implementation of the Privacy Shield has opened a new dynamic between institutionalisation and judicialisation that we propose to examine in the following sections. We argue that the thesis may apply to other EU international data transfer regimes that have been and continue to be the subject of weak institutionalisation and increasing judicialisation. It is thus an important dynamic to study.

We will firstly, present the theoretical framework based on the notions of institutionalisation and judicialisation. Then we will move to the empirical analysis and make a brief presentation of the evolution from the Safe Harbour to the Privacy Shield, before assessing both the institutionalisation and the judicialisation of the Privacy Shield.

B. Theoretical Framework: on Institutionalisation and Judicialisation

I. Institutionalisation

There is no innately shared understanding of institutionalisation across disciplines, either those focussed upon law and governance in the Nation State, or beyond the Nation State. Institutionalisation is often regarded as the ultimate antidote to concerns about law-making beyond the Nation State.[8] To others, however, it is a horror-show of over-regulation, interference and an unnecessary reaction against informal governance.[9] In most scholarship, however, organisations that incorporate 'institutionalised' practices, ideals or systems are understood to be more legitimate and likely to succeed.[10]

[6] Case C-362/14, Schrems v. Data Commissioner, EU:C:2015:650.
[7] Fabien Terpan, *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One*?, 3 J.L. & INTEGR. 1045 (2018).
[8] See Elaine Fahey, *Introduction* to INSTITUTIONALISATION BEYOND THE NATION STATE (Elaine Fahey ed., 2018).
[9] See Paul M Schwartz, *The EU–US Privacy Collision: a Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).
[10] John Meyer & Brian Rowan, *Institutionalized Organizations: Formal Structure as Myth and Ceremony,* 83 AM. J. SOC. 340, 363 (1977); Elizabeth Sanders, *Historical Institutionalism*, in THE OXFORD HANDBOOK OF POLITICAL INSTITUTIONS 40 (Sarah Binder et al. eds., 2008).

In European studies, 'institutionalism' -in its old and new forms- is one of the main grand theories of EU integration, focussing on the way formal and informal institutions trigger integration in the long term.[11] The density of institutionalised regimes is high in the EU in comparison with many other regions globally.[12] EU institutionalisation has been conventionally understood as the formalisation and stabilisation of both procedures and institutional coordination, and the ability of individual actors to influence institutional development and has also been widely studied in the field of external relations.[13] While the EU has a recent history of promoting global multilateral institutions, from the International Criminal Court, a Multilateral Investment Court, to WTO reform, some allege 'partial' institutionalisation is said to be at the root of many internal EU policy crises, from the euro to migration- although without a legally exact understanding thereof.[14] Institutionalisation has its origins in IR literature, analysing the evolution of EU powers, actors and architectures. Institutionalisation literature notably has a history of studying weakly institutionalised regimes with limited powers involving soft law, historically very limited litigation and limited fundamental rights challenges.

Today, however, many still pay insufficient attention to legal aspects of institutionalisation, e.g. shifts in legal autonomy, rule-making powers, competences or the 'hardening' of soft law. In EU IR law this is particularly legally salient. The latter may be significant triggering formal institutionalisation from informal or partial institutionalisation. We consider that the legal aspects of institutionalisation is crucial, especially in IR systems like the EU-US system of data transfer with mostly informal rules where judicialisation is likely. One of the most salient features of transatlantic relations according to scholars has been an agreement as to its historic non-institutionalisation.[15] This is principally because formal bilateral transatlantic relations have long been conducted through a network of informal transatlantic dialogues and non-institutional actors.[16] Such policy frameworks are not formally binding agreements. It is widely agreed that many transatlantic agreements have been doomed to failure through non-institutionalisation, non-compliance, i.e. plagued with sub-optimal remedies and a lack of accountability.[17] This makes their transformation in data transfer agreements crucial to be studied, subject to more institutionalisation and judicialisation.

II. Judicialisation

Judicialisation can be defined as the "reliance on courts and judicial means for addressing core moral predicaments, public policy questions, and political controversies".[18] If we see this concept as describing an evolution rather than a static situation, then, for judicialisation to occur, there must be a growing tendency to rely on courts and judicial means in a given political system, as well as a tendency for these courts to actively exert its judicial control. This is precisely what has been analysed by a wide range of scholars applying the notion to different national political systems like the United States, Japan or Germany,[19] as well as to different legal fields like trade, environment or security.[20] Processes of judicialisation have also been observed at regional[21] and international level, [22] with several courts emerging and playing an increasing role in public policy-making. There is a broad scholarship on 'juristocracy' and the rise of judicial authority beyond the State in light of the emerging

[11] Peter A Hall & Rosemary C Taylor, *Political Science and the Three New Institutionalisms*, 44 POLIT. STUD. 936 (1996); THE INSTITUTIONALIZATION OF EUROPE (Alec Stone Sweet et al. eds., 2001).

[12] CRISIS AND INSTITUTIONAL CHANGE IN REGIONAL INTEGRATION (Sabine Saurugger & Fabian Terpan eds., 2016).

[13] Petar Petrov, *Early Institutionalisation of the ESDP Governance Arrangements: Insights from the Operations Concordia and Artemis* in UNDERSTANDING THE ROLE OF BUREAUCRACY IN THE EUROPEAN SECURITY AND DEFENCE POLICY (Sophie Vanhoonacker et al. eds., 2010); MICHAEL SMITH, EUROPE'S FOREIGN AND SECURITY POLICY: THE INSTITUTIONALISATION OF COOPERATION (2004).

[14] James A Caporaso, *Europe's Triple Crisis and the Uneven Role of Institutions*, 56 J. COMMON MARK. STUD. 1345 (2018).

[15] Mark Pollack, *The New Transatlantic Agenda at Ten: Reflections in an experiment in International Governance*, 43 J. COMM. MKT. STUD. 899 (2005).

[16] TRANSATLANTIC GOVERNANCE IN THE GLOBAL ECONOMY 25-34, 298 (Mark Pollack & Gregory Shaffer eds., 2001)

[17] See MARK POLLACK & GREGORY SHAFFER, WHEN COOPERATION FAILS: THE INTERNATIONAL LAW AND POLITICS OF GENETICALLY MODIFIED FOODS (2009); A TRANSATLANTIC COMMUNITY OF LAW (Elaine Fahey & Deirdre Curtin eds., 2014).

[18] Ran Hirschl, *The Judicialisation of Politics*, in THE OXFORD HANDBOOK OF LAW AND POLITICS (Gregory A. Caldeira et al. eds., 2018).

[19] Tokujin Matsudaira, *Judicialisation of Politics and the Japanese Supreme Court*, 88 WASH. UL REV. 1559 (2010): Christine Landfried. *The Judicialisation of Politics in Germany*, 15 INT'L POL. SCIENCE REV. 113 (1994).

[20] Aletta Mondré et al., *Uneven Judicialisation: Comparing International Dispute Settlement in Security, Trade, and the Environment,* 4 NEW GLOBAL STUDIES (2010).

[21] THE JUDICIALISATION OF POLITICS IN LATIN AMERICA (Rachel Sieder et al. eds., 2016); THE JUDICIALISATION OF POLITICS IN ASIA (Björn Dressel ed., 2012).

[22] Anne-Marie Slaughter, *Judicial Globalization*, 40 Va. J. Int'l L. 1103 (2000): Gleider I. Hernández. *The Judicialisation of International Law: Reflections on the Empirical Turn*, 25 Eur. J. Int'l L. 919 (2014); KAREN J. ALTER, THE NEW TERRAIN OF INTERNATIONAL LAW: COURTS, POLITICS, RIGHTS (2014).

proliferation of international courts,[23] largely concerned with the numerical proliferation of courts and their significance.[24]

In the EU, the role of the judiciary has been acknowledged first by lawyers seeing European integration as "Integration through law",[25] then by political scientists focussing on judicial politics in the EU,[26] and the CJEU as a "political power"[27] or an activist court. [28] Publications in this field made it clear that a large number of different actors have contributed to judicialisation. In a complex and multilevel system like the European Union, the supremacy of European law could not only rely on the CJEU, but had to involve national courts and private actors using litigation strategies to make their interests prevail.[29] For the civil society, it has proved difficult to have legal standing before the European Court, but the role of national courts as court of ordinary law in EU matters has compensated for this difficulty, and an evolution towards enlarged admissibility of NGO's annulment actions is underway.[30] The CJEU is an unusually powerful court in IR, with powers of, e.g. ex ante Opinion review pursuant to Article 218 TFEU, that are viewed as non-justiciable political questions in some legal orders. With the European Charter of Fundamental rights transformed into a binding commitment, the CJEU now has even more solid grounds to exert judicial control over EU 'internal' and 'external' (i.e. IR) law.

In legal regimes beyond the state, interactions between legal orders tend to make the localisation of judicialisation more complex. The latter may take the form of a legal instrument common to the partners (the EU and the US in a transatlantic regime) if some kind of dispute settlement or compliance mechanism is foreseen. But judicialisation may also occur within each of the two partners, through internal procedures (before US courts, the CJEU and the Member States' courts). From a European perspective, the globalised effects of EU law have also brought with it added significance as to its courts powers, particularly as to areas where the global reach of EU law is said to be significant.[31]

In this article we do not take into account the relationship between legal orders within the same political entity. Interactions between EU and Member States law are out of our scope, as is the relationship between federal and states law in the United States. We focus on a IR legal regime established by two entities, the EU and the US, that are clearly independent from one another. And we argue that, in the case of an emerging and evolving legal regime like the Privacy Shield, negative and positive judicialisation forms a useful analytical distinction. The former has the potential to challenge the new legal regime, though conflicts of law and jurisdictions, while the latter would rather enhance it by guaranteeing its proper implementation. When rules in the EU and the US are different, a strong institutionalisation aimed at bringing the two systems closer together is needed in order to avoid negative judicialisation in order for an effective IR regime to be in place. We argue that weak institutionalisation and a lack of robust rules creates uncertainty. This uncertainty invites instabilities through the increased likelihood of negative judicialisation. This is argued to be which particularly unhelpful in the IR context.

Moreover, judicialisation places courts at the heart of legalisation processes within institutions and in this way is not necessarily 'an opposition' to institutionalisation but rather a mechanism deeply intertwined with institutionalisation. To say it differently, (negative) judicialisation may challenge the legal foundations and the existence of an institutionalised regime, and then trigger de-institutionalisation (when the legal regime is said to be unlawful and needs to be ended), giving rise to re-institutionalisation (if a new legal regime is put in place). But (positive) judicialisation may also be part of an institutionalised legal regime, contributing to its normal

[23] RAN HIRSCHL, *TOWARDS JURISTOCRACY* (2004 & 2007); INTERNATIONAL COURT AUTHORITY (Karen J. Alter et al. eds., 2018).
[24] *See* Doreen Lustig and J.H.H. Weiler, *Judicial Review in the Contemporary World—Retrospective and Prospective,* 16 I-CON 1 (2018).
[25] Eric Stein, Lawyers, *Judges and the Making of a Transnational Constitution*, 75 AM. J. INT'L L. 1 (1981); INTEGRATION THROUGH LAW: EUROPE AND THE AMERICAN FEDERAL EXPERIENCE (Vol. 1, Maurizio Cappelletti et al. eds., 1986).
[26] ALEC STONE SWEET. GOVERNING WITH JUDGES: CONSTITUTIONAL POLITICS IN EUROPE (2000); SABINE SAURUGGER & FABIEN TERPAN, THE COURT OF JUSTICE OF THE EUROPEAN UNION AND THE POLITICS OF LAW (2016).
[27] Anne-Marie Burley & Walter Mattli, *Europe Before the Court: a Political Theory of Legal Integration*, 47 INT'L ORG., 41 (1993).
[28] RENAUD DEHOUSSE, THE EUROPEAN COURT OF JUSTICE: THE POLITICS OF JUDICIAL INTEGRATION (1998); David Keeleng, *In Praise of Judicial Activism, but what does it mean? And has the European Court of Justice ever practiced it?*, in SCRITTI IN ONORE DI G. F. MANCINI 505 (Giuffrè ed., 1998); Robert A. Kagan, *Globalization and Legal Change: the "Americanization" of European Law?*, 1 REG. & GOV. 99 (2007); SUSANNE K. SCHMIDT, THE EUROPEAN COURT OF JUSTICE AND THE POLICY PROCESS (2018); ROGER DANIEL KELEMEN, EUROLEGALISM: THE TRANSFORMATION OF LAW AND REGULATION IN THE EUROPEAN UNION (2011).
[29] *See* Karen J. Alter, *The European Court's Political Power*, 19 WEST EUR. POLIT. 458 (1996); *See also* LISA CONANT, *JUSTICE CONTAINED: LAW AND POLITICS IN THE EUROPEAN UNION* (2002).
[30] RACHEL CICHOWSKI, THE EUROPEAN COURT AND CIVIL SOCIETY: LITIGATION, MOBILIZATION AND GOVERNANCE (2009).
[31] *See* Anu Bradford, *The Brussels Effect: how the European Union rules the world* (2020), Ch. 5.

functioning and making commitments credible. In both cases we can see judicialisation as closely entwined with institutionalisation. EU IR generates complex balances of powers when it comes to informal rules and judicialisation. Both the US and the EU are highly judicialised systems, and courts and laws from both sides usually prioritize legal autonomy and are suspicious other external legal orders. Clashes between EU and US legal orders are not unlikely, and can lead to judicial claims of incompatibility as well as extra-territorial laws and judgements. The lack of a common judicial system further explains potential judicialisation occurring within each of the two legal systems.

The analysis next turns to a practical case study as the focus of the subject and object of this paper, that of transatlantic relations in one regulatory sphere, EU-US data transfer in the Privacy Shield.
This leads next to our substantive discussion of transatlantic data transfer.

C. Safe Harbour to the Privacy Shield

I. From EU-US Safe Harbour to the Schrems *ruling*

The Safe Harbour Agreement was an important departure for transatlantic relations with a so-called 'hybrid' style governance founded upon *non-institutionalisation* where the private sector was the primary subject and object of the regulation.[32] The Safe Harbour principles, as endorsed by the European Commission in a Decision of 26 July 2000,[33] were until at that time the only 'binding' and enforceable element of the relationship between the EU, the US, the Federal Trade Commission (FTC) and certification bodies. The essence of Safe Harbour was to require US companies to treat data of EU citizens as if the data were physically in Europe operating through a voluntary self-certification system with public enforcement conducted by the US FTC.

The NSA surveillance saga opened by the Snowden revelations resulted in an EU-US Working Group on data protection, raising the profile of data transfers and surveillance.[34] An increasing number of decisions of the Court of Justice, such as the decision to annul the Data Retention Directive,[35] culminated in 2015 in the *Schrems v. Data Protection Commissioner* decision invalidating the Safe Harbour Agreement, discussed in detail below.[36] Shortly thereafter, the EU's General Data Protection Regulation (GDPR)[37] was adopted, giving substantial powers to national data protection authorities as well as individual citizens and increasing the territorial reach of EU data governance law. An increasing number of high profile GDPR and data privacy related decisions dominate the docket of the CJEU.[38]

II. The EU-US Privacy Shield

A replacement for Safe Harbour in the form of the EU-US Privacy Shield agreement was announced and adopted in 2016 based on a Commission new adequacy decision in record time.[39] From its inception in 2016, the Privacy

[32] *Cf.* Gregory Schaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbour Agreements*, 9 COLUM. L. REV. 29, 77 (2002).

[33] Commission Decision of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000/520/EC, O.J.(L 215) 7. Article 25 of the Directive provided that Member States would prohibit all data transfers to a third country if the Commission did not find that they ensured an adequate level of protection.

[34] Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection', Council doc. 16987/13, (27 November 2013); Commission, 'Rebuilding Trust in EU-US Data Flows' COM (2013) 846 final; Commission, 'Communication on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU' COM (2013) 847 final.

[35] In Joined Cases C-293/12 & C-594/12, Digital Rights Ireland and Seitlinger and Others, EU:C:2014:238; *Cf* Case C-31/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, EU:C:2014:317; Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB/ Watson, ECLI:EU:C:2016:970, bolstered additionally by new Treaty of Lisbon provisions on data protection in the treaties on data privacy and the Charter of Fundamental Rights. Subsequent decisions increasingly roll back on the scope of the right to be forgotten, in part: e.g. Case C-507/17, Google v. CNIL, ECLI:EU:C:2019:772.

[36] See section III.

[37] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU).

[38] See *supra* note 34.

[38] Commission Implementing Decision (EU) 2016/1250 of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (notified under document C) (2016) 4176) 2016 O.J. (L 207) 1 (hereinafter Commission Implementing Decision 2016/1250). See ANTHONY GARDNER, STARS WITH STRIPES: THE ESSENTIAL PARTNERSHIP BETWEEN THE EU AND US, Ch. 5 (2020).

Shield, like the Safe Harbour, aimed to protect the fundamental rights of EU citizens whose personal data is transferred to the United States for commercial purposes. To this end, it allowed the free transfer of data to companies that are certified in the United States under the Privacy Shield. Although it was presented as a much more protecting mechanism than the Safe Harbour, it purports to follow Safe Harbour with modest institutional innovations and largely replicating the self-certification approach of Safe Harbour. It had a complicated structure scattered across a series of 'letters' and so its institutionalised dimensions were ostensibly weak and predominately 'localised,' bottom-up.

The Privacy Shield was conveyed by the EU and US to be an improvement upon Safe Harbour, albeit far from optimal because of its localised 'centre of gravity'. The Privacy Shield purported to 'institutionalise' transatlantic data processing through the evolution of oversight layers, structures and processes (Data Protection Agencies (DPAs), ombudsman, judicial authorities). It arguably follows closely existing EU-US data transfer agreements. The Notice provisions aimed to be significantly more robust. The guarantees provided by US authorities in the Privacy Shield are stronger. However, notably, Annex VI to the Privacy Shield Decision contained a letter from the Office of the Director of National Intelligence to the United States Department of Commerce (DoC) and to the International Trade Administration from 21 June 2016, in which it is stated that PPD-28 allowed for '"bulk" collection of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target to focus the collection. Similarly, other NSA's activities and surveillance programmes can be based on Executive Order 12333 (E.O. 12333).

As far as the commercial dimension was concerned, they included stricter obligations on certified companies receiving personal data from the EU, regarding limitations on how long a company may retain personal data (data retention principle) or the conditions under which data can be shared with third parties outside the framework (accountability for onward transfers principle). Citizens rights are intended to be better protected through information rights, enforceable at national level. DPAs acquired much more significance, whereas US enforcement rested largely with the FTC and appears to strike an imbalance overall through divergent and disparate institutionalisation and enforcement.[40] The DoC provided more regular and rigorous monitoring and EU citizens had enlarged possibilities to obtain redress.

An Ombudsman had an oversight function whereby they reported to the Secretary of State. Consequently, there were many who argue that insufficient distance exists from the intelligence community that is required for the body to act in an independent manner and not to be a true Ombudsman. With regards data protection and mass surveillance, the Privacy Shield, in the Commission's views, provides better guarantees that U.S. authorities' access to personal data coming from Europe for national security, law enforcement and other public interest purposes is subject to clear limitations.[41] However, a close look at the new system shows that there is no real improvement in terms of effective administrative and judicial redress for the data subjects whose personal data are being transferred.
The Privacy Shield met with extensive critique from the Article 29 Working Party, the EDPS and the European Parliament.[42] Overall, the nature of the evolution from Safe Harbour to Privacy Shield seems to have shifted towards further weak institutionalisation in terms of legal commitments and judicial redress opportunities. In practice, evidence suggests that many larger companies used SCCs preventatively rather than the Privacy Shield, whereas the majority of SMEs found the Privacy Shield more efficient and cost-effective, with many larger businesses concerned about its vulnerability.[43]

---

[40] ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 1/2016 ON THE EU-US PRIVACY SHIELD DRAFT ADEQUACY DECISION WP 238 (Apr. 13, 2016); EUROPEAN DATA PROTECTION SUPERVISOR, OPINION ON THE EU-US PRIVACY SHIELD ADEQUACY DECISION (May 30, 2016), European Parliament Resolution of May 26, 2016 on transatlantic data flows 2016/2727(RSP) 2016 O.J. (C 76) 82.

[41] European Commission Press Release, EU-U.S. Privacy Shield: First review shows it works but implementation can be improved (2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3966 (last visited July 26, 2020); European Commission Press Release, EU-U.S. Privacy Shield: Second review shows improvements but a permanent Ombudsman should be Nominated by 28 February 2019 (2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6818 (last visited July 26, 2020); European Commission Press Release, EU-U.S. Privacy Shield: Third review welcomes progress while identifying steps for improvement (2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134 (last visited July 26, 2020).

[42] On 5 July 2018, the Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) recommended in a resolution that the Commission suspend the EU/U.S. Privacy Shield unless and until all defined corrective actions are taken by the US Department of Commerce, particularly as to the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch ensuring protection of privacy and civil liberties in the field of counterterrorism policies.

[43] Oliver Patel & Nathan Lea, Privacy Shield, *Brexit and the future of transatlantic data flows*, UCL European Institute Policy Paper (May 2020), https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf (last visited July 26, 2020).

D. The Privacy Shield at work: further (limited) institutionalisation of EU-US data transfer

In this section we analyse the institutionalisation of the Privacy Shield from 2016 onwards, explain how the review process is organised, analyse the development of the Privacy Shield and assess its institutionalisation.

I. Reviews of the Privacy Shield (2017, 2018 and 2019): separating the commercial and surveillance aspects

A strengthened monitoring of the framework has been established by the 2016 adequacy decision of the Commission, with annual joint reviews by EU and US authorities to monitor the correct application of the arrangement discussed next, and a public report to be submitted by the Commission to the European Parliament and the Council. The first review took place in Washington, DC on 18 and 19 September 2017, The second on 18 and 19 October 2018 in Brussels and the third in Washington on 12 and 13 September 2019.[44]

In this context, and contrary to the Safe Harbour, the Commission makes its *own* evaluation of how data transferred from the EU to the US is protected. The Commission's findings have been summarized in three reports, published in 2017, 2018, and 2019[45] after the annual reviews were conducted.[46] The Commission is thus not fully dependent on declarations made by US authorities when itself evaluating the framework. This should give more credibility to the Commission's assertion, made in both reports, that the Privacy Shield reflects the principles and requirements laid down by the European Court of Justice in its decision in the *Schrems* case. It thus constitutes a broader and wider form of governance, involving learning and information sharing across institutions and actors.

This improved assessment mechanism, as well as the guarantees provided by the US government, was supposed to protect the Privacy Shield from another judicial invalidation (negative judicialisation).[47] However, we argue that the Commission's role was still ambiguous and its decisions with regard the Privacy Shield remain fragile, because they are dependent upon decisions taken at US level and discussed within an international / transatlantic framework. This is made clearer when looking at the difficulties encountered during the implementation phase of the Privacy Shield.

II. The Development of the Privacy Shield throughout the review process

The three Commission's reports confirmed the adequacy of the Privacy Shield with the EU data protection rules. The U.S. authorities, it is said in the 2017 report, 'have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield'. According to the 2018 report, they continue 'to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to

[44] On the US side, four categories of actors participated, mostly from the US administration: US Secretary of Commerce, as well as representatives of the Department of Commerce, the Federal Trade Commission (FTC), the Department of Transportation, the Department of State, the Office of the Director of National Intelligence and the Department of Justice. Representatives of official bodies enjoying some degree of independence, like the Ombudsman, a Member of the Privacy and Civil Liberties Oversight Board (PCLOB) and the Office of the Inspector General of the Intelligence Community, also participated. The American Arbitration Association, acting as administrator of the Privacy Shield Arbitration Panel, and offering independent dispute resolution under the Privacy Shield was also represented. Some Privacy Shield-certified companies were invited to provide some input.
On the EU side, the review was opened by either the Commissioner for Justice, Consumers and Gender Equality or the Director-General for Justice and Consumers and the delegation was composed of representatives of the Commission's Directorate General for Justice and Consumers, the Chair of the European Data Protection Board (EDPB) and representatives designated by the EDPB.

[45] Report From the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield {SWD(2017) 344 final} (Oct. 18, 2017); Report From the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU–U.S. Privacy Shield {SWD(2018) 497 final} (Dec. 19, 2018); Report From the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU–U.S. Privacy Shield {SWD(2019) 390 final} (Oct. 23, 2019); https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited July 26, 2020).

[46] These reports are based on the discussions held during the annual review but are also informed by a study commissioned by the Commission, which takes into consideration publicly available material, such as: court decisions; implementing rules and procedures of relevant U.S. authorities; annual reports from independent recourse mechanisms; transparency reports issued by Privacy Shield-certified companies through their respective trade associations; reports and studies from NGOs active in the field of fundamental rights and in particular digital rights and privacy; press articles and other media reports. In addition to the collection of written input, and prior to the annual reviews, the Commission had meetings with industry and business associations and with non-governmental organisations.

[47] Arguably there are strong parallels here with the EU-US governance arrangements as to e.g. the SWIFT (EU-US TFTP Agreement), involving similar learning, exchanges and specific time periods of governance.

organisations in the United States', while the 2019 report soberly confirms the Commission's findings in the adequacy decision. However, the reports brought to light a number of shortfalls. From the Commission's point of view, progress towards stronger institutionalisation of the Privacy Shield could be realised provided that US authorities actually implement the recommendations made during the annual review and written its evaluation reports. The reports themselves, but also reports published by the WP29 and European Data Protection Board,[48] as well as external independent assessments, provide a mixed picture and continue to raise concerns. This can be seen regarding both the commercial and the surveillance aspects of the Privacy Shield.

1. Commercial aspects of the Privacy Shield

On the commercial side, the Commission assessed the effectiveness of the mechanisms introduced by the DoC to proactively monitor compliance by certified companies. Based on a recommendation made by the Commission in its 2017 Report, the certification process has been strengthened by the DoC to prevent US companies from claiming compliance with the Privacy Shield before the procedure is finalised by the DoC. The Commission has urged the DoC to be more pro-active and systematic in searching for false claims of participation.[49] However, in its third Report, the Commission regretted that the DoC had not yet targeted companies that have never applied for certification under the Privacy Shield. The Commission also invited the DoC to better check whether certified companies actually comply with the Privacy Shield principles, which lead the DoC to introduce new mechanisms, such as random spot-checks, the monitoring of public reports about the privacy practices of Privacy Shield participants and, in April 2019, a new system in which the DoC checks 30 companies each month. The third report welcomed the spot checks but regretted that it was limited to formal requirements and did not address any substantive issues.[50]

As far as compliance is concerned, the Commission encouraged the DoC to assess companies' compliance with the Accountability for Onward Transfers Principle, "including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer" (Third Report). The Commission also asked the DoC, together with the FTC and the DPAs, to develop guidance on principles, and interpret some concepts in need for clarification and improvement.

Although between the second and the third annual, the Federal Trade Commission (FTC) concluded seven enforcement actions related to Privacy Shield violations and the FTC also started to investigate into the Facebook / Cambridge Analytica case, Information on the FTC's work was lacking, the Commission said in its 2018 Report, before adding, in its 2019 Report, that the information provided by the FTC remained too limited to appropriately evaluate progress in enforcement. The lack of information, according to the Commission, was 'not in line with the spirit of cooperation among authorities, on which the Privacy Shield is based'.

2. Surveillance aspects of the Privacy Shield

As far as surveillance is concerned, limitations and safeguards result from Presidential Policy Directive 28 (PPD 28) on Signals Intelligence Activities, issued in 2014.[51] The Commission proposed in the first Report to include them in section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA), which was re-authorized at the beginning of 2018. This was not taken over by the US administration and Congress. The Commission seems satisfied with the fact that the powers of the U.S. Intelligence Community to acquire foreign intelligence information by targeting non-U.S. persons have not been expanded. The third Report acknowledges the clarifications by the U.S. authorities on the way in which the collection of intelligence information is targeted under Prism and Upstream, ie. the intelligence programmes carried out pursuant to Section 702 of the FISA. For

[48] European Data Protection Board, EU-US Privacy Shield, Second Annual Review 2019 (Jan. 22, 2019), https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en (last visited July 26, 2020).

[49] In response, the DoC has introduced new tools, such as a quarterly review of companies that have been identified as more likely to make false claims, and a system for image and text searches on the Internet. This has allowed the DoC to refer several cases of false claims to the Federal Trade Commission (FTC), which in turn took enforcement action.

[50] In addition, a new issue has emerged at the third annual review as to the leniency of the DoC. At the expiration of the certification period, if a company has not yet completed the re-certification process, the DoC grants to the company a "grace period" of at least three months. In the Commission's opinion, the Department of Commerce could shorten the different time periods that are granted to companies for completing the re-certification process.

[51] Presidential Policy Directive 28: Signals Intelligence Activities (Jan. 17, 2014), https://www.hsdl.org/?abstract&did=748332 (last visited July 26, 2020).

the Commission, it confirms that the collection of foreign intelligence information continues to be "targeted through the use of selectors", and that "the choice of selectors is governed by law, subject to independent judicial and legislative oversight". On all these points, however, the Commission continues to rely entirely on declarations made by US authorities.

The Commission also acknowledged in its second and third reports the developments concerning the Privacy and Civil Liberties Oversight Board (PCLOB), as an "important oversight body in the area of government surveillance" (Third Report) which is now capable of fulfilling its functions thanks to a number of staff appointments requested by the Commission in its first Report, and progressively implemented by the US administration. The PCLOB has also adopted a work programme consisting of ten oversight projects, some of which were of particular relevance for the review, according to the Commission. The Commission also recommended the release of the Board's report on Presidential Policy Directive 28, which was done on 16 October 2018. Of course, the Commission had no real power to confirm the assertion made in the PCLOB Report that the PPD28 is fully applied across the Intelligence Community, and the mere fact that means are dedicated to government's control does not guarantee the effectiveness of this control.

3. EU-US Ombudsman

The Ombudsman mechanism, which may contribute to protect European citizens against unlawful signals collection, was a central feature of the framework established by the Privacy Shield, but it raised some concerns from the outset.[52] Assessing the implementation of the Ombudsman mechanism, along with other instruments and procedures within the Privacy Shield, remains a major challenge.

Under the Privacy Shield, EU citizens are supposed to enjoy strengthened possibilities to obtain redress in case of an illegal use of their personal data, and the third review noted progresses made. The US authorities had put in place the complaint-handling and enforcement mechanisms, as well as procedures to safeguard individual rights, including an arbitration panel and the Ombudsman mechanism.

Indeed, although an Acting Ombudsman was designated in January 2017 (Manisha Singh), the nomination of a permanent Ombudsman was still pending on late 2018, which lead the Commission to fix a deadline on 28 February 2019. The appointment of Keith Krach was finally announced by Donald Trump on 29 January 2019, under EU pressure, and confirmed by the Senate on 20 June 2019. The position is now to be filled on a permanent basis. So far, the Ombudsman has not received any admissible request.[53] Different types of remedies are foreseen including structural measures such as a change in the collection practice, and individual ones, such as the deletion of unlawfully obtained data and its removal from all government databases and intelligence reports. The CJEU would ultimately invalidate the Privacy Shield in 2020 on the basis of the Ombudsman, thus we return to this issue below.

Based on the above we can argue that weak institutionalisation is particularly apparent from the 3 reviews to date, where key forms of institutional actors evolve late in the process and certain key actors lack complete independence, rendering the overall institutional framework to appear to be less than robust. A strong institutionalisation would imply the "guarantees" provided by US authorities would go beyond vague information and declaratory action. The assessment below will confirm the weakness of the institutionalisation process.

III. Assessing the Institutionalisation of the Privacy Shield

On both commercial and surveillance aspects of the Privacy Shield, limited institutionalisation has thus taken place. The ostensibly 'light-touch' enforcement practices of the FTC thus far may indicate limited formal institutionalisation- for now. Commercial providers are not as of yet subject to meaningful infrastructures. As to surveillance, the embryonic role of the now permanent Ombudsman and newly constituted PCLOB indicates further layers of oversight and accountability being put in place- slowly but surely, and in embryonic form.

[52] See EUROPEAN OMBUDSMAN, FOLLOW-UP REPLY FROM THE EUROPEAN OMBUDSMAN TO COMMISSIONER JOUROVÁ ON THE USE OF THE TITLE "OMBUDSMAN" IN THE EU-US PRIVACY SHIELD AGREEMENT (May 2, 2016).

[53] US authorities have given further explanations during the third review on Ombudsman. The independent Inspector General of the Intelligence Community would be "systematically informed of any complaint submitted to the Ombudsman", and carry out his own assessment. The Ombudsman would report violations of the procedures under s. 702 of the FISA to the FISA Court, to "carry out an independent review and, if necessary, order the relevant intelligence agency to take remedial action" (Third Report).

However, the scope of the annual reviews may not cover all aspects that might be brought before courts by a variety of litigants. As seen above, the most serious weaknesses relate to the surveillance aspects and the Ombudsman mechanism, which do not provide for the necessary limitations and safeguards with regard to the interferences authorised by the U.S. legislation and do not ensure effective judicial protection against such interferences.

Formal institutionalisation appears still then rather limited for three main reasons. First, this is a 'soft law' international agreement which has not undergone relevant Article 218 TFEU treaty procedures. This entails that the Commission cannot go beyond recommendations to US authorities and is dependent on the latter's willingness to respond to these demands, although as we will note below the CJEU emphasises its bindingness in Case C-311/18. Second, while so far, the Commission considers that the US government takes the Privacy Shield requirements seriously, on the other US legislation on data protection and privacy has not aligned with EU rules. In ongoing litigation, the US Government has argued that this lack of alignment is not material under the terms of the adequacy decision and the array of applicable rules. This question of applicable and relative standards is and will always fundamental, without needing to know the outcome of pending litigation. Thirdly, another reason is specific to EU-US relationship which never been strongly institutionalised: there is not strong existing experience on which the Privacy Shield should build. At best, levels of partial or quasi-institutionalisation appear likely to constitute the high-water mark of institutionalisation.

Thus, the current level of institutionalisation was unlikely to prevent future invalidation though judicialisation-ie that *Schrems* II was arguably inevitable. The Commission had to arguably regularly identify shortfalls because it is the only way to comply with *Schrems I* obliging it to continuously and genuinely evaluate the Privacy Shield, and to provide legal grounds for maintaining its adequacy decision. At the same time the Commission arguably could not go too far, and had to demonstrate that the Privacy Shield, while imperfect, was performing well enough to prevent invalidation.

E. The judicialisation of the Privacy Shield

In the previous section we argued that the institutionalisation of EU-US data transfer has been limited. In the current section we will see that the institutionalisation of EU-US data transfer has been increasingly subject to judicial review, both directly and indirectly, and more often concerning standards. Safe Harbour can be seen to have been as a weak informal institutionalisation giving rise to strong and negative judicialisation. The Privacy Shield therefore constitutes a specific development of institutionalisation to enhance review thereof, not just in the court room. Ironically, judicialisation has pressed for stronger and more revitalised institutionalisation this far.

I. Judicial review

Apart from the annual reviews based on EU-US exchange of views and information (see section on institutionalisation), the Privacy Shield is still constrained by CJEU rulings issued during the Safe Harbour period (Cases 1 and 2 below) and has been subjected to three other sets of judicial proceedings, not counting the joinder of cases (Cases 3, 4 and 5 below). These proceedings are examined because they are highly instructive of the issues at stake. The core features of the litigation are outlined here next, setting out the relevant facts, legal challenge, key actors and outcome, where applicable.

A *first case* involved the CJEU developing the conditions of institutionalisation, evolving weak institutionalisation through negative judicialisation in C-362/14 *Maximillian Schrems v Data Protection Commission*.[54] In 2015, the Court considered a now seminal complaint to the Irish Data Protection Commissioner (DPC) from an Austrian law student and privacy activist as to the operation of the Safe Harbour Agreement whereby the Court found them to be bound by the Commission Decision setting up the Safe Harbour Regime, having regard to the Charter of Fundamental Rights.[55]

[54] *Schrems,* Case C-362/14.

[55] See Statement of the Article 29 Working Party on the implementation of the Judgment of the ECJ of 6 October 2015 in *Schrems*, Case C-362/14; Loïc Azoulai and Marijn Van der Sluis, *Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: Schrems*, 53 COMM. MKT. L. REV. 1343 (2016).

The CJEU invalidated Safe Harbour and held that a third country was not required to ensure a level of protection identical to that guaranteed under Union law. However, the Commission had to ensure that the level of protection under U.S. law was essentially equivalent to that guaranteed within the EU by virtue of the Directive 1995/46/EC in light of the Charter of Fundamental Rights.[56] The first and initial *Schrems* decision might thus be characterised as a decision challenging the weak institutionalisation of Safe Harbour. Austrian Law Student and privacy activist Maximilian Schrems was supported by the NGO Digital Rights Ireland, who were joined as a party, a 'repeat player' litigant. Observations were submitted by the European Data Protection Supervisor, the Irish Data Protection Commission, the European Parliament, European Commission and 8 Member States, with the vast majority opposing Schrems or not supporting him. The CJEU invalidated Safe Harbour without direction as to its temporary effects. *Schrems I* after the NSA, Snowdon and PRISM revelations[57] spurred the development of the Privacy Shield and significant developments as to other instruments and enforcement regimes, such as an EU-US Umbrella Agreement and the General Data Protection Regulation (GDPR).[58] We argue that *Schrems I* forced the EU and US parties to further institutionalise and formalise the data transfer regime.

A *second* case involved the CJEU developing individualisation as to the subjects of the Privacy Shield: C-498/16 *Maximilian Schrems v. Facebook Ireland Limited (Case 2)*.[59] Schrems features here again personally and centrally in this preliminary reference in 2018 from the Austrian Supreme Court in litigation against Facebook Ireland Limited sought declarations and other remedies in respect of private Facebook accounts and individuals who had assigned their claims to him where the case turned on the definition of consumer status under the Brussels Convention. The CJEU held that Schrems' high profile activities did not mean that he had lost the designation as a 'consumer' under EU law. He thus benefitted from a broader interpretation of the term 'consumer' in a decision in early 2018 on Regulation EC No. 44/2001, as amended, on the recognition and enforcement of judgements in civil and commercial matters, concerning his applications seeking declarations and other remedies in respect of private Facebook accounts and individuals who had assigned their claims to him. The CJEU here tacitly acknowledged Schrems de facto/ de jure status as a public figure but still did not find it enough to deprive him of the full protection of EU law as an ordinary litigant. On foot of the first and prominent CJEU decision, Schrems published two books on his legal proceedings, gave lectures including remunerated ones, and registered many internet websites, blogs, online petitions and sought crowdfunded financing of his legal proceedings. He founded a not for profit association to uphold the fundamental right to data and received many prizes and has had 25,000 claims world-wide assigned to him, relating to his claim that the defendant had commute numerous infringements of data protection provisions and that he had locus standi on his own rights and for those assigned to him residing in Austria, German or in India. The initial proceedings were dismissed by the Regional Civil Court in Vienna in Austria on the basis that he was using Facebook for professional purposes and could not rely on jurisdiction over consumer contracts. Even in a very small chamber of the CJEU (unlike *Schrems* I), it is a telling indication of the procedural protections that the CJEU accords to him at EU law level and not deprive him of remedies. An expansive reading is given to the concept of the consumer such that Schrems' litigation in the public interest as part of a broader campaign of activism are not excluded from the scope of EU law by virtue of his own institutionalisation of his work in the public interest. In this decision, the definition of a consumer entails that the actors of the Privacy Shield is enlarged by a three judge chamber of the CJEU. It is thus an outcome of much significance for the judicialisation of the Privacy Shield (or any EU-US regime) through the enlargement of its subjects and objects. Paradoxically, however, these are still limited and arguably only consolidate the outcome of *Schrems* I. This is because ultimately soft law –and not hard law- continues to govern the Privacy Shield. Arguably, this case developed some level of both positive judicialisation and institutionalisation of the Privacy Shield architecture. This is because it resulted in Safe Harbour being replaced by the Privacy Shield. However, it can also plausibly be regarded as the 'high water mark' of positive judicialisation because the outcome of that judiciliation is the Privacy Shield, which is not radically different from its predecessor. As a framework of institutionalisation of IR relations, we thus argue overall that it is a weak one.

A *third* case developed the conditions for representation as to the Privacy Shield litigation: Case T-670/16, *Digital Rights Ireland Ltd v. European Commission* (Case 3).[60] The Irish NGO Digital Rights Ireland, Digital Rights, Ireland

[56] Para 73.
[57] Commission Implementing Decision 2016/1250, *supra* note 77**;** *Schrems,* Case C-362/14.
[58] Where the principles went beyond the regulatory requirements prevailing in the US.
[59]Case C-498/16, Schrems v. Facebook Ireland*,* ECLI:EU:C:2018:37; Council Regulation No 44/2001 of Dec. 22, 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, 2001 O.J. (L 12) 1 (EC) (Brussels I).
[60] Case T-670/16, Digital Rights Ireland Ltd v. European Commission – Order of the General Court (Second chamber) of 22 November 2017 ECLI:EU:T:2017:838

(DRI), a not for profit organisation, with its object as the defence of individual internet freedoms, sought to annul before the General Court the Privacy Shield, i.e. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament. A variety of French NGOs had applied for leave to intervene in support of DRI whilst at the same time several Member States, Microsoft and the US Government and a business organisation intervene in favour of the Commission. The Commission raised an objection of inadmissibility as to the rules of procedure of the General Court (Article 130). The question arose as to whether an organisation could have its personal data transferred to the US under the contested decision. It argued this was possible given that it possesses a mobile phone and computer and that legal persons could claim protections under the Charter of Fundamental Rights as to privacy. However, the General Court held that as a legal person, it could not enjoy protections as to personal data. The Court held that the implementation of the decision would not result in a breach of its obligations and annulment could not procedure any advantage. As regards the general admissibility of the claim, the applicant argued it had to represent the interests of its members. However, the Court held it had not demonstrated an entitlement to act on behalf of its members and that EU law did not allow for the possibility of bringing an action popularis in the public interest. The General Court thus dismissed the action as inadmissible pursuant to Article 263 TFEU.[61] DRI is an experienced EU litigator supported by a number of other NGOs defending the same cause: La Quadrature du Net, French Data Network, *Fédération des Fournisseurs d'Accès à Internet Associatifs and UFC Que choisir.* Other actors to the proceeding took positions in favour of the Commission, predominantly EU MS states, the US and business alliances, including the Czech Republic, the Federal Republic of Germany, Ireland, the United Kingdom of Great Britain and Northern Ireland, the United States of America, the Kingdom of the Netherlands, the French Republic, BSA (Business Software Alliance), Microsoft Corporation, La Quadrature du Net, French Data Network, *Fédération des Fournisseurs d'Accès à Internet Associatifs and UFC - Que choisir.* It is thus a broad alliance in all respects. The decision is an ostensibly interesting one for the Privacy Shield as its first major challenge and it indicates the evidential challenges of contesting it in the public interest through annulment. The legal basis for the challenge as an action for annulment is a complex one in so far as an annulment action carries with it different evidential standards and proofs. Either way, it appears to set the scene for negative judicialisation.

A *fourth* pending case -*Case T-738/16 La Quadrature du Net vs. Commission*- in keeping with Case T-670/16, (see above) substantively begins the process of challenging institutionalisation (and, attacking weak institutionalisation at the moment of entry into force of the Privacy Shield.[62] The applicants were French NGOs, including a French privacy activist group, who sought a preliminary reference in late 2016 as to whether the US regulatory regime encompassed by the Commission Implementing Decision of the Privacy Shield was contrary to privacy rights protected under the Charter and impugned the substantial equivalence of the implementing decision with US law despite it not being as limited to what was strictly necessary. The week prior to the litigation being lodged, the Irish digital rights NGO, Digital Rights Ireland similarly lodged its complaint. The effectiveness of remedies and limited independent monitoring under the US regulatory regime supported by the Privacy Shield is the subject of challenge here in annulment proceedings. The timing of the challenge and its direct challenge to the Privacy Shield is of note, issued immediately after its inception. French privacy activists, NGOs, *La Quadrature du Net*, French Data Network, *Fédération des Fournisseurs d'Accès à Internet Associatifs* (F-FDM) took the proceeddings against the Commission. The pending decision is part of a broad ranging attack on the substantive provisions of the Privacy Shield. The action has not been found inadmissible, but this issue will be joined with the substance of the case when the General Court issues its judgement. This was potentially a major step towards judicialisation : first, because NGOs and private litigants could possibly be given wide access to the CJEU in cases related to the Privacy Shield and second, because it *could* substantively challenge it, thereby generating significant negative judicialisation.

Finally, more recently a *fifth* case has developed the standards of judicialisation with respect to instituitonalisation in Case C-311/18 *Facebook Ireland and Schrems (Schrems II)* (Case 5). The Irish Data Protection Commissioner (DPC) was investigating Schrems complaint to it as to Facebook in the aftermath of *Schrems I* and Schrems was joined as complainant. The proceedings raised issues as to the validity of the Standard Contractual Clauses (SCC) decisions arising from the Privacy Shield Decision with respect to the Charter of Fundamental Rights, as to Articles 7 and 8 there and in light of the ruling in *Schrems I*.[63] The DPC considered

[61] The General Court noted Art. 80 of the GDPR, which allows consumers to permit a "not-for-profit body, organisation or association" to assert their privacy rights before EU courts, not then yet in force.
[62] Case T-738/16, La Quadrature du Net vs. Commission, pending.
[63] Data Protection Commissioner v. Facebook Ireland Limited, IEHC 54 (2017).

provisionally that US did not offer effective remedies in accordance with the Charter to EU citizens whose data had been transferred where any safeguards provided were not binding. The Irish High Court held that the case 'of very major, indeed fundamental concern to millions of people within the European Union and beyond…', with implications for billions of euro of trade.[64] Ms. Justice Costello in the Irish High Court held that the crucial issue for resolution was the validity of the SCC decisions, only to be resolved by a decision of the CJEU where the High Court had jurisdiction to make a reference on the validity of the decisions and that Union law and the Charter were engaged, also raising issues as to judicial independence.[65] The questions referred related to an array of issues in 11 questions.[66]

The reference is notable for it being generated by Facebook as primary plaintiff rather than Schrems. It turns on the powers of the DPC newly empowered under the Privacy Shield. Schrems himself objected to the reference i.e. that the relevant clauses in the agreement did not conform with the SCC and that Facebook could not rely on them. Four parties were permitted to act as amici to the proceedings after a hearing and decision: the US, Business Software Alliance, Digital Europe and the Electronic Privacy Information Centre. Written observations were lodged by the DPC, Facebook Ireland, Schrems, the US Government, EPIC, BSA, DigitalEurope, 9 Member States, the European Parliament and Commission and similarly at the hearing, with 6 Member States and also the EDPB.Advocate General Saugmandsgaard Øe in his Opinion on 19 December 2019 held that there was nothing which affected the validity of the Commission Decision on Standard Contractual Clauses.[67] He found that the DPC had considerable powers to stop data transfers albeit he expressed doubts about US guarantees, in the context of the activities of their intelligence services on the basis of section 702 of the FISA and E.O. 12333, as to an adequate level of protection. The CJEU held on 16 July 2020 that the SCC decision was not invalid having regards to the Charter. It also affirmed that a national supervisory authority could suspend or prohibit a transfer of data to a third country pursuant to the standard data protection clause in the annex to that decision. However, the CJEU held that the Commission's finding that US law was of an adequate level of protection essentially equivalient to EU law under the GDPR read in light of the Charter, was called into question by the surveillance programmes in section 702 FISA and E.O. 12333 because they authorised surveillance programmes such as PRISM and UPSTREAM. FISA did not indicate limitations on powers and E.O. did not confer enforceable rights on EU citizens against the US authorities. This violated the principle of proportionality because surveillance programmes could not be regarded as limited to what was strictly necessary. Moreover, Ombudsman could not remedy deficiencies which the Commission had found (e.g. lack of a redress mechanism) as to the transfers impugning findings as to adequacy with respect to essential equivalence as guaranteed by Article 47 of the Charter. However, the annulment of the adequacy decision did not create a legal vacuum on account of the provisions of Article 49 of the GDPR allowing for derogations in special situations.[68] Ultimately, weak instituionalisation (e.g. as to the Ombudsman) could not amount to adequate oversight in the face of such surveillance. We thus argue that this weak institutionalisation led to inevitable negative judicialisation. In other words, the decision was not just exclusively about US surveillance laws but was also about the fragile construct of institutionalisation underpinning the Privacy Shield architecture. The lack of a robust institutional framework here overall was of salience to the CJEU. A stronger institutionnalisation could have resulted from truly legal guarantees provided by US authorities, which was not the case. The CJEU decision is thus useful analytically because it helps us to see the causal impact between institutional frameworks which are not robust giving rise to negative judicialisation.

---

[64] *Id.*

[65] Data Protection Commissioner v. Facebook Ireland Ltd & Anor, IESC 46 (2019); Whilst the proceedings are still pending, the Irish Supreme Court dismissed the appeal in part in Summer 2019.

[66] I.e.: What obligations are incumbent upon the DPC? Is the Privacy Shield an adequacy decision? Whose laws must satisfy whom? How should US law be understood and interpreted in Europe precisely? It may consider: where there is a violation of rights through transfer, what precisely is the comparator? The Charter, EU treaties, secondary legislation e.g. a Directive or the European Convention on Human Rights (ECHR)? The adequacy of the Ombudsman under the Privacy Shield was also the subject of the reference.

[67] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145.

[68] It noted in para. 15: 'Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.'

II. Synthesising key features of the Privacy Shield litigation

1. The actors of the institutionalisation and judicialisation of the Privacy Shield

The actors contesting the Privacy Shield arguably seek legitimation and empowerment from litigation, with litigation strategies giving voice to those excluded from the law-making processes (e.g. NGOs, Schrems or data protection authorities initially with limited staffing and resources). The autonomy of actors of the Privacy Shield later litigated (e.g. by DPAs) provides further evidence of empowerment. The litigation against the Privacy Shield brings individuals centre-stage into an agreement designed with multiple subjects and objects and has ostensibly sought to empower consumers and citizens as the subject of the Privacy Shield- as evidenced by the judicialisation mapped here. Yet the Privacy Shield has consistently overlapping subjects and objects e.g. technology companies, those certifying, data protection authorities, an Ombudsman and States. Thus the list of entities seeking to act as amicus curiae in some of the proceedings is vast and shows its multilevel significance (Case 5). Latest caselaw on the Privacy Shield at national level concerns denigrating judicial independence, where Facebook explicitly sought to row back on the capacity of national courts to refer in pending litigation (Case 5) and is also of concern showing how the interests of the manifold subjects and objects unsurprisingly do not align where they are so diverse.

2. Evolutions in the type of judicialisation, from Safe Harbour to Privacy Shield

The caselaw to date challenges both procedural and substantive dimensions of the new architectures put in place and shows an evolution in its contestation.

The initial caselaw, prior to the Privacy Shield, contests to a high degree the structures and procedures governing acts, as well as the relevant standards applying (Case 1). It presses for the development of actor autonomy, individualisation of the consumer and better standards (Case 2). By and large, the CJEU has defended high standards of data protection, stemming from both primary and secondary law, and has ruled in favour of data activists at the expense of EU-US data transfer mechanisms. It might thus be said that earliest caselaw concerns a lack of formal institutionalisation: strong and even negative judicialisation is a result of the weak formal institutionalisation of the Safe Harbour (Case 1), compare to the far more perfectionate legal protection system ensured by the EU (Cases 1 and 2).

Later caselaw (Case 3 to 5) concerns the conditions of the new (and limited) institutionalisation in the Privacy Shield. Institutionalisation did not put an end to judicialisation, quite the contrary: the Privacy Shield was even more subjected to legal attacks, indirectly but also directly through annulment procedures. *Schrems I* (Case 1) begins as a substantive challenge to the application of the European Charter of Fundamental Rights and similarly the latest pending litigation at root (Cases 3 to 5) also contests the substantive application of fundamental rights standards to the charter. Increasingly there were direct conflicts on standards in successive caselaw. The caselaw increasingly also developed institutionalisation *through* standards, where the autonomy of actors in deeper institutionalisation structures is tested. While earliest caselaw appears to provide a *push to* partial institutionalisation, later caselaw was concerned with operative standards and 'partial' institutionalisation- and its shortcomings. It is clearly a push *away* from the institutionalisation created.

In addition, the caselaw also demonstrates the embedding of commerce and security in transnational data legislation where security emerges alongside privacy and commercial/ consumer interests, as an evolving set of issue linkages.[69] Linkages that appear through the judicialisation process provide additional incentive to institutionalise the Privacy Shield. While the annual reviews keep commercial and security aspects separate (ie as two different chapters of the negotiations), judicialisation shows that they are intertwined, with weak instituionalisation being directly affected by surveillance towards strong judicialisation.

Our analysis of the reviews and caselaw and its evolution from the Safe Harbour to the Privacy Shield period allows us to conclude that: firstly, insufficient formal institutionalisation (Safe Harbour) has led to high level of judicialisation, including negative judicialisation (Cases 1 and 2); secondly, increased but limited formal institutionalisation (through the Privacy Shield) has not put an end to previous legal issues, but, on the contrary,

[69] *See* HENRY FARRELL & ABRAHAM NEWMAN, OF PRIVACY AND POWER (2019).

has created demands for further institutionalisation through judicialisation. Negative judicialisation (Schrems II) finally pointed at and 'sanctioned' this lack of institutionalisation.

3. Application beyond the Privacy Shield

We argue that there are other applications of this thesis potentially beyond the Privacy Shield. Arguably, there are strong parallels here between the EU-US Privacy Shield and other EU-US data transfer governance arrangements involving similar learning, exchanges and time periods of governance.[70] In the period since the 9/11 2001 terrorist attacks eight law enforcement agreements have been passed by the EU and US including two agreements between the US and Europol (signed in 2001), the extradition and mutual legal assistance agreements (signed in 2003), the Agreement between the US and Eurojust (2006), the Agreement on the processing and Transfer of Financial Messaging data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (TFTP) (signed in 2009), the Passenger Name Record (PNR) Agreement (signed in 2011), and finally the so-called "Umbrella Agreement" (signed in 2016). Two of these agreements have been challenged before the CJEU, the PNR and the TFTP/SWIFT Agreement.

The EU-US PNR Agreement decision of the CJEU in 1995[71] resulted in the invalidation of the agreement and the negotiation of a new agreement known to be *worse* than the previous one. The weak institutionalisation of this agreement can explain the judicial 'negative' outcome. The PNR ruling remains a famously sour decision secured by the European Parliament (EP), who succeeded in having the agreement struck down which they perceived to harbor adverse effects for EU citizens' rights with limited oversight. [72] It is a notorious decision precisely because the CJEU granted in few words an ostensible victory to the EP in a highly technical judgment failing to deliver any fundamental rights analysis on a highly controversial Agreement. While cooperation on PNR was formalised in a proper agreement, the latter suffered from a number of weaknesses and the decision to conclude the agreement was finally found invalid for reasons related to its lack of correct legal basis. Other weaknesses could have been found by the Court, if it had proved necessary to examine the other pleas. From our perspective, however, the incorrect legal basis is an element of the weak institutionalisation of the agreement, leading to negative judicialisation.

The TFTP/SWIFT agreement was brought before the General Court and the CJEU. Again, the judgements did not concern the substance of the agreement, but public access to a Council legal service document, during the negotiation phase. In 2009, a Dutch Member of the European Parliament and long-term civil liberties campaigner, acting without support of the European Parliament, sought access under Regulation No 1049/2001, to document 11897/09 of 9 July arguing that legal basis of the SWIFT Agreement was flawed, which was denied on secrecy grounds which she challenged before the General Court. The General Court partly ruled in her favour, a judgement which was confirmed on appeal by the CJEU.[73] Negative judicialisation weighed in against blanket institutional secrecy covering a debate on the proper legal basis of the agreement, which can be seen as a weak institutionalisation of EU-US data transfer under the SWIFT agreement.

Similar examples could be found in arrangements between the EU and other states. Opinion 1/15 about the EU-Canada agreement is particularly relevent. In 2014, a resolution of the EP sought an Opinion of the Court on the validity of the EU-Canada PNR Agreement.[74] In 2017, the CJEU held that, although surveillance is a necessary tool to prevent terrorism, there should be very strict rules as to the concrete implementation of such surveillance. [75] Some provisions of the draft agreement were considered incompatible with Articles 7 (privacy) and 8 (data protection), in conjunction with Article 52 (principle of proportionality) of the Charter of Fundamental Rights of the European Union. Again, it can be argued that the failure to specify the conditions of mass surveillance in the EU-Canada Agreement (lack of institutionalisation) explains the 'negative' Opinion or the CJEU.

[70] Marike De Goede, '*The SWIFT Affair and the Global Politics of European Security*', 50 J. COMM. MKT. STUD. 214 (2012).
[71] Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission [2006] ECR I-4721.
[72] *See* Grainne Gilmore and Jorit Rijpma, '*Annotation of Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission*' *44* C.M.L.REV. 1081. (2007); Mario Mendez, '*Annotation, Joined cases C-317/04 and C-318/04, European Parliament v. Council and Commission*' 3 EU.CON. L. REV. 127 (2000).

[74] 25 November 2014 (OJ 2016 C 289, p. 2).
[75] Opinion 1/15 of the Court (Grand Chamber) ECLI:EU:C:2017:592 (26 July 2017).

F. Conclusions

This paper has shown how the dynamic between institutionalisation and judicialisation is of much value in the context of the analysis of evolving legal frameworks relating to IR but also more broadly. It has shown how judicialization per se is not identified here as normatively problematic or damaging. We have instead argued that the link between institutionalisation and judicialisation is well suited to explaining the consequences of EU IR powers, in an area like data protection and privacy where the degree of protection afforded by the US and the EU is very different, with EU law being far more protective than US law. The interaction between institutionalisation and judicialisation is a useful framework to analyse international emerging legal regimes such as the EU-US regime of data transfer. The degree of institutionalisation more particularly matters as weak institutionalisation more than certainly leads to negative judicialisation (invalidation of the regime) while strong institutionalisation can lead to positive judicialisation and the strengthening of the regime. As we have shown, the dynamic between weak institutionalisation and negative judicialisation, caused by a lack of a robust legal framework, is exemplified well in the Privacy Shield as a weak form of soft law institutionalisation due to the lack of clarity and serious commitments. These weaknesses must be signficiantly alleviated if the soft law arrangement is to escape negative judicialisation. The Privacy Shield litigation exemplifies these issues well.

We have thus argued that the Safe Harbour can be seen as a weak formal institutionalisation giving rise to strong negative judicialisation but also weak institutionalisation (see cases 1 and 2 above). Indeed, the initial invalidation of Safe Harbour by the CJEU forced the EU and the US to negotiate urgently a new framework capable of securing transfer of data from Europe to the US, which perhaps shows in the modesty of the architecture resulting. An analysis of both the content and review process of the Privacy Shield shows that only limited institutionalisation took place since 2016. A light institutional apparatus was strengthened but still limited guarantees are not sufficient to transform the new EU-US framework into a strong institutionalised mechanism. The possibilities to have redress on the US side being insufficient, and the surveillance programmes providing no real limitations and safeguards, the Privacy Shield has been targeted by a number of actors in Europe, at both national and supranational level (Cases 3 to 5).

Judicialisation in Europe appears to be a way to compensate for the historic lack of formal institutionalisation of the transatlantic relations. The Privacy Shield was consistently threatened by invalidation at the CJEU, while institutionalisation was weak. Since the European Charter of Fundamental Rights has become binding and the GDPR entered into force, the CJEU acquired solid legal grounds to exert a judicial control over the Privacy Shield. Therefore, it was unlikely that a weak institutionalisation of the EU-US framework could prevent negative judicialisation. This was confirmed by the CJEU landmark ruling in the Case of Schrems II, which we suggest is a particularly vivid example of the dynamic between weak institutionalisation and negative judicialisation.
From a normative perspective, the CJEU judgment may be criticised for having destabilised the EU-US arrangement once again, with important consequences for business transatlantic relations, or on the contrary it can be approved for rightly challenging a legally flawed IR framework. Our point is not to critically evaluate the merit of the invalidation, but rather to explain negative judicialisation by the (low) degree of institutionalisation, a dynamic that could potentially help to understand many EU IR frameworks. It might not be easy to precisely evaluate the level of institutionalisation needed to prevent from negative institutionalisation. However, we know for sure that informal arrangements, based on merely declaratory and loose commitments, entail a strong risk of negative judicialization in all areas where judicial scrutiny is possible.

Could the invalidation of the Privacy Shield starts a new process of institutionalisation? The US Secretary of Commerce, Wilbur Smith, has announced that the Department of Commerce "will continue to administer the Privacy Shield program", as the Schrems II ruling "does not relieve participating organizations of their Privacy Shield obligations".[76] In the meantime the European Commission together with the Departement of Commerce will try to find a solution in order to preserve transatlantic data flows. The European Data Protection Board, in a statement welcoming the CJEU ruling in Schrems II, « stands ready to provide the European Commission with assistance and guidance to help it build, together with the U.S., a new framework that fully complies with EU

[76] U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows, 16 July 2020, https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and, (last visited July 26, 2020).

data protection law ». [77] In the meantime, it will assess the judgment in more detail and provide further clarification for stakeholders and guidance on the use of instruments for the transfer of personal data to third countries pursuant to the judgment. But the EDPB also made clear that there will be no grace period as the Court invalidated the Privacy Shield Decision without maintaining its effects.[78] At the very least EU Data Protection Authorities could slow-roll enforcement, giving companies time to figure out how to respond, as they did when Safe Harbor was invalidated.[79]

Whether the Privacy Shield can be successfully and rapidly renegotiated remains to be seen. What is clear is that a new period of uncertainties has started.[80] The larger context of EU-US relations appears to suggest at the time of writing that this is unlikely. A renegotiation of the Safe Harbour Agreement took place under closer administrative ties than ever before willing to extend protections to EU citizens as to privacy under US law. There still a willingness to negotiate from both sides but U.S. law cannot be so easily adjusted to EU standards.

[77] European Data Protection Board, Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July 2020, https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_fr (last visited July 26, 2020).
[78] European Data Protection Board publishes FAQ document on CJEU judgment C-311/18 (Schrems II), https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en .
[79] Jennifer Daskal, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers*, https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/, (last visited July 26, 2020).
[80] Theodore Christakis, *After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ , (last visited July 26, 2020).