University of New South Wales Law Research Series

DATA TRANSFERS AFTER SCHREMS II: THE EU-US DISAGREEMENTS OVER DATA PRIVACY AND NATIONAL SECURITY

MONIKA ZALNIERIUTE

Forthcoming (2022) 55(1) Vanderbilt Journal of Transnational Law
[2021] *UNSWLRS* 35

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

DATA TRANSFERS AFTER *SCHREMS II*: THE EU-US DISAGREEMENTS OVER DATA PRIVACY AND NATIONAL SECURITY

MONIKA ZALNIERIUTE*

Abstract

In the long-awaited *Schrems II* decision, the Court of Justice of the European Union (CJEU) took a radical, although not an unexpected, step in invalidating the Privacy Shield Agreement which facilitated the European Union – United States data transfers. *Schrems II* illuminates the long-lasting international disagreements between the EU and USA over data protection, national security, and the fundamental differences between the public and private approaches to protection of human rights in data-driven economy and modern state. This article approaches the decision via an interdisciplinary lens of *international law and international relations* and situates it in a broader historical context. In particular, I rely on the *historical institutionalist* approach which emphasizes the importance of time and timing (also called sequencing) as well as institutional preferences of different actors to demonstrate that *Schrems II* decision further solidifies and

* Senior Lecturer and Australian Research Council DECRA Fellow at the Faculty of Law & Justice; Lead of 'AI and Law' research Stream at Allens Hub for Technology, Law and Innovation, UNSW Sydney, m.zalnieriute@unsw.edu.au. This research was supported by Australian Research Council Discovery Early Career Research Award (project number DE210101183). I would like to thank Frank Pasquale at Brooklyn Law School, Abraham Newman at Georgetown University, Henry Farrell at Johns Hopkins University, Thomas Streinz at NYU, Lee Bygrave at University of Oslo, Graham Greenleaf and Lyria Bennett Moses at UNSW Sydney, Christopher Kuner at Vrije Universiteit Brussel, Megan Richardson and Andrew Kenyon at University of Melbourne, Alexander Trechsel at University of Lucerne and Giovanni Sartor at European University Institute for their input into development of these ideas. I am also grateful to Sophie Kwasny and Lee Hibbard at Council of Europe and Mario Oetheimer at EU Fundamental Rights Agency for introducing me to workings of data protection institutions. I thank Jacob Silove for his research assistance.

cements CJEU's principled approach to data protection, rejecting data securitization and surveillance in the post-Snowden era. *Schrems II* aims to re-balance the terms of international cooperation in data-sharing across the Atlantic and beyond. It is the outcome that the US tech companies and the government feared. Yet, they are not the only actors displeased with the decision. An institutionalist emphasis enables us to see that the EU is not a monolithic block, and *Schrems II* outcome is also contrary to the strategy and preferences of the EU Commission. The invalidation of the Privacy Shield will now (again) require either a reorientation of EU policy and priorities, or accommodation of the institutional preferences of its powerful political ally – the USA. The CJEU decision goes against the *European Data Strategy*, and places a $7.1 trillion transatlantic economic relationship at risk. Historical institutional analysis suggests the structural changes in the US legal system to address the inadequacies in the *Schrems II* judgment are unlikely. Therefore, the EU Commission will act quick to create a solution - another quick contractual 'fix' - to accommodate US exceptionalism and gloss over the decades of disagreement between the EU and USA over data protection, national security and privacy. When two powerful actors are unwilling to change their institutional preferences, 'contracting out' the protection of human rights in international law is the most convenient option.

TABLE OF CONTENTS

INTRODUCTION

> 'For national security experts, it is puzzling in the extreme to think that citizens of one country have a right to review their intelligence files from other countries.' - *Peter Swire*, 2020[1]

> 'It isn't the CJEU's judgment or European privacy policies that need to be revised. What needs to change is how U.S. policymakers think about national security and surveillance in a world of global information networks. For two decades, the U.S. has been able to have its cake and eat it too - behaving like a unilateral, imperialist power in an interdependent world. *Schrems II* shows how that strategy is reaching its limits.' – *Henry Farrell and Abraham Newman, 2020*[2]

Never before have data protection, national security and information privacy been more important for the protection of human rights than today; the global COVID-19 pandemic has required governments and citizens to have an open dialogue about contract tracing and data collection for protecting public health during the times of global health crisis and public emergency. Often, personal data collected by COVID-tracing apps in one country can be transferred to another, leaving individuals across the globe vulnerable to commercial and government surveillance

[1] Peter Swire, *"Schrems II" backs the European legal regime into a corner — How can it get out?*, https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/ (last visited Aug 11, 2020).
[2] Henry Farrell & Abraham L. Newman, *Schrems II Offers an Opportunity—If the U.S. Wants to Take It*, LAWFARE (2020), https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it (last visited Aug 11, 2020).

practices without any recourse.[3] This is especially so because there are no truly international – as opposed to regional – agreements on data protection and information privacy to ensure that individuals can seek effective remedy if their fundamental rights have been violated. Despite the increasing importance of personal data processing in running the modern state (as well as business), nations have not yet found an agreement over the appropriate regulatory policy and where the limits of private and public data collection lie.

International disagreements in data protection, national security and information privacy policy between the leading global regulatory actors – the European Union (EU) and United States of America (USA) - have significant implications for the protection of human rights in a world where most aspects of our lives are increasingly surveilled by both private companies and governments entities. These disagreements – which entail even more profound human rights implication during the 2020 global health pandemic – date all the way back the late 1960s, when data protection and information privacy first emerged as a policy concern on both sides of the Atlantic. Since then, conflicts over data protection, national security, and global data flows between the EU and US have been resurfacing in new forms every few years.

The latest iteration of this decades-long history of transatlantic data 'wars',[4] 'tensions',[5] and 'battles,"[6] is the long anticipated *Schrems II*

[3] For example, Australians' data from COVID-19 tracing app to is held by US cloud giant Amazon, (2020), https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682 (last visited Jul 23, 2020); Simon Kolstoe, *Coronavirus: researchers no longer need consent to access your medical records*, THE CONVERSATION , http://theconversation.com/coronavirus-researchers-no-longer-need-consent-to-access-your-medical-records-138567 (last visited Jul 23, 2020); Eerke Boiten, *Why we need to know more about the UK government's COVID-19 data project – and the companies working on it*, THE CONVERSATION , http://theconversation.com/why-we-need-to-know-more-about-the-uk-governments-covid-19-data-project-and-the-companies-working-on-it-141078 (last visited Jul 23, 2020).

[4] H Farrell & A Newman, *The Transatlantic Data War: Europe Fights Back Against the NSA*, 95 FOREIGN AFFAIRS 124–133 (2016).

[5] LEE A. BYGRAVE, *Transatlantic Tensions on Data Privacy* (2013).

[6] S Hare, *For your eyes only: US technology companies, sovereign states, and the battle over data protection*, 59 BUSINESS HORIZONS 549 (2016).

decision, [7] handed down by the highest Court of the European Union sitting in Luxembourg – the Court of Justice of the European Union (CJEU). On 16 July 2020, the CJEU held that the scope of US surveillance programmes, and the lack of legal remedies in the USA, are fundamental problems under EU law, and consequently struck down the legal basis for the EU-US data transfers. The CJEU invalidated the key mechanism for EU-US data transfers – this time under *Privacy Shield* arrangements – for the *second* time in a decade. It held that US laws do not provide 'essentially equivalent' protection for personal data to that guaranteed under EU law – an EU law requirement for data transfers to third countries – because of the extensive US surveillance regime. While the CJEU did not invalidate another venue for data transfers – Standard Contractual Clauses (SCC) – its reasoning implies that personal data cannot be transferred to the US using this legal basis either for the same reasons: lack of adequate safeguards for personal data in the USA. *Schrems II* has significant implication for the future of personal data transfers between EU-USA, the transatlantic economy, as well as global data law and governance more generally.

While the judgment affects many areas of law and politics, in this article I focus on the human rights protection in the EU-US data transfers, and argue that Schrems II illuminates the long lasting disagreements between the EU and USA over data protection and privacy, and the fundamental differences between the public and private approaches to protection of personal data. In this decision, the CJEU has rejected the approach of 'contracting out' the protection of human rights via private arrangements – under schemes such as *Privacy Shield* or SCC – where public institutions fail to provide adequate safeguards. The Court was clear that no private mechanism – a contractual guarantee or self-certification scheme – is sufficient to compensate or gloss over the fundamental flaws of public institutions – data protection and surveillance laws

[7] Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems, (2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9755430 (last visited Jul 23, 2020).

of third country – in ensuring the 'essentially equivalent' to that guaranteed under EU law. The rejection of this approach of 'contracting out' human rights, which has been long championed by the USA and EC Commission alike, is a win for the right to privacy and personal data protection; however, the long-term political impact of the judgment is less certain in the context of the wider historical context of EU-USA disagreements in this area of law and policy since the 1970s.

To understand the role of these disagreements in *Schrems II,* I look at the institutional preferences of different actors in transatlantic data sharing arrangements via an interdisciplinary lens of *international law and international relations*.[8] While political science and legal disciplines are organized around distinct goals and addressed at different audiences, there is nonetheless a substantial and burgeoning intersection between the two.[9] In particular, I rely on the *historical institutionalist* approach which emphasizes the importance of time and timing (also called process tracing or sequencing) as well as institutional preferences of different actors in causal process,[10] to demonstrate that *Schrems II* further solidifies

[8] Robert O. Keohane, *International Relations and International Law: Two Optics*, 38 HARV. INT'L. L. J. 487 (1997); Anne-Marie Slaughter, Andrew S. Tulumello & Stepan Wood, *International Law and International Relations Theory: A New Generation of Interdisciplinary Scholarship*, 92 THE AMERICAN JOURNAL OF INTERNATIONAL LAW 367–397 (1998); Kenneth W. Abbott, *Toward a Richer Institutionalism for International Law and Policy*, 1 JOURNAL OF INTERNATIONAL LAW AND RELATIONS 9 (2005).

[9] Roberto Vilchez Yamato et al., *Counter-disciplining the Dual Agenda: towards a (re-)assessment of the interdisciplinary study of International Law and International Relations*, 61 REVISTA BRASILEIRA DE POLÍTICA INTERNACIONAL (2018), http://www.scielo.br/scielo.php?script=sci_abstract&pid=S0034-73292018000100211&lng=en&nrm=iso&tlng=en; INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART, (Jeffrey L. Dunoff & Mark A. Pollack eds., 2013); Anne Peters & Ulrich K Preuss, *International Relations and International Law*, *in* ROUTLEDGE HANDBOOK OF CONSTITUTIONAL LAW 33–44 (Mark Tushnet, Thomas Fleiner, & Cheryl Saunders eds., 2013); Emilie M. Hafner-Burton, David G. Victor & Yonatan Lupu, *Political Science Research on International Law: The State of the Field*, 106 AMERICAN JOURNAL OF INTERNATIONAL LAW 47–97 (2012).

[10] Sven Steinmo, *Historical Institutionalism*, *in* APPROACHES IN THE SOCIAL SCIENCES 118–138 (Donatella Della Porta & Michael Keating eds., 2008); Kathleen Thelen et al., *Historical Institutionalism in Comparative Politics*, *in*

and cements CJEU's strong rejection of data securitization in the post-Snowden era, aimed at re-balancing the terms of international cooperation in data-sharing across the Atlantic and beyond.

Schrems II is the outcome that US tech companies feared. Yet, I will argue in this Article, that they are not the only actors displeased with the decision. Historical institutionalist analysis illuminates that the EU is not a monolithic block, and that Schrems II is also an outcome contrary to the wishes of EC Commission. The invalidation of the Privacy Shield will now (again) require either a reorientation of EU policy and priorities, or accommodating the institutional preferences of its powerful political ally – the USA. The CJEU decision goes against the European Data Strategy,[11] and places a $7.1 trillion transatlantic economic relationship at risk. Historical institutional analysis suggests the structural changes in the US legal system to address the inadequacies in the *Schrems II* judgment are unlikely. Therefore, the EC will act quick to create a solution – another quick contractual 'fix' – to accommodate US exceptionalism and gloss over the decades of disagreement between the EU and USA on data privacy and protection. When two powerful actors are unwilling to change their institutional preferences, 'contracting out' human rights seems to be the most convenient option.

Part I of this Article provides a background to the Schrems challenge and the disagreements between the EU and USA over data protection that are at heart of Schrems' complaint. Part II focuses on the CJEU's decision in depth and explains its reasoning. In Part III, I evaluate the *Schrems II* decision, arguing that it is a further evidence of the CJEU's pushback against data seucuritization. Part V discusses the implications of the CJEU's judgment for the EU-USA arrangements as well international data

---

STRUCTURING POLITICS: HISTORICAL INSTITUTIONALISM IN COMPARATIVE ANALYSIS (1 edition ed. 1992); Henry Farrell & Abraham L. Newman, *Making global markets: Historical institutionalism in international political economy*, 17 REVIEW OF INTERNATIONAL POLITICAL ECONOMY 609–638 (2010).

[11] European Commission, *European data strategy*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited Jul 23, 2020).

transfers more generally. I conclude by looking at the prospects for substantial future reforms of another quick 'fix', such as Privacy Shield, to gloss over data securitization and the decades of disagreements between the EU and US.

I. SHORT HISTORY OF EU-US DISAGREEMENTS OVER DATA PROTECTION AND PRIVACY

Schrems II is the second decision stemming from the long running challenge, based on fundamental human rights, to the legality of EU-USA data transfers by data protection and privacy activist Maximillian Schrems. Following the Snowden revelations related to US mass surveillance programmes in 2013,[12] Schrems lodged a complaint with the Irish Data Protection Commissioner about Facebook Ireland's transfer of data to the US. At the heart of the Schrems' challenge lies the EU-US disagreement over data protection and privacy, which date back to the late 1960s and early 1970s, when data protection first emerged as a policy issue. Understanding Schrems' challenge therefore requires looking back at the history of data protection law and policy.

Early Agreements and Differences

The early discussion in the 1960s and 1970s on data protection and privacy were similar in both Europe and the US – they focused on the fears about rising surveillance potential of public administration bodies.[13] Swiftly, a common opinion emerged that these fears

[12] James Ball, *NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show*, THE GUARDIAN, 2013, http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

[13] See DAVID H. FLAHERTY, PRIVACY AND GOVERNMENT DATA BANKS: AN INTERNATIONAL PERSPECTIVE (1979); COLIN J. BENNETT, COLIN BENNETT & COLIN J. AND BENNETT COLIN BENNETT, REGULATING PRIVACY: DATA

would be best tackled with the 'fair information principles', which specified how personal information should be dealt with. These principles revolved around practices of openness about personal data use, disclosure, secondary use, correction, and security. The principles did not articulate precise legal requirements, but instead provided a conceptual framework for balancing data privacy versus other interests.[14]

These principles were first comprehensively articulated in 1973 by the US Department of Health, Education and Welfare's special task force in the seminal report 'Records, Computers and the Rights of Citizens' ('HEW Report').[15] The report was adopted following several years of intense discussions, media investigations and US Congressional hearings in the early 1970s in the US scrutinizing the abuse of power and surveillance programmes by the US President Richard Nixon and the first Director of the US Federal Bureau of Investigation (FBI) John Edgar Hoover.[16]

The fair information principles have dominated the US approach to information privacy protection since their inception.[17] However, their impact reached well beyond the US; the principles also laid the foundations for the future legal developments in other countries and internationally. They provided the basis not only for the *Privacy Act of 1974* (US), but also for the early data protection Acts passed in the 1970s in Western European countries, such as

---

PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1 edition ed. 1992).

[14] For a detailed analysis, see, eg, LEE ANDREW BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 5 (2014); See also ROBERT GELLMAN, *Fair Information Practices: A Basic History - Version 2.19* (2019), https://papers.ssrn.com/abstract=2415020 (last visited Aug 11, 2020).

[15] See Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, OFFICE OF THE ASSISTANCE SECRETARY FOR PLANNING AND EVALUATION, DEPARTMENT OF HEALTH, EDUCATION AND WELFARE (1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens (last visited Aug 11, 2020).

[16] See generally RHODRI JEFFREYS-JONES, WE KNOW ALL ABOUT YOU: THE STORY OF SURVEILLANCE IN BRITAIN AND AMERICA (1st edition OUP ed. 2017) chapter 8.

[17] Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 JOURNAL OF SOCIAL ISSUES 431–453, 436 (2003).

Germany and France.[18] Some places in Europe adopted similar laws earlier than the HEW Report. For example, in the year 1970, the Lände of Hesse in Germany passed data protection legislation, which was also the first data protection law in the world.[19] Sweden soon followed in 1973,[20] and subsequently other European countries began to implement similar policies, with the first federal data protection acts in Germany and France Act coming into force in 1978.[21]

While the principles of data protection and privacy principles adopted by Western democracies in the early 1970s were similar, great differences quickly emerged quickly as to *how* and to *whom* such principles should be applied. As more private companies started to advance their own data processing databases to collect significant quantities of personal data for business purposes, initial public debates over government use of personal data expanded to include the private sector. Many European countries commenced the development of comprehensive data privacy regimes that have been enforced by dedicated national data protection authorities (DPAs) uniformly, both in the public and private sectors. DPAs are independent public authorities that supervise the application of data protection laws by providing expert advice and handling complaints with respect to violations of, formerly, national data protection laws, and, since 2018, the GDPR.[22] The US legislative

---

[18] See Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44 (2001).

[19] HESSISCHES GESETZ-UND VERORDNUNGS BLATT I, *Datenschutzgesetz [Data Protection Act]* (1970).

[20] RIKSDAG, *Datalagen [Swedish Data Act]*, No. 289 of 1973 (1973).

[21] For France, see LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS (LAW NO. 78-17 OF 6 JANUARY 1978 CONCERNING INFORMATION TECHNOLOGY, FILES AND CIVIL LIBERTIES,), (1978); For Germany, see GESETZ ZUM SCHUTZ VOR MIBBRAUCH PERSONENBEZOGENER DATEN BEI DER DATENVERARBEITUNG (BUNDESDATENSCHUTZGESETZ - BDSG) [LAW ON PROTECTION AGAINST THE MISUSE OF PERSONAL DATA IN DATA PROCESSING (FEDERAL DATA PROTECTION ACT - BDSG)], (1977).

[22] For more on DPAs, see F Bieker, *Enforcing Data Protection Law - The Role of the Supervisory Authorities in Theory and Practice*, *in* PRIVACY AND IDENTITY MANAGEMENT. FACING UP TO NEXT STEPS 125–139 (Anja Lehmann et al. eds., 1st ed. 2016 edition ed. 2017); Charles Raab & Ivan Szekely, *Data protection*

framework, on the other hand, regulated federal government activities comprehensively but failed to cover the private actors, which were subject only to sectoral laws, a voluntary compliance model and enforcement in the courts (as opposed to enforcement by a central authority).[23]

Prevailing legal scholarship discourse claims that disagreement on an international scale, and the growth of different regulatory approaches to data protection and privacy between the US and EU, are a consequence of different cultural and philosophical traditions in those regions. James Whitman provides an influential comparison of these purported 'two western cultures of privacy', which presents the EU and US approaches to privacy as foundationally disparate and irreconcilable. Basing on the 'Three Concepts of Privacy' work by Robert Post,[24] and in particular focusing on France and Germany, Whitman observes that the European perspective of privacy flows from the concept of 'dignity', whereas the US formulation is a consequence of their pursuit of 'liberty'.[25] Whitman's account is closely related to another variation of a 'socio-culturalist' explanation, which has also gained a strong prominence to many scholars as a main driving force for the transatlantic differences. Named 'fascist legacy' theory by political scientists working in institutionalist tradition,[26] this approach suggests that Europeans developed a stronger taste for the protection of personal data than Americans because of Europe's experiences with totalitarianism in the twentieth

authorities and information technology, 33 COMPUTER LAW & SECURITY REVIEW 421–433 (2017).

[23] For a summary of the US system, see Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 324 (Beate Roessler & Dorota Mokrosinska eds., 2015); For the state of privacy law in the US, and how its substantive protections are weaker than in other countries, see Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355 (2015).

[24] Robert Post, *Three Concepts of Privacy*, 89 GEORGETOWN LAW JOURNAL 2087 (2001).

[25] James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 THE YALE LAW JOURNAL 1151 (2003).

[26] PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY, (1 edition ed. 2008); See also Agustín Rossi, *How the Snowden Revelations Saved the EU General Data Protection Regulation*, 53 THE INTERNATIONAL SPECTATOR 95–111 (2018).

century.[27] For example, Wolfgang Kilian suggests that WW2 experiences, including long-standing intellectual and cultural issues of privacy in the private sphere, made Germany one of the first countries in the world to adopt data privacy codes, and to this day Germans remain particularly concerned about the invasion of privacy.[28]

However, lack of private sector regulation in the US cannot be accounted for solely by different philosophical conceptions of society and liberty. The resistance to the regulation of private actors in the US comes from influential businesses, who instead powerfully argued for self-regulation as an effective means to protect individuals (or 'consumers') in the USA.[29] This approach, dictated by a 'law and economics' mindset and considerations of efficiency[30] is often described as the 'FTC-model', so-named after the US Federal Trade Commission (FTC). The FTC-model has gradually become the main venue of enforcement for data protection and privacy in the US.[31]

The EU Adequacy Criterion

[27] See, eg, LE DROIT DE LA PERSONNALITÉ, (1992); G. W. GREENLEAF, ASIAN DATA PRIVACY LAWS : TRADE & HUMAN RIGHTS PERSPECTIVES (2014); David Lindsay, *An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law*, 29 MELBOURNE UNIVERSITY LAW REVIEW 131, 134 (2005); RAMON MULLERAT, *EU-US Data Protection Vindicating Rights to Privacy* 16 (2007), http://aei.pitt.edu/8197/ (last visited Aug 11, 2020); Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J. L. & PUB. POL'Y 605 (2013); STRATEGIES OF THE EU AND THE US IN COMBATING TRANSNATIONAL ORGANISED CRIME, (Brice de Ruyver, G. Vermeulen, & Tom Vander Beken eds., 2002).

[28] W Kilian, *Germany*, *in* GLOBAL PRIVACY PROTECTION 80–106 (James B. Rule & Graham Greenleaf eds., 2008).

[29] See, eg, PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995) chapter 4; See also PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR, (Russell Miller ed., 2017).

[30] For a rich overview of the FTC role in data privacy, see CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

[31] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA LAW REVIEW 583 (2014).

At the same time, during the early 1990s, the EU coordinated extensive consultations and discussions to harmonize domestic legislation of Member States and strengthen the Single Market by enabling enable data flows within the European Economic Area (EEA). This culminated in the development of distinctively European standards of data protection - the EU Data Protection Directive in 1994 ('EU Directive') [32] – which aimed to establish similar data protection principles in the EU Member States. The EU Directive regulated the processing of personal data within and between Member States, recognising the increasing importance of data transfers and analysis in an increasingly technologized world. By focussing on concerns relating to transparency, the purpose of the data processing, and the proportionate use of personal data as assessed by supervisory authorities, the EU evinced a clear intention to provide its population with strong-form data protection rights.

Importantly for international disagreements and data transfers, the EU Directive established an 'adequacy' criterion – a 'border control' approach to data transfers beyond the EU. This approach, originally articulated under Article 25 of the Directive, requires the EU Member States to limit personal data transfers to third countries unless they are able to establish an 'adequate' level of protection:

> '1.The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the

[32] EUROPEAN PARLIAMENT AND EUROPEAN COMMISSION, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281 31 (1995), http://data.europa.eu/eli/dir/1995/46/oj/eng (last visited Aug 11, 2020) art 3(2). The Directive was incorporated into the EEA 1992 Agreement on 25/06/1999 and in addition to EU Member States, it binds Norway, Iceland and Liechtenstein.

> other provisions of this Directive, the third country in question ensures an adequate level of protection.'[33]

Interestingly, the initially proposed requirement for countries to provide 'equivalent' protection in the draft of the EU Directive was watered-down due to effective lobbying from US companies such that they only have to provide 'adequate' protection.[34] This lower standard was replicated under Article 45 of the General Data Protection Regulation ('GDPR'), which has replaced the EU Directive, when it came into force in May 2018:

> '1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.'[35]

The GDPR further provides that the third countries' level of personal data protection is determined by the European Commission, which, when making such an assessment must take into account the 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation'; 'the existence and effective functioning of one or more independent supervisory authorities;' and 'the international commitments' or 'other obligations.'[36]

---

[33] *Id.* art 25(1).
[34] See Priscilla Regan, *American Business and The European Data Protection Directive: Lobbying Strategies and Tactics*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 199–216 (Colin J. Bennett & Rebecca Grant eds., 1 ed. 1999).
[35] EUROPEAN PARLIAMENT AND EUROPEAN COUNCIL, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 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*, 119 OJ L 1–88 (2016) art 45.
[36] *Id.* art 45(2).

Only a very small number of countries have been recognized as 'adequate' for the purpose of the EU data protection law, and many of them are small jurisdictions located on the European continent with tight political, administrative, and economic relationships with certain EU Member States or the UK. [37] To date, the EU Commission has recognized Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the US (limited to the now invalidated the Privacy Shield framework) as providing adequate levels of data protection. South Korea has announced that it is seeking an adequacy assessment.[38] India has in the past attempted to obtain an adequacy finding but was unsuccessful.[39] The Commission's adequacy decision may be limited also to specific territories or to more specific sectors within a country. The GDPR envisages that the European Commission would review its adequacy decisions at least every four years. Such a decision can be repealed, amended or suspended without retro-active effect.

Unsurprisingly, the 'adequacy' requirement has caused considerable controversy in countries that would potentially be recognized as 'inadequate', particularly the US, where the Directive was regarded as setting a dangerous precedent for re-imposing government regulation over e-commerce, even though it was drafted before the so-called e-commerce revolution in 1995.[40] The legality of the 'adequacy' requirement was also questioned by some US scholars under international law and the General Agreement on Trade in Services ('GATS'), which restricts signatory states from imposing restrictions on international data flows in a manner

[37] There are 11 Jurisdictions recognized as 'adequate' by the EU Commission; see European Commission, *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.* (2019), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Aug 11, 2020).
[38] See Graham Greenleaf, *International Data Privacy Agreements after the GDPR and Schrems*, 139 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 12–15 (2016).
[39] Graham Greenleaf, *India's Draft the Right to Privacy Bill 2014 – Will Modi's BJP Enact it?*, 129 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21 (2014).
[40] See generally PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

involving arbitrary or unjustified discrimination against other states.[41] Despite these concerns, no legal claim has been brought challenging the legality of the 'adequacy' requirement.[42]

Because of these strong external effects, the EU Directive was perceived as a window for policy change in the US. Privacy advocates expected that the Directive would help to lobby for the federal data protection legislation in the US, that would satisfy the European 'adequacy' criterion.[43] However, these expectations encountered strong resistance from domestic corporate interests in the US in two ways. First, the US legislative process is complicated and challenging for any reform packages to pass through because it allows vetoes at numerous stages of the procedure.[44] Second, the US's liberal market economy generally favours business interests over those of the citizen or consumer.

This is not to say that the 1995 EU Data Protection Directive did not have any impact on developments in the US. For example, Gregory Shaffer has observed that the policy reports commissioned by the European Commission for examining the level of protection in different sectors in the US might have helped to trigger the enactment of the *Health Insurance Portability and Accountability Act of 1996* in the US.[45] Similarly, the enactment of the

---

[41] UNITED NATIONS, *GATS: General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B*, 1867 U.N.T.S. 410 (1994) See especially Arts II(1), VI(1), XIV(ii) and XVII; SWIRE AND LITAN, *supra* note 41 at 189–193; For a comprehensive account of the potential interaction between EU privacy and data protection laws, and the GATS, see S Yakovleva & K Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 191 (2016).

[42] For an overview on trade agreements and data privacy as well as a scholarly debate on potential challenges to data privacy under the WTO, see Graham Greenleaf, *The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?*, No. 2016-08 SSRN ELECTRONIC JOURNAL (2016).

[43] Priscilla M. Regan, *The Globalization of Privacy: Implications of Recent Changes in Europe* (1993).

[44] See G. Tsebelis, *Veto players and institutional analysis*, 13 GOVERNANCE 441–474 (2000).

[45] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards*, 25 YALE JOURNAL OF INTERNATIONAL LAW 1, 25–26 (2000).

US Children's Online Privacy Protection Act (COPPA) in 1998 has been traced to the impact of the EU Data Protection Directive, even if indirectly.[46]

However, despite these minor indirect impacts, the Clinton Administration strongly opposed a comprehensive regulation approach, such as that created by the EU Data Protection Directive, and instead attempted to establish an alternative mode of regulation based on self-regulation and 'privacy seal' organizations which would certify that certain companies are to be trusted online by consumers with special branding and logos.[47] Such regulatory approach mirrored the stance and viewpoints of the main US technology industry actors, who preferred to treat data protection as part of the US e-commerce strategy and opposed any e-commerce regulation.[48] The strong bargaining power and position of corporate entities in the US precluded the EU from instigating comprehensive private sector regulation reform in the US.

Bridging the EU–US Differences: The Safe Harbor Arrangements

However, the form of self-regulation that the US government and its corporate actors promoted internationally was not accepted by the Europeans either. In particular, it was the European Parliament and some Member States' DPAs who opposed pure self-regulation, while the EU Commission often sided with its US counterparts.[49] Yet, both the US and the EU agreed that no cooperation at all – which meant no international data transfers – was not an acceptable solution to the problem, and thus it is the least favoured

[46] HOOFNAGLE, *supra* note 31 at 193.
[47] See Clinton Administration, *The Framework for Global Electronic Commerce*, THE WHITE HOUSE (1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/ (last visited Jul 24, 2020).
[48] David Bach & Abraham L. Newman, *The European regulatory state and global public policy: micro-institutions, macro-influence*, 14 JOURNAL OF EUROPEAN PUBLIC POLICY 827–846, 833–34 (2007).
[49] This is especially so for the Safe Harbour negotiations, discussed below. See generally Henry Farrell, *Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement*, 57 INTERNATIONAL ORGANIZATION 277–306 (2003).

outcome of the 'game' of data privacy policy for both players. However, each player favoured a particular model for data protection. Therefore, the main question was which model would prevail: American-style self-regulation or stringent full coverage European-style data protection rules?

These differences in data protection policy between the EU and USA resulted in the 'Safe Harbor' arrangement, adopted in 1998.[50] The Safe Harbour provided arrangement where US businesses could 'self-certify' that they provided 'adequate' protection for the purpose of the EU Directive if they agreed voluntarily to be bound by a set of data protection principles.[51] These principles included:

> *'Notice* – Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.
> *Choice* – Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.
> *Onward Transfer* – Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
> *Security* – Reasonable efforts must be made to prevent loss of collected information.
> *Data Integrity* – Data must be relevant and reliable for the purpose it was collected.

[50] Commission Decision of 26 July 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000D0520-20000825 (last visited Jul 23, 2020).
[51] *Id.*; For Safe Harbor negotiations, see Farrell, *supra* note 50; DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION (2005).

> *Access* – Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.
> *Enforcement* – There must be effective means of enforcing these rules.' [52]

The enforcement of these principles was of a hybrid nature that included a combination of various public and private actors.[53] Some important data protection principles under the EU Directive were significantly 'relaxed' under the Safe Harbour. For example, the 'purpose limitation' (requiring data processing to be limited to the purposes for which it was collected) was turned into a much more lower principle of 'choice' under Safe Harbour, which was enforced largely through private dispute resolution mechanisms.[54]

Only companies within the jurisdiction of the FTC – which excludes entire financial, insurance sectors and air carriers – could self-certify compliance with the Safe Harbour principles.[55] Many US tech companies, such as Facebook, Amazon, and Apple relied on Safe Harbour to continue their business model of collecting and processing personal data in the EU and transferring in to the US. The Safe Harbour agreement displays the enormous bargaining power of the US and its corporate entities on international scale, because this arrangement so significantly limited the impact and extraterritorial effects of EU data protection law in order to accommodate US exceptionalism and enable its powerful corporate actors to operate with little hindrance from the EU data protection laws.

---

[52] SAFE HARBOUR DECISION, *supra* note 51.
[53] Detailed information about Safe Harbor is available at International Trade Administration, *Search the U.S. - EU Safe Harbor List*, EXPORT.GOV , https://www.export.gov/safeharbor_eu (last visited Aug 11, 2020).
[54] See Bilyana Petkova, *Domesticating The 'Foreign' in Making Transatlantic Data Privacy Law*, 15 INTERNATIONAL JOURNAL OF CONSTITUTIONAL LAW 1135–1156, 8 (2017).
[55] Under Section 5 of the Federal Trade Commission Act banks, savings and loan institutions, as well as federal credit unions and air carriers are excluded from FTC jurisdiction; See UNITED STATES CONGRESS, *Title 15 Commerce and Trade*, 15 U.S.C § 45 (a)(2).

Schrems' Complaint and the US Surveillance Programmes

It was in this policy context of the special EU-US data sharing arrangements that Max Schrems argued that the legal basis for EU-US transfers, provided under the Safe Harbour arrangement, was invalid in light of the 2013 revelations about the mass surveillance programmes. The scope of the US surveillance programmes and the extent of collusion between the US tech industry and government interests first became apparent after a former NSA contract computer analyst, Edward Snowden, leaked classified documents about secret mass-surveillance programmes in 2013. As the famous story in the *Guardian* and the *Washington Post* reported, the NSA was accessing the emails, documents, photographs and other sensitive data of users from Facebook, Google, Apple, Microsoft, and five other major tech giants under a secrete programme called PRISM.[56] Many other programmes were soon revealed, and even though the NSA had been engaging in surveillance activities previously, the extent of complicity of big tech drew a grey cloud over the US tech industry's previously undamaged image. Simultaneously, it became known that the NSA UPSTREAM program directly accessed communications made via fibre cables and other transmission infrastructure. This surveillance method could be conducted without a warrant where it related to collection relating to foreigners thought to be overseas.[57]

---

[56] Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN, June 7, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (last visited Jul 23, 2020); Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, THE WASHINGTON POST, June 7, 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (last visited Jul 24, 2020).

[57] Craig Timberg, *NSA slide shows surveillance of undersea cables*, WASHINGTON POST, July 10, 2013, https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (last visited Jul 23, 2020).

These programmes were authorized under the *US Foreign Intelligence Surveillance Act* ('*FISA*') passed by the US Congress in 1978.[58] FISA is a separate regime from the ordinary law enforcement surveillance framework under Title III (known as the 'Wiretap Statute'),[59] because it focuses the government's collection of 'foreign intelligence' information for the purpose of advancing US counterintelligence goals. FISA was initially limited to electronic eavesdropping and wiretapping, but it was amended in 1994 to cover covert physical entries in connection with 'security' investigations, and again in 1998 to cover pen/trap orders.[60] Of particular relevance is section 702 of FISA, which allows the US government to search, collect, and process foreign intelligence from non-US citizens located outside of the US jurisdiction, without the need for a warrant. Additionally, the *1981 Executive Order 12,333 (EO-12,333)* reinforced the need and ability to collect 'timely and accurate information' for the 'national security of the United States'.[61]

In light of the revelations about the lack of safeguards for personal data under the US foreign intelligence framework and the secret US programmes, Max Schrems challenged the legality of data transfers to the US by lodging a complaint with the Irish Data Protection Commissioner ('DPC'). The EU constitutional architecture allows individuals to raise challenges to EU legal measures which directly and individually affect them.[62] Typically,

---

[58] UNITED STATES CONGRESS, *Foreign Intelligence Surveillance Act*, 92 Stat. 1783; 50 U.S.C. ch. 36 § 1801 et seq (1978).

[59] UNITED STATES CONGRESS, *18 U.S. Code Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communication*, 82 Stat. 212 (1968).

[60] UNITED STATES CONGRESS, *Counterintelligence and Security Enhancements Act* (1994); UNITED STATES CONGRESS, *Intelligence Authorization Act for Fiscal Year 1999* (1998).

[61] President Ronald Reagan, *Executive Order 12,333 - United States intelligence activities*, NATIONAL ARCHIVES (1981), https://www.archives.gov/federal-register/codification/executive-order/12333.html (last visited Aug 11, 2020).

[62] See EUROPEAN UNION, *Treaty on the Functioning of the European Union*, OJ C 3262 47–390 (2012) art 263 263 ("[A]ny natural or legal person may, under the same conditions, institute proceedings against a decision addressed to that person or against a decision which, although in the form of a regulation or a decision addressed to another person, is of direct and individual concern to the former."); see also Xavier Lewis, *Standing of Private Plaintiffs to Annul Generally*

the primary avenue to challenge the legality of EU legislation is to begin proceedings before national courts or regulatory bodies,[63] such as the Irish DPC. This is because, typically, the EU adopts legislation which must then be implemented by Member States legislatures.[64] National courts of last instance are required to refer a question to the CJEU where the validity or interpretation of an EU measure is at stake, through what is known as the preliminary reference procedure.[65]

The Irish DPC initially dismissed Schrems' complaint based on the existence of a 'Safe Harbour Decision', which is an EC 'adequacy' decision. Max Schrems then took the matter to the High Court of Ireland, which referred two questions to the CJEU in a case now known as *Schrems I*: first, whether the DPAs are bound by EC adequacy decisions, such as that pertaining to Safe Harbour; and second, whether the DPAs have an ability (or obligation) to investigate the safeguards under (or despite of) an adequacy decisions.

As is typical in EU Law, before the CJEU delivers its judgment it received independent legal advice from the Advocate General ('AG') on how the case should be decided. In the *Schrems I* proceedings, AG Bot delivered his Opinion in 2014. While the AG Opinions generally influence the deliberations of the Court, they are not legally binding, and CJEU does not always follow them.[66]

Applicable European Community Measures: If the System is Broken, Where Should it be Fixed?, 30 FORDHAM INTERNATIONAL LAW JOURNAL 1496 (2003).

[63] See generally MONICA CLAES, THE NATIONAL COURTS' MANDATE IN THE EUROPEAN CONSTITUTION (Edición: UK ed. ed. 2006) (explaining the role of national courts in enforcing EU law).

[64] Daniel Halberstam, *Comparative Federalism and the Issue of Commandeering*, *in* THE FEDERAL VISION: LEGITIMACY AND LEVELS OF GOVERNANCE IN THE UNITED STATES AND THE EUROPEAN UNION 213 (Kalypso Nicolaidis & Robert Howse eds., 2001) (explaining that in most contexts, the EU delegates implementation of laws to the member states).

[65] TFEU, *supra* note 62 art 267 (stating that the ECJ "shall have jurisdiction to give preliminary rulings concerning [a] the interpretation of the Treaties; [and] [b] the validity and interpretation of acts of the institutions of [the Community]" upon referral by a national court).

[66] EUROPEAN PARLIAMENT AND EUROPEAN COUNCIL, *Protocol No. 3 on the Statute of the European Court of Justice*, 2010 O.J. (C 83) 210 art 20 (stating that as

The AG Bot recommended that the CJEU find that the presence of an adequacy decision does not prevent investigation of complaints made to DPAs and, more controversially, that Safe Harbour be found invalid.[67] The CJEU agreed, and in its *Schrems I* judgment delivered in 2015, invalidated the EC Safe Harbour Decision[68] which had authorised personal data transfers from the EU to the US since 2000.[69] The CJEU held that the transfer of personal data by Facebook to the US for a commercial purpose, then subjected to further processing by US public authorities for national security purposes, coupled with a lack of processes by which EU citizens can raise concerns, resulted in Safe Harbour not ensuring essentially equivalent protection as required by Article 25(6) DPD, read in the light of EUCFR.[70]

After the invalidation of Safe Harbour in 2015, the Irish Court referred Schrems' complaint back to the Irish DPC, who then asked Schrems to reformulate his original complaint since Safe Harbour was already invalidated at that time. Facebook and other US tech companies, who have been operating under the Safe Harbour regime, after its invalidation then relied upon the Standard Contractual Clauses - another private legal mechanism under the EU law - to provide an 'adequate' protection for personal data under EU Law. Standard Contractual Clauses are one of the exceptions to the general 'adequacy' rule found in Article 46(1) GDPR (and previously in Article 26 of the Data Protection Directive). In particular, Article 46 of the GDPR articulates that

---

a general rule, the CJEU shall decide cases only after having received a submission from the Advocate General, save for when a case raises no new point of law); The Advocate Generals' opinions often play an influential role in the ECJ's deliberations; however, the Advocate Generals' opinions technically have no binding effect PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXT, CASES, AND MATERIALS (6 ed. 2015) There are multiple cases in which the ECJ has not followed the Advocate General's opinion in its ruling, including in the present case in Schrems II.

[67] Advocate General, Opinion of Advocate General Bot, Maximillian Schrems v Data Protection Commissioner, 237 (2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CC0362 (last visited Jul 23, 2020).

[68] SAFE HARBOUR DECISION, *supra* note 51.

[69] Grand Chamber Court of Justice of the European Union, C-362/14 Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, 80–82, 86 (2015).

[70] *Id.* at 96–98, 103–106.

personal data can be transferred to a third country even in the absence of an adequacy decision if data exporters provide appropriate safeguards; and on the condition that enforceable data subject rights and effective legal remedies are available in the given country. The appropriate safeguards, under Article 46 of the GPDR, can be laid down in the following most relevant instruments:

- Binding corporate rules - an internal code of conduct adopted by multinational corporations, under Article 47 GDPR, and allow transfers between different entities of the company;
- Standard Contractual Clauses adopted by the EC or by a national DPA and approved by the EC;
- Other ad hoc contractual clauses agreed between the data exporter and the data importer which can be deemed to be appropriate if they have been submitted and authorized by the competent DPA.

Schrems' revised complaint focused on Facebook data transfers outside of the EU based on SCCs. Schrems argued that Facebook's reliance on SCCs could not be valid because, under US law, private companies must provide US national security agencies with access to data transferred from the EU, and this arguably fails to satisfy the conditions under Article 26 of the Data Protection Directive (and now replaced by Article 46 GDPR).[71]

Based on Schrems' revised complaint, the DPC requested a determination from the High Court of Ireland. The Irish High Court reasoned that mass and indiscriminate processing of personal data processing by the US authorities under surveillance programmes might expose the data subjects to a risk of a violation of the rights which they derive from Articles 7 and 8 of the

[71] *Schrems II*, *supra* note 7 at 151-153.

Charter.[72] Sharing the DPCs doubts on the validity of the SCC Decision, the Irish High Court decided to seek clarification from the CJEU by referring 11 questions to the CJEU in a case now called *Schrems II*.[73] These questions primarily focused on the validity of the SCC Decision and actions DPAs can take, therefore shifting the focus towards validity of SCCs and, only by inference, the validity of the new EU-USA agreement – called Privacy Shield - which replaced Safe Harbour after Schrems has revised his complaint.[74]

The EU-US Privacy Shield was negotiated by the EU Commission and the US Department of Commerce soon after Safe Harbour was invalidated.[75] That arrangement again established a 'self-certified' regime for EU-US data transfers. The Privacy Shield contained requirements for: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability. Unlike Safe Harbor, the Privacy Shield included an arbitration model and commitments from US national security officials. The US Secretary of Commerce Penny Pritzker called the agreement 'a tremendous victory for privacy for individuals, and businesses on both sides of the Atlantic', one that would 'help grow the digital economy by ensuring that thousands of European and American businesses and millions of individuals can continue to access services online.'[76]

---

[72] The High Court, The Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 193 (2017), http://www.europe-v-facebook.org/sh2/HCJ.pdf (last visited Jul 23, 2020).

[73] High Court (Ireland), *Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (2018), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62018CN0311&from=EN (last visited Jul 23, 2020).

[74] EUROPEAN COMMISSION, *Commission Implementing Decision (EU) 2016/1250 of 12 July 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) (Text with EEA relevance)*, OJ L 207 1–112 (2016), http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng (last visited Jul 23, 2020).

[75] *Id.*

[76] The agreement and ancillary documents are at International Trade Administration, *Privacy Shield*, PRIVACY SHIELD FRAMEWORK ,

However, many noted that the Privacy Shield failed to address the CJEU's core concerns in multiple respects: fundamental rights safeguards of Privacy Shield were too limited, the newly created Ombudsperson mechanism did not guarantee full redress for individuals, and commercial transactions are mixed with the regulation of law enforcement access to privately held data.[77] It was still strikingly similar to the now invalidated Safe Harbour regime.[78]

II. THE CJEU JUDGMENT IN *SCHREMS II*

The CJEU delivered its *Schrems II* judgment on the 16th July 2020, which invalidated the Privacy Shield for data transfers between the US and the EU. While it found that the SCC could be valid in certain circumstances, the inadequacy of safeguards in the US meant that the nation did not provide 'essentially equivalent' safeguards to those present under EU law. Consequently, the use of SCC's to transfer personal data between the EU and US was declared to breach EU law requirements, removing lawful mechanisms for such transfers to go forward. This section briefly outlines the Opinion of AG, before looking at CJEU's judgement in more detail.

The Opinion of the Advocate General

Before the CJEU delivered its judgment, it received independent legal advice from AG Saugmandsgaard Øe, who recommended that the CJEU declare the SCCs a valid mechanism for data transfer

https://www.privacyshield.gov/welcome (last visited Jul 23, 2020); Pritzger's laudatory words can be found at Nathalie Thomas, *Europe and US agree new data privacy deal* (2016), https://www.ft.com/content/1f849862-c3af-3062-9766-d7edcff7ddd7 (last visited Jul 23, 2020).

[77] See also Maria Tzanou, *European Union Regulation of Transatlantic Data Transfers and Online Surveillance*, 17 HUMAN RIGHTS LAW REVIEW 545–565, 565 (2017).

[78] *Id.* at 563.; CHRISTOPHER KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems* 20 (2017), https://papers.ssrn.com/abstract=2732346 (last visited Jul 23, 2020); MARTIN A. WEISS & KRISTIN ARCHICK, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield* 9–10 (2016).

beyond the EU under Articles 46(1) of the GDPR.[79] However, the continued validity of the SCC, according to the AG, depended on a requirement that companies undertake additional measures to assure compliance and adequacy of safeguards in the third country. In particular, the AG argued that data exporters must make specific assessments with regard to the compliance of a data importer with the SCC contractual terms.[80] Such an examination would require consideration of:

> 'all of the circumstances characterising each transfer, which may include the nature of the data and whether they are sensitive, the mechanism employed by the exporter and/or the importer to ensure its security, the nature and the purpose of the processing by the public authorities of the third country which the data will undergo, the details of such processing and the limitations and safeguards ensured by that third country'.[81]

Further, the AG indicated that supervisory authorities must declare illegality where appropriate protections to satisfy the contractual clauses are not complied with.[82] This strict application of the SCC terms, according to the AG, would place additional burdens on the

[79] Advocate General, Opinion of Advocate General Saugmandsgaard Øe, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, interveners: The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope E, 120 (2019), http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=141944 (last visited Jul 23, 2020); Marcus Evans et al., *Schrems II: AG deems SCCs valid but comes up with difficult new obligations and expresses "doubts" over privacy shield*, DATA PROTECTION REPORT (2019), https://www.dataprotectionreport.com/2019/12/schrems-ii-ag-deems-sccs-valid-but-comes-up-with-difficult-new-obligations-and-expresses-doubts-over-privacy-shield/ (last visited Jul 23, 2020); The Advocate General tends to provide an opinion prior to the decision of the ECJ. However, while these opinions are influential on the deliberations of the Court, they are not binding Federico Fabbrini, *Human Rights in the Digital Age*, 28 HARVARD HUMAN RIGHTS JOURNAL 65, 80 (2015).

[80] ADVOCATE GENERAL, *supra* note 80 at 129–139.

[81] *Id.* at 135.

[82] *Id.* at 140–160.

data exporter, as it requires investigations of the national security laws of the data importer country.[83]

Finally, the AG *Saugmandsgaard Øe's* also recommended the Court should not engage with questions on the validity of Privacy Shield,[84] as this question was not specifically referred to the CJEU by the High Court.[85] A direct challenge on the validity of Privacy Shield was underway in the General Court (*Quadrature du Net*, Case T-738/16).[86] However, this did not dissuade the AG from expressing strong doubts as to the validity of Privacy Shield,[87] given his extensive analysis of the adequacy of safeguards provided by the US law.[88]

In relation specific to whether the US legislative and judicial protections were sufficient to satisfy the requirements of the SCC, the AG raised specific doubts with respect to firstly, the surveillance safeguards in the US being equivalent to those of the General Data Protection Regulation ('GDPR') and the EUCFR,[89] and secondly, whether the existence of a Privacy Ombudsperson was a sufficient compensation for the lack of judicial protection afforded to those whose data is transferred to the US.[90] Ultimately, the AG found that while the SCC should not be impugned *in general*, it was open (an in fact necessary) to supervisory authorities to declare illegal *specific* instances of data transfers between the EU and US which did not comply with the SCC terms. However, as described in the following paragraphs, the Court's reasoning diverged from that of the AG by finding the SCC, when used to transfer data between the EU and US, is illegitimate.

The CJEU Judgment

[83] *Id.* at 108. 131.
[84] *Id.* at 161–166, 187.
[85] *Id.* at 179.
[86] *Id.* at 179.
[87] *Id.* at 340–341.
[88] *Id.* at 187–342.
[89] *Id.* at 231–308.
[90] *Id.* at 309–342.

Emphasizing the significance of the case, the CJEU decided to rule on the preliminary reference request as a Grand Chamber—a special 15-judge composition reserved for high-profile cases—and, on the 16th of July 2020, delivered its ruling. After summarising the law and the facts, the CJEU began by noting that the questions before the Court would be answered the questions put before it by reference to the GDPR.[91] The Court interpreted the provisions in Articles 2-4 of the GDPR, finding that the GDPR applies to the transfer of personal data for commercial purposes between a Member State and an economic operator established in a third country.[92] Further processing of the data for national security purposes did not invalidate the application of the GDPR.[93]

The Court confirmed the validity of the SCC Decision, highlighting that SCCs can be validly used under Article 46(1) GDPR where the safeguards in the contractual terms provided an 'essentially equivalent' of protection for the data transferred from the EU.[94] When assessing the level of protection afforded, the agreed contractual clauses between the data controller and the third country recipient/processor, any access by public authorities to the data and the legal system of the third country should be considered.[95] These safeguards are outlined under Chapter V of the GDPR,[96] and must afford appropriate safeguards, enforceable rights and effective legal remedies.[97] Data controllers still have an obligation to act if there is a conflict between the SCC and local laws, including suspending data flows.[98] In circumstances where the SCC cannot provide an essential equivalent to EU law, and data controllers have not acted, it is the role of DPAs[99] to suspend, limit,

[91] *Schrems II*, *supra* note 7 at 79.
[92] *Id.* at 89.
[93] *Id.* at 89
[94] *Id.* at 105.
[95] *Id.* at 105.
[96] *Id.* at 93.
[97] *Id.* at 103.
[98] *Id.* at 134-135.
[99] DPAs are independent public authorities that supervise the application of data protection laws, by providing expert advice and handling complaints with respect to violations of the GDPR. Each EU Member State has a DPA. See further European Commission, *What are Data Protection Authorities (DPAs)?*,

or even ban international data transfer.[100] This is particularly pertinent where an SCC cannot be complied with (due to local laws) or are not been complied with by the data importer. If the circumstances arise under SCCs where Member State DPAs have diverging opinions about the adequacy of safeguards in third country, the CJEU highlighted that the matter should be referred to the European Data Protection Board for an opinion.[101] Ultimately, the Court held that SCCs were a valid mechanism for ensuring essentially equivalent protections in third countries and as such the SCC Decision was found to be valid.[102]

However, the CJEU found that the obligation of DPAs to suspend, limit, or ban data transfers is prevented where there is an adequacy decision, such as the Privacy Shield.[103] The adequacy decisions by the EC must be adhered to and DPAs 'cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection'.[104] Instead, DPAs must investigate the complaints received, and if concerned about the adequacy of protection, bring an action before national courts, who can, in turn, make a reference for a preliminary ruling by the CJEU on the validity of an adequacy decision.[105] Given that in the present case, the High Court of Ireland had already expressed concerns around the adequacy of the protection under Privacy Shield,[106] the CJEU then undertook an examination of the current protection under US law to determine the validity of Privacy Shield.

The Court ultimately found the Privacy Shield invalid because of the largely unrestrained surveillance regime, a lack of redress under those regimes and the lack of independence for the

---

EUROPEAN COMMISSION , https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (last visited Jul 24, 2020).

[100] *Schrems II*, *supra* note 7 at 113, 121.

[101] *Id.* at 147.

[102] *Id.* at 148-149.

[103] *Id.* at 156.

[104] *Id.* at 118.

[105] *Id.* at 157.

[106] *Id.* at 159.

Ombudsperson.[107] In this regard, the CJEU first noted the European Commission could only make a decision on adequacy if 'the third country's relevant legislation' provides 'all the necessary guarantees' to conclude that the 'legislation ensures an adequate level of protection'.[108] Further, the EC must give reasons as to why the third country provides 'a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order'.[109] These reasons could include the assurance of that standard through domestic law or international commitments.[110] The Court then moved to assess the level of protection afforded by the US. First, it held that US surveillance regimes permitted under *section 702 of the FISA* (which, as explained in Part II of the paper, authorises programmes like PRISM and UPSTREAM), failed to meet the principle of proportionality, as it was not limited to what was strictly necessary: it did not lay down any limitations or scope of the programmes nor impose any minimum safeguards.[111] Further, the *Executive Order 12,333* and the 2014 *Presidential Policy Directive 28 (PPD-28)*, which was established after Snowden revelations to govern 'signals intelligence activities',[112] did not grant actionable rights to individuals, failing to provide effective and enforceable rights against US authorities.[113]

The CJEU also noted that the EU legal order also provides a right to a hearing before an independent and impartial tribunal.[114] While the Privacy Shield Decision made provision for an Ombudsperson, surveillance programs based on section 702 of the FISA and *Executive Order 12,333,* even when read in conjunction with the 2014 PPD–28, do not provide data subjects with actionable rights, leaving no effective remedy against US

[107] *Id.* at 199.
[108] *Id.* at 129.
[109] *Id.* at 162.
[110] *Id.* at 162.
[111] *Id.* at 179-180.
[112] President Barack Obama, *Presidential Policy Directive 28 -- Signals Intelligence Activities* (2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (last visited Aug 11, 2020).
[113] *Schrems II*, *supra* note 7 at 181-182, 184.
[114] *Id.* at 186.

authorities.[115] Consequently, the Court concluded that these surveillance regimes could not provide minimum safeguards as, under the principle of proportionality, they were not limited to what was strictly necessary.[116] Therefore, the US surveillance regime had failed to protect the right to respect for his or her private and family life, home and communications and the right to the protection of personal data concerning him or her, as required by the EU law. Similarly, the CJEU found that the appointment and/or dismissal of the Ombudsperson was not surrounded by guarantees which would prevent interference from the executive branch of government.[117] Thus, the Privacy Shield Decision could not provide 'essentially equivalent' safeguards for fundamental rights, to those guaranteed under the EU legal order, and was therefore invalid.[118]

III. THE CJEU PUSHBACK AGAINST DATA SECURITIZATION AND SURVEILLANCE

CJEU Developing a Principled Stance on Data Protection

Schrems II is the latest CJEU ruling among many on the role of data protection and privacy in the EU legal order in the context of increasing 'securitization' of data protection policy and surveillance. Following the Snowden revelations in 2013, the CJEU has been very vocal on the constitutional significance of data protection in EU legal framework well beyond the Schrems' saga. As I will explain in this section, the Court has delivered numerous

[115] *Id.* at 181-182, 192.
[116] *Id.* at 184.
[117] *Id.* at 194.
[118] *Id.* at 185, 191, 197.

judgments, including *Digital Rights Ireland*,[119] *Tele2 Sverige AB*,[120] and *Opinion 1/15 (Passenger Name Records)*,[121] which demonstrate CJEU's persistence in ensuring EU fundamental rights are protected in a world where surveillance has become the norm, not the exception.

These judgments started with the ground-breaking decision in *Digital Rights Ireland*, where the CJEU invalidated the EU Directive 2006/24/EC ('the Data Retention Directive'), because it represented a disproportionate and unjustified interference with the Articles 7 and 8 EUCFR, guaranteeing right to private life and data protection respectively. Concerns over data retention schemes in the EU and Member States have a long history - indeed, data protection and privacy advocates, DPAs as well the EU Parliament have been concerned about the data retention schemes, as well as PNR, SWIFT and other regimes since the early 2000s.[122] Similarly, national Courts of Member States have scrutinized domestic legislation implementing EU data retention regime in the Czech Republic, Romania, and Germany and found them incompatible with the fundamental rights of the citizens in those countries.[123]

---

[119] European Court of Justice, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, E.C.R. I-238 (2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first∂=1&cid=8886631.

[120] Court of Justice of the European Union, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis, ECLI:EU:C:2016:970 (2016).

[121] Grand Chamber, Court of Justice of the European Union, Opinion 1/15 of the Court, OJ C 138 (2017).

[122] For a detailed account, see E. Kosta, *The way to Luxemburg: National court decisions on the compatibility of the data retention directive with the rights to privacy and data protection*, 10 SCRIPTED 339–363 (2013).

[123] See The Czech Republic Constitutional Court Judgment In the Name of the Republic of 2011/03/22, (2011); Constitutional Court of Romania Decision No 1258, , Official Monitor of Romania No 798 (2009); German Federal Constitutional Court, Judgment the First Senate of 2 March 2010, 1 BvR 256/08; 1 BvR 263/08; 1BvR 586/08 (2010); For more details on these judgments and their relation to the Data Retention Directive, see Commission of the European Union, *Report from the Commission to the Council of the European Parliament: Evaluation Report on the Dadta Retention Directive (Directive 2006/24/EC)*, COM(2011) 255 Final (2011).

Soon after *Digital Rights Ireland*, in the *Schrems I* case, already mentioned in Part II of this article, the CJEU invalidated the EU Commission's decision on adequacy of data protection provided by the Safe Harbour agreement, which had facilitated EU-US data-sharing between 2000 and 2015.[124] In the subsequent *Tele2 Sverige or Watson case*,[125] arising out of a decision by the Swedish telecommunication operator to comply with *Digital Rights Ireland* decision in Sweden, the CJEU confirmed that ubiquitous data storage interfered seriously with the right to a private life, and extended the *Digital Rights Ireland* ruling to national data retention regimes in Member States. The Court further reinforced its commitment to the protection of fundamental rights in *Opinion 1/15 (Passenger Name Records)*[126] when it invalidated the proposed EU-Canada agreement on the transfer of PNR data due to lack of data protection safeguards and incompatibility of the agreement with EU fundamental rights framework.[127]

The Courts' pronouncement in Schrems II thus is fully consistent with, and fits well among, a number of recent far-reaching CJEU judgments, suggesting that the Court has now developed a strong principled position on the appropriate limits of data retention regimes and transfers of personal data to third countries, from which it is unlikely to depart in any near future. This principled approach on data protection and transatlantic data sharing in the judgments contrasts sharply with the CJEU's post 9/11 caution, when the Court restrained from ruling on the substantial validity and compliance of EU's international data sharing arrangements, such as PNR, with the EU data protection law.[128]

---

[124] *Screms I*, *supra* note 69.
[125] *Tele 2 Sverige*, *supra* note 120.
[126] *Opinion 1/15*, *supra* note 121.
[127] See further Monika Zalnieriute, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, 81 MODERN LAW REVIEW 1046–1063 (2018).
[128] Monika Zalnieriute, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, 81 MODERN LAW REVIEW 1046–1063 (2018).

The CJEU's recent progressive approach, which escalated after Snowden, has been criticised as 'hyper-constitutionalization' of data privacy in the EU through a 'CJEU project to constitutionalize transnational privacy politics'.[129] Some perceive this recent activism and constitutionalist ambitions by the CJEU as a 'largely self-congratulatory exercise that amounts to little actual advances for privacy rights "on the ground" and that uses a strategy of "othering" in order to build a specific European identity upon the very idea of privacy'.[130]

CJEU Pushing Against Data Securitization

Yet, I argue that the Courts principled approach and judicial activism should be understood within a broader historical and institutional context, and that it was the policy shock created, by the Snowden revelations, which have shifted an international data privacy discourse, and, in turn, resulted in a series of CJEU judgments that are much less tolerant towards the securitization and surveillance measures than in the pre-Snowden era. An emphasis on timing of political and legal events, that I will discuss below, illuminates that *Schrems II* is just the latest chapter in CJEU's pushback against mass surveillance and data securitization practices both within the EU and in international data sharing. As I have argued elsewhere,[131] the Snowden revelations has presented the CJEU with an opportunity to reinvent itself as a main champion of the fundamental right to data protection and privacy in the EU legal order and transatlantic relations. This trend of CJEU pushback against mass surveillance also fits well in the broader palette of CJEU decisions, championing human rights, including human dignity, non-discrimination on the basis of gender or sexual orientation, freedom of expression, social rights, and political entitlements.[132]

---

[129] Thomas Wischmeyer, *"Faraway, So Close!" – A Constitutional Perspective on Transatlantic Data Flow Regulation*, *in* OBAMA'S COURT: RECENT CHANGES IN U.S. CONSTITUTIONAL LAW IN TRANSATLANTIC PERSPECTIVE , 8–10 (Anna-Bettina Kaiser, Niels Petersen, & Johannes Saurer eds., 2018).
[130] *Id.* at 15.
[131] Zalnieriute, *supra* note 128 at 1055–6.
[132] Fabbrini, *supra* note 80 at 81–2.

Historical institutionalist analysis with its emphasis on timing of the political events and CJEU's pronouncements shows how the Snowden revelations provided the Court with a momentum to establish leadership and position itself as a champion of fundamental rights. The 'Snowden effect' in the EU immediately led to increased political scrutiny of both the commercial EU–US agreements, such as Safe Harbor, the PNR and SWIFT agreements, as well as law enforcement data sharing arrangements.[133] For example, following the Snowden revelations, the European Parliament aimed to introduce stricter rules on data transfers and retention with regard to private actors and, in particular, 'would require US companies to seek permission from European officials before complying with US government demands for private data on Europeans.'[134] Such post-Snowden climate enabled the CJEU to invalidate the *Safe Harbour* agreement in *Schrems I*. The reinforcement of that decision in *Schrems II* is a strong confirmation that the CJEU will no longer accept the transatlantic data sharing model with security interests at its centre, that the Court tolerated in the previous decades.

A joint approach of international law and international relations provides means to understand how the data sharing model with security interests at the heart – which the CJEU has now once more confirmed it rejects - was developed during the period between the September 11th 2001 terrorist attacks 9/11 and the Snowden revelations. Utilising a historical institutionalist lens and a process tracing methodology, allows us to understand how data protection

[133] The EP have raised questions about the security of PNR data and called for the suspension of the SWIFT agreement. For more on data privacy concerns in the field of law enforcement after Snowden, see PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR, *supra* note 30; MARIA TZANOU, THE FUNDAMENTAL RIGHT TO DATA PROTECTION: NORMATIVE VALUE IN THE CONTEXT OF COUNTER-TERRORISM SURVEILLANCE (2017); CRISTINA BLASI CASGRAN, GLOBAL DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT: AN EU PERSPECTIVE (2016).

[134] EU Parliament, *Q & A on EU Data Protection Reform*, EU PARLIAMENT NEWS (2013), http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (last visited Feb 13, 2014).

as a policy objective has been transformed and reoriented from what was once largely a commercial concern in both the EU and the US into a security and surveillance issue.

In particular, the original EU Data Protection Directive was adopted as a measure of the EU Internal Market in 1994, evincing an understanding of privacy as being an aspect of economic integration.[135] In the US, information privacy was dealt with by the US Department of Commerce, where data protection rules were largely framed as an obstacle to e-commerce in the early days of the Internet.[136] Process tracing, and an emphasis on timing, display how transatlantic data privacy policy negotiations after 9/11 have moved from DG Internal Market and the US Department of Commerce to security officials and interior ministers (EU) and the Department of Homeland Security and Treasury (US) respectively. [137] While formal transfer of data protection from the DG Internal Market to DG Justice and Home Affairs took place in March 2005, security officials and interior ministers have been heavily involved in transatlantic data protection negotiations since 9/11.

This policy shift, or what I call the 'securitization' of data protection policy, is also apparent in international data sharing agreements. For example, the SWIFT information exchange systems have been used for national security purposes more regularly and significantly since 9/11. For instance, in 2006, US authorities including the CIA attempted to gain access to SWIFT for terrorist finance tracing;[138] in 2012, the US Senate Banking Committee approved sanctions against SWIFT to pressure it into

[135] See, early texts on data protection from the 1990s, e.g,. G Pearce & N Platten, *Achieving personal data protection in the European Union*, 36 JOURNAL OF COMMON MARKET STUDIES 529 (1998).
[136] See, eg, the Clinton Administration's Clinton Administration, *supra* note 48.
[137] J ZARATE, TREASURY'S WAR: THE UNLEASHING OF A NEW ERA OF fiNANCIAL WARFARE (2013).
[138] CONSTANT BRAND, *Belgian PM: Data Transfer Broke Rules*, September 28, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html (last visited Jul 24, 2020).

terminating its ties with Iranian banks tied to terrorist activities;[139] in that same year, it was revealed that SWIFT transfers between two EU countries could be routed through the US and were therefore subject to domestic law surveillance and seizure risks.[140] In 2013, it was reported that the NSA intercepted and retained data transmitted via SWIFT.[141] After Snowden, the CJEU has pushed against securitization of such international data sharing agreements, as illustrated by the EU-Canadian PNR agreement struck down as invalid in the *Opinion 1/15*.

Some CJEU decisions, which covered commercial data processing by US tech companies can also be viewed as CJEU's pushback - even if indirect - against data securitization. For example, the CJEU's decision in *Google Spain* delivered in 2014, did not concern surveillance measures, but rather de-listing on search engines, where the Court held that Google (and search engines generally) had to consider individual requests to remove individual's name and links to web pages from the list of search results.[142] This decision, known as the 'right to be forgotten' case, also came out soon after the 2013 Snowden revelations that mass-surveillance was being conducted by the US through commercial data exchanges taking place on US tech infrastructure, including e-mail and social media platforms. In 2019, the CJEU somewhat limited

---

[139] Jay Solomon and Adam Entous, *Banking Hub Adds to Pressure on Iran*, WALL STREET JOURNAL, February 4, 2012, https://www.wsj.com/articles/SB10001424052970203889904577201330206741436 (last visited Jul 24, 2020) SWIFT disconnected Iranian banks from its networks in March 2012. They were mostly reinstated in 2016 with the lift of sanctions.

[140] Simon Bendtsen, Peter Suppli Benson & Simon Bendtsen og Peter Suppli Benson, *Dansk politimand fanget i amerikansk terrornet*, BERLINGSKE.DK (2012), https://www.berlingske.dk/content/item/564445 (last visited Jul 24, 2020).

[141] Spiegel International, *SPIEGEL Exclusive: NSA Spies on International Bank Transactions*, https://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html (last visited Jul 24, 2020); This claim was given increased strength in 2017 with the further release of documents outlining NSA monitoring activities: Clare Baldwin, *Hackers release files indicating NSA monitored global bank transfers*, REUTERS, April 15, 2017, https://www.reuters.com/article/us-usa-cyber-swift-idUSKBN17G1HC (last visited Jul 24, 2020).

[142] Court of Justice of the European Union, Case C-131/12 Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos, EU:C:2014:317 (2014).

the implication of *Google Spain* in *Google vs CNIL* by holding that Google does not have to to de-list its search results globally.[143] However, the Court found that worldwide de-referencing could still be required by Member States, leaving the glaring loophole in what supposedly looked like a limiting judgment.[144] These CJEU judgments suggest that commercial data processing could no longer be separated from national security issues after Snowden.

Consequently, the CJEU's pushback against data securitization, in a number of cases and most recently *Schrems II,* should not be viewed as simply or solely against the US surveillance policies; rather, it can be seen as disapproval of the EU's internal, transatlantic and international securitization policy and mass-surveillance regimes, which was embraced not only by the US but also by the EU Commission and Member States during the period between 9/11 and the 2013 Snowden revelations.

Political Climate Around Privacy Shield: Latest Developments in the US

Historical process tracing, distinguishing among different institutions inside a particular polity, also enables us to see that Schrems II outcome was not unexpected in the context of the political climate in the EU surrounding the Privacy Shield. It enables us to see that the EU is not a monolithic bloc and different EU institutions have different policy preferences. The EU Commission was very fast in negotiating and drafting the Privacy Shield Decision after the Safe Harbour was invalidated in 2015, which has raised strong doubts among other EU bodies about the quality of changes in the new proposed arrangements. While the EU Commission has defended the legality and safeguards provided under the Privacy Shield arrangements in three annual reviews,

[143] Court of Justice for the European Union, C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (2019).

[144] See further Monika Zalnieriute, *Google LLC v. Commission Nationale de l'informatique et des Libertés (CNIL)*, 114 AMERICAN JOURNAL OF INTERNATIONAL LAW 14 (2020).

delivered since its adoption in 2016.[145] The Commission did not receive a lot of support from other EU institutions.

For example, during the rushed negotiations of the Privacy Shield, the European Data Protection Supervisor ('EDPS') expressed concerns about the decision, and noted that the Privacy Shield now normalized what was previously an exceptional access for national security purposes:

> 'Whereas the 2000 Safe Harbour Decision formally treated access for national security as an exception, the attention devoted in the Privacy Shield draft decision to access, filtering and analysis by law enforcement and intelligence of personal data transferred for commercial purposes indicates that the exception may have become the rule.'[146]

Similarly, the European Parliament's Civil Liberties Committee has repeatedly recommended that the Privacy Shield was inadequate,[147]

---

[145] EUROPEAN COMMISSION, *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* (2019); EUROPEAN COMMISSION, *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* (2018); EUROPEAN COMMISSION, *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* (2017).

[146] As the EDPS observed: 'Whereas the 2000 Safe Harbour Decision formally treated access for national security as an exception, the attention devoted in the Privacy Shield draft decision to access, filtering and analysis by law enforcement and intelligence of personal data transferred for commercial purposes indicates that the exception may have become the rule.' See EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 04/2016 on the EU–U.S. Privacy Shield Draft Adequacy Decision* 2 (2016), https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf (last visited Mar 17, 2020).

[147] Claude Moraes, *European Parliament Resolution on the Adequacy of the Protection Afforded by the EU-US Privacy Shield* (2016), https://www.europarl.europa.eu/doceo/document/B-8-2018-0305_EN.html?redirect (last visited Mar 17, 2020); CLAUDE MORAES, *Amendments 1 - 88 Adequacy of the protection afforded by the EU-U.S. Privacy Shield* (2018).

and the European Parliament has called on the EU Commission to review and repeal the arrangement.[148]

The emphasis on sequencing and timing also enables us to track that the US foreign intelligence regime has not been fundamentally reformed since the Snowden revelations in 2013. The Obama administration encountered strong pressure following the leaks, and the 2014 *Presidential Policy Directive 28 (PPD-28)* governing 'signals intelligence activities'[149] was part of the mild reform package that was adopted. Soon after the Privacy Shield was negotiated in 2016, the US Foreign and Intelligence Surveillance Act (FISA) was amended in 2017 to re-authorize the surveillance scheme in the USA;[150] and raised further concerns at the European Parliament.[151] In 2018, breaches of section 702 FISA became public when declassified judicial opinions by the special FISA courts detailed how the US the FBI have conducted backdoor searches in violation of court orders and attempted to thwart oversight of the procedures.[152] Following the release of the opinions, the US Department of Justice issued a report on FISA in 2019,[153]and the *US Freedom Reuathorization Act 2020* was introduced into US

---

148 EU committee approves resolution against Privacy Shield, , https://www.telecompaper.com/news/eu-committee-approves-resolution-against-privacy-shield--1190285 (last visited Jul 23, 2020); Texts adopted - Adequacy of the protection afforded by the EU-US privacy Shield - Thursday, 6 April 2017, , https://www.europarl.europa.eu/doceo/document/TA-8-2017-0131_EN.html (last visited Jul 23, 2020).

149 President Barack Obama, *supra* note 113.

150 UNITED STATES CONGRESS, *FISA Amendments Reauthorization Act*, S.139 (2017).

151 Data Privacy Shield: MEPs alarmed at undermining of privacy safeguards in the US | News | European Parliament, (2017), https://www.europarl.europa.eu/news/en/press-room/20170329IPR69067/data-privacy-shield-meps-alarmed-at-undermining-of-privacy-safeguards-in-the-us (last visited Jul 23, 2020).

152 Judge James E. Boasberg, Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications (2018); Judges Cabranes, Tallman, and Sentelle, In Re: DNI/AG 702(h) Certifications 2018 (2019); Judge James E. Boasberg, Government's Ex Parte Submission of Amendments to DNI/AG 702(h) Certifications and Related Procedures, Ex Parte Submission of Amendments to DNI/AG 702(g) Certifications, and Request for an Order Approving Such Amended Certifications (2019).

153 OFFICE OF THE INSPECTOR GENERAL, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (2019).

Congress.[154] So far these reform attempts have not led to any substantial changes in the US surveillance framework.

A historical tracing technique also illuminates that the efforts to reform data protection regime on the federal level in the USA have also failed and added further strains on the Privacy Shield regime. Immediately after the Snowden revelations, privacy advocates in the US once again started pressuring the White House for action on a long-promised *Consumer Privacy Bill of Rights*, originally proposed by the Obama administration in 2012, which they now saw 'a top priority for the administration.'[155] In response, the administration issued a new discussion draft of the Bill in 2015, calling on industries to develop their own codes of conduct on the handling of personal information.[156] Civil society advocates criticized the draft for giving lip-service to privacy rights but ultimately ceding control over personal data to private companies.[157] The 2015 privacy Bill - however weak - lapsed despite all efforts and the supportive view of the FTC.[158] In 2016,

---

[154] REP NADLER, JERROLD, *USA FREEDOM Reauthorization Act* (2020).

[155] See the statement by Marc Rottenberg, director of the Electronic Privacy Information Center in Tom Hamburger, *Consumer Privacy Rights Need Urgent Protection in Washington, Activists Say*, WASHINGTON POST, February 24, 2014, https://www.washingtonpost.com/politics/consumer-privacy-rights-need-urgent-protection-in-washington-activists-say/2014/02/24/1764ba22-9cb7-11e3-975d-107dfef7b668_story.html (last visited Aug 13, 2020).

[156] UNITED STATES CONGRESS, *Consumer Privacy Bill of Rights Act* (2015), https://perma.cc/4AC6-H8YJ; For a comment on the Bill, see Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, THE NEW YORK TIMES, February 27, 2015, https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html (last visited Aug 14, 2020).

[157] See, eg, A letter to President Obama by Consumer Watchdog and other NOGs, (2015), https://www.consumerwatchdog.org/resources/ltrobamagroups030315.pdf (last visited Aug 13, 2020); Tracey Lien, *Consumer Privacy Bill of Rights doesn't go far enough, critics say*, PERMA.CC (2015), https://perma.cc/7FY3-4794 (last visited Aug 13, 2020); Analysis of the Consumer Privacy Bill of Rights Act, , PERMA.CC (2015), https://perma.cc/UVN9-E2QG (last visited Aug 13, 2020); The Editorial Board, *The President's Weak Privacy Proposal*, THE NEW YORK TIMES, March 6, 2015, https://www.nytimes.com/2015/03/06/opinion/the-presidents-weak-privacy-proposal.html (last visited Aug 13, 2020) at A28.

[158] See, eg, Commissioner Julie Brill "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" Address at the Woodrow Wilson

the US Federal Communications Commission (FCC) developed new information privacy rules called '*Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* in 2016.[159] These rules imposed restrictions on how internet service providers were to handle their users' information and required customers to 'opt in' before their data could be sold. However, they have been rejected by the US Congress in March 2017, fuelling further criticism of the US laws at the European Parliament, who saw it as a further sign of the weakness of Privacy Shield. [160] In this context, the infamous Cambridge Analytica affair, which was made public in 2018 and related to voter manipulation through Facebook [161] has further highlighted that if Privacy Shield was to be maintained, it required at least better monitoring.

Finally, during this period, the US also adopted a highly contentious *Clarifying Lawful Overseas Use of Data Act ('CLOUD Act')* in 2019, which permits US access to data held by US companies across the globe.[162] In the past year, the US has entered into a bilateral agreement with the UK pursuant to its *CLOUD Act*, which establishes a framework through which law enforcement and national security agencies can access data directly from private

School of Public and International Affairs Princeton, University, 8 (2014), https://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf (last visited Aug 13, 2020): "I believe adoption of baseline privacy legislation for the commercial arena would close the gaps in consumer privacy protections and help level the playing field among businesses."

[159] FEDERAL COMMUNICATIONS COMMISSION, *Protecting the privacy of customers of broadband and other telecommunications services, WC Docket 16-106, Notice of Proposed Rulemaking (Broadband Privacy Notice of Proposed Rulemaking)*, https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf (accessed 15 November 2016).

[160] EUROPEAN PARLIAMENT, *European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield*, 2018/2645(RSP) (2018), https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html.

[161] Quinn Emanuel Urquhart & Sullivan, LLP, *March 2020: Cambridge Analytica Found Liable for Violating Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, and the European Union-United States Privacy Shield Framework*, JD SUPRA , https://www.jdsupra.com/legalnews/march-2020-cambridge-analytica-found-89327/ (last visited Jul 23, 2020).

[162] UNITED STATES CONGRESS, *Clarifying Lawful Overseas Use of Data Act*, H.R. 4943 (2018).

companies abroad.[163] The interplay between EU data protection law, the *US CLOUD Act*, its potential effects on Privacy Shield and its ability to circumvent existing data sharing arrangements under Mutual Legal Assistance Treaty processes have also attracted attention by the European Data Protection Board and European Data Protection Supervisor.[164]

In light of these legal developments in the US and political climate in the EU on Privacy Shield, the *Schrems II* outcome is not surprising. It is part of the broader historical trend of the CJEU pushback against EU's internal, transatlantic and international data securitization and mass-surveillance regimes, developed and embraced during the period between 9/11 and the 2013 Snowden revelations.

Rejecting the 'Contracting Out' of Human Rights Protection to Cover Data Securitization

Situated in this historical context, the Courts pronouncement is both a simple and radical solution in response to mounting economic and geopolitical pressure on the EU to concede that its own human rights standards would not be honoured across the globe.[165] The Schrems decision illustrates the fundamental differences between the public and private approaches to protection of human rights in data-driven economy and modern state. The Court has questioned (again) and undermined (again) the ability of private 'self-certification' schemes, such as Privacy Shield,

---

[163] Department of Justice, Office of Public Affairs, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online* (2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (last visited Jul 23, 2020); Justin Hendry, *Govt clears the way for US CLOUD Act data swap deal*, ITNEWS (2020), https://www.itnews.com.au/news/govt-clears-the-way-for-us-cloud-act-data-swap-deal-538959 (last visited Jul 23, 2020).

[164] EUROPEAN DATA PROTECTION SUPERVISOR & EUROPEAN DATA PROTECTION BOARD, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence* (2019).

[165] Joel R. Reidenberg, *The Transparent Citizen*, 47 LOYOLA UNIVERSITY CHICAGO LAW JOURNAL 437, 462 (2015).

to provide 'adequate' safeguards where public laws of the third country provide little protection for fundamental rights.

SCCs are contractual assurances between businesses for the protection of human rights in third countries, which are guaranteed under EU law. In a similar vein, Privacy Shield is a business self-certification scheme. In the international legal order, where private actors lack legally binding human rights obligations,[166] voluntary contractual assurances between businesses are encouraged ensure the protection for human rights, for example, in supply chains and offshore manufacturing.[167] However, as the CJEU explicitly noted in *Schrems II*, private contracts, and the SCC's cannot bind a public authority in the third country.[168] Instead, contracts be easily over-ridden by the laws of the third countries.

Therefore, the Court is sending a message that private contractual arrangements for data transfers, such as the Safe Harbour and Privacy Shield, have lost their legitimacy after the Snowden revelations that commercial data exchanges taking place on US tech company infrastructure was being leveraged for mass-surveillance by the US government. The CJEU's decision in *Schrems II* to effectively 'de-list' the US as a third country party with whom EU data transfer can take place is a reassertion of a strong-form and holistic protection of EU citizens' human rights, which, according to the Court, should not be 'contracted out' but rather take primacy over the US, and even EU's own, economic interests in continuing data transfers with the 'business as usual' approach. A fundamental thesis, underlying the reasoning of the Court, is that the private self-certification contractual arrangements are not capable *in principle* of glossing over the fundamental flaws of public institutions.

---

166 Monika Zalnieriute, *From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Case of Internet Governance and ICANN*, YALE JOURNAL OF LAW & TECHNOLOGY 278–336 (2019).

167 JOHN RUGGIE, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

168 *Schrems II*, *supra* note 7 at 123, 125.

IV. IMPLICATIONS OF *SCHREMS II* FOR INTERNATIONAL DATA TRANSFERS

The CJEU's *Schrems II* ruling, however, has not only cemented CJEU's pushback against data securitization by rejecting the private fixes to public flaws, but will also significantly impact the transatlantic economy and commerce, data sharing frameworks in law enforcement, and international data transfers well beyond the US. This Part first looks at the varied reception of the judgment across the Atlantic before scrutinizing the practical impact of the CJEUs pronouncement for data sharing regimes.

Varied Reception of the Judgment

> 'I am very happy about the judgment. It seems the Court has followed us in all aspects. This is a total blow to the Irish DPC and Facebook. It is clear that the US will have to seriously change their surveillance laws, if US companies want to continue to play a major role on the EU market.' – *Max Schrems, 2020* [169]

While the *Schrems* outcome was not unexpected, given the history of transatlantic disagreements in data protection policy, its reception varies across the Atlantic. While the EP, and commentators in the EU more generally, see *Schrems II* as a victory for fundamental rights,[170] many in the US called it a European

[169] noyb, *CJEU Judgment - First Statement*, NOYB.EU (2020), https://noyb.eu/en/cjeu (last visited Aug 11, 2020).

[170] Julia Yvonne HODDER, *EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")*, EUROPEAN DATA PROTECTION SUPERVISOR - EUROPEAN DATA PROTECTION SUPERVISOR (2020), https://edps.europa.eu/press-

'overreach', 'hypocrisy', and even 'imperialism'. For example, a former general counsel of NSA, Stewart Baker described the *Schrems II* decision as 'gobsmacking in its mix of judicial imperialism and Eurocentric hypocrisy', and proposed that US should impose trade penalties to force the EU to back down form *Schrems* decision and emphasize that US is serious about its 'right to write U.S. laws without getting permission from European governments.'[171] Similarly, a US national security scholar Peter Swire said that '[f]or national security experts, it is puzzling in the extreme to think that citizens of one country have a right to review the intelligence laws from other countries.'[172] Such accusations of European 'overreach' are nothing new: many scholars, policy makers and commentators have claimed the EU was asserting its jurisdiction in data protection policy globally from the mid-1990s, when the EU Directive mandated auditing data processors in third countries for compliance with the EU law.[173] Thus, the EU and its data protection regime, and not only the CJEU judgments, have been accused of 'regulatory overreach,' from the time the EU data protection framework was developed.[174]

---

publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en (last visited Aug 11, 2020); 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 | European Data Protection Board*, EDPB (2020), https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en (last visited Aug 14, 2020); Pavlina Ittelson, *Schrems II - The judgement and initial reflections*, DIPLO (2020), https://www.diplomacy.edu/blog/schrems-ii-judgement-and-initial-reflections (last visited Aug 14, 2020).

[171] Stewart Baker, *How Can the U.S. Respond to Schrems II?*, LAWFARE (2020), https://www.lawfareblog.com/how-can-us-respond-schrems-ii (last visited Jul 24, 2020).

[172] Swire, *supra* note 2.

[173] See Dan Svantesson, *A "Layered Approach" to the Extraterritoriality of Data Privacy Laws*, 3 INTERNATIONAL DATA PRIVACY LAW 278–286 (2013); CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (2013); See also P Ford, *Implementing the EC Directive on Data Protection – An Outside Perspective*, 9 PRIVACY LAW & POLICY REPORTER 141–149 (2003); EUROPEAN PARLIAMENT AND EUROPEAN COMMISSION, *supra* note 33 Art 4(1)(c) also prescribes certain conditions when European data protection rules may apply outside of the EU territory.

[174] See, eg, Ford, *supra* note 174; See also EUROPEAN PARLIAMENT AND EUROPEAN COMMISSION, *supra* note 33 art 4(1)(c).

After the first *Schrems* ruling in 2015, then US Secretary of Commerce, Penny Pritzker, said the Obama Administration was 'deeply disappointed' in the CJEU decision and that it 'necessitates release of the updated Safe Harbor Framework as soon as possible'.[175] Similarly, after *Shrems II*, US Secretary of Commerce Wilbur Ross stated that the current administration was 'deeply disappointed' in the outcome, citing the $7.1 trillion transatlantic economic relationship to state that 'it is critical that companies… be able to transfer data without interruption'.[176] However, the US Department of Commerce also emphasized that, during the *Schrems II* case, the US government 'participated actively in the case with the aim of providing the court with a full understanding of U.S. national security data access laws and practices and how such measures meet, and in most cases exceed, the rules governing such access in foreign jurisdictions, including in Europe'.[177] Such statement suggests that US government perceives the CJEU's examination of its national security laws as unjust, given that the CJEU is barred from scrutinizing surveillance regimes of the EU Member States, under the division of competence under EU law, leaving the national security policy at the hands of Member States.[178]

This aspect of EU law has been criticized as hypocritical by US scholars, who think it incomprehensible that the CJEU can declare US national security framework 'inadequate' from the data protection and fundamental rights perspective, while the Court has no right to examine the national security policies of its Member States.[179] Thus, it is not strange the commentators in the US would

---

[175] See Department of Commerce, *Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision* (2015).
[176] U.S. Department of Commerce, *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*, U.S. DEPARTMENT OF COMMERCE , https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and (last visited Jul 24, 2020).
[177] *Id.*
[178] EUROPEAN UNION, *Treaty of Lisbon: Amending the Treaty on European Union and the Treaty Establishing the European Community*, (OJ 2007 C 306/02) (2007) art 4.
[179] Swire, *supra* note 2; Jennifer Daskal, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers*, JUST SECURITY (2020),

see Courts rulings as attempts to 'legislate' in third-country jurisdictions, or at least withholding transactions and consequent revenue but for a change in government policy. However, as discussed in the Part II, this perception dates back all the way to the days when adequacy criterion was first introduced with the EU Data Protection Directive in 1994.

Impact on Commercial EU-US Data Transfers

Importantly, beyond displeasure and dislike for the CJEU's ruling in the US, the judgment nonetheless will have significant implications for commercial data transfers to the US. Schrems II was the second EU-US decision on adequacy invalidated in a period shorter than five years. Over 5,000 companies used Privacy Shield,[180] and its invalidation will have significant implications for data transfers to the US. The question now becomes: how can data be lawfully transferred from the EU to the US?

The Court has not imposed a general ban to on data transfers to the US, but merely invalidated the Privacy Shield decision and analysed the safeguards provided to the individuals in the US legal system. As I pointed in Section II of this article, 'adequacy' decisions are not the only mechanisms for transfers of personal data to third countries under EU law, and data transfers may take place in the absence of an adequacy decision under article 45(3) of the GDPR or appropriate safeguards under article 46 of the GDPR, which provide for SCCs and BCC, among other tools.

However, data controllers/exporters now face a significant dilemma: how can they rely on SCCs for data transfers to US to ensure 'adequate' protection for the rights of the data subjects despite the overarching US surveillance regime? Since the CJEU held that the US legal system as a whole does not provide 'adequate'

https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/ (last visited Jul 24, 2020).

[180] International Trade Administration, *Privacy Shield | News and Events | Privacy Shield*, PRIVACY SHIELD FRAMEWORK , https://www.privacyshield.gov/NewsEvents (last visited Jul 23, 2020); U.S. Department of Commerce, *supra* note 177.

protection, the use of SCCs is of limited use. In other words, whichever the mechanism for data transfers are used, they still must ensure the 'adequate' level of protection for personal data. Indeed, DPAs in the EU already have issued guidelines to data controllers, advising them to cease EU-US transfers. For example, since the *Schrems II* judgment the EDPS has 'reaffirmed the importance of maintaining a high level of protection of personal data transferred from the European Union to third countries', and stated that as a consequence of the decision they will be 'carefully analysing the… judgment on the contracts concluded by EU institutions, bodies, offices and agencies'.[181] Similarly, the Berlin DPA has also pressured data controllers to ensure they get the legal basis for international data transfers right.[182] Fines for breaching the GDPR can be up to four per cent of a company's global revenue,[183] and with DPAs now obliged to take action against unlawful transfers, contracting out the protection of human rights where the public institutions fail to provide adequate safeguards seems like risky business.

However, two options – both risky – emerge that could save the fate of the SCCs for the EU-US transfers: first, they SSCs could potentially be still used with some US companies, which are sufficiently isolated from the risk of government surveillance that they are not in breach of the *Schrems II* protection concerns; or second, adding 'additional safeguards' to circumvent the risk of surveillance.[184] However, as I will describe below, both are problematic and it is uncertain if they could be used.

---

[181] HODDER, *supra* note 171.

[182] OneTrust DataGuidance, *Berlin: Berlin Commissioner issues statement on Schrems II case, asks controllers to stop data transfers to the US*, DATAGUIDANCE (2020), https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data (last visited Aug 11, 2020).

[183] EUROPEAN PARLIAMENT AND EUROPEAN COUNCIL, *General Data Protection Regulation (GDPR)*, OJ L 119 (2016), https://gdpr-info.eu/ (last visited Aug 14, 2020) art 83(4)-(6).

[184] Theodore Christakis, *After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, EUROPEAN LAW BLOG (2020), https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ (last visited Jul 24, 2020).

With regards to the first option, it is true that not all companies are subject to the US surveillance regime – as Omer Tene pointed, s 702, EO 12333 and PPD 28 do not apply to retailers, manufacturers, health care or pharma companies.[185] However, given the breadth of the surveillance programmes named by the Court in Schrems II decision - PRISM and UPSTRAEM - and the likelihood that they 'tap' undersea cables irrespective of the ultimate destinations, it is still unlikely that these companies would be completely exempt from US surveillance laws. To allow some US companies to determine their likelihood of being subject to US surveillance framework would be a novel experiment, but it is 'far from clear which EU regulatory authority can provide comfort that such transfers are lawful'.[186]

An alternative option could be adding additional safeguards to the SSCs, such as 'technical' safeguards (e.g., end-to-end encryption) and/or 'legal' safeguards (e.g., companies challenging intelligence community demands for EU data).[187] The CJEU itself referred to 'supplementary measures',[188] 'additional safeguards',[189] 'additional measures',[190] and 'effective mechanisms to make it possible, in practice, to ensure compliance' in *Schrems II* judgment.[191] Similarly, the DPAs called for the immediate suspension of data transfers impugned by the judgment, and reemphasised the need to ensure proper protections are in place where using standard contractual

[185] Omer Tene argues that the impugned s 702, EO 12333 and PPD 28 do not apply to retailers, manufactuers, health care or pharma companies, or the "thousands of companies that use SCCs to export employee data to headquarters in the U.S" Omer Tene, *The show must go on*, IAPP (2020), https://iapp.org/news/a/the-show-must-go-on/ (last visited Jul 24, 2020).
[186] Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision (last visited Jul 24, 2020).
[187] Christakis, *supra* note 185; Jennifer Daskal recognises that there is "no guarantee that the companies will win such challenges; they are, after all, ultimately bound by U.S. legal obligations to disclose" Daskal, *supra* note 180.
[188] *Schrems II*, *supra* note 7 at 133.
[189] *Id.* at 132, 134.
[190] *Id.* at 135
[191] *Id.* at 137, 148.

clauses.[192] However, while many EU DPAs have called for suspension of data transfers to the US and highlighted the need for 'additional safeguards', [193] no DPA has so far specified explicitly what these 'additional' or 'extra' safeguards might be. It is therefore questionable whether these 'extras' would address the concerns of the Court in *Schrems II*, as no 'extra safeguard' arguably can provide a 'silver bullet' protection against the US surveillance which so concerned the CJEU, or facilitate genuine forms of legal remedies and judicial review akin to the GDPR and EU equivalent.

Implications for Other Data Sharing Regimes

The *Schrems II* decision will also have broader implications for other EU-US and global data sharing arrangements, as they are closely related to transatlantic securitisation and US mass-surveillance policies. First, the *Shrems II* pronouncement on the extent of the US surveillance framework can impact the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which facilitates global interaction between financial institutions, within and between the EU and third countries.[194] SWIFT is established in Belgium and, in 2018, it handled half of the world's high-value cross-border payments.[195] As I have explained in the previous Part

---

[192] CONFERENCE OF INDEPENDENT DATA PROTECTION REGULATORS & OF THE FEDERAL AND STATE GOVERNMENTS, *Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger (Judgment of the European Court of Justice for the transfer of personal data to third countries ("Shrems II") strengthens data protection for EU citizens* (2020), https://datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.

[193] OneTrust Data Guidance, *Europe: Data protection authorities react to Schrems II judgment*, DATAGUIDANCE (2020), https://www.dataguidance.com/news/europe-data-protection-authorities-react-schrems-ii-judgment-updated-12-august-2020 (last visited Aug 14, 2020).

[194] SWIFT has two agreements between the co-operative at the EU as a collective: SWIFT, *Agreement between the European Union and The United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, L 8/11 (2010); SWIFT, *SWIFT Agreement*, L 195/5 (2010); See further V Pfisterer, *The Second SWIFT Agreement between The European Union and the United States of America – An Overview*, 11 GERMAN LAW JOURNAL 1173 (2010).

[195] Martin Arnold, *Ripple and Swift slug it out over cross-border payments* (2018), https://www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6 (last visited Jul 24, 2020).

on the CJEU's pushback against securitization, the SWIFT arrangements have also been subjected to increased 'securitization' between 9/11 and the 2013 Snowden revelations, and the analogy between the data transfer regimes impugned in *Schrems II* and SWIFT is evident.

Secondly, the decision has implications for the US-EU negotiations with respect to the US CLOUD Act.[196] As was mentioned in Section II of this paper, the US CLOUD Act regime forces US companies to provide US authorities with access to personal data stored offshore.[197] In the past year, the U.S. has entered into a bilateral agreement with the UK pursuant to its CLOUD Act.[198] and negotiations have begun between the EU and the US to establish such a bilateral agreement.[199] The ability of the data sharing arrangements under the US Cloud Act to circumvent existing MLAT processes and evade the data protection law requirements have already been noted by both the EDPB and EDPS, who ultimately found that it would be necessary to establish a 'future international agreement' for compliance to be in accordance with the GDPR.[200] Given that EC Commission has to take CJEU's rulings into account, the fate of the negotiations between the EU and US with respect to a transatlantic law enforcement data sharing network remain uncertain.

Transfers to Third Countries Generally

Finally, the *Schrems II* decision will have significant implications for data transfers to third countries, including the post-Brexit UK, China and other countries, whose national security laws arguably would fall short of the strict CJEU's requirements articulated in

[196] Joint US-EU Statement on Electronic Evidence Sharing Negotiations, (2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations (last visited Jul 24, 2020).
[197] Hendry, *supra* note 164.
[198] Department of Justice, Office of Public Affairs, *supra* note 164; Hendry, *supra* note 164.
[199] Joint US-EU Statement on Electronic Evidence Sharing Negotiations, *supra* note 197.
[200] EUROPEAN DATA PROTECTION SUPERVISOR AND EUROPEAN DATA PROTECTION BOARD, *supra* note 165.

Schrems. Whilst the focus of the *Schrems II* decision itself was on EU-US data transfers, SCCs are relied on by 88 per cent of EU companies transferring data outside the EU,[201] and so the impact of the decision is much wider. *(Role for DPAs in SCCs)* In light of the Court's ruling that DPA's must act on user complaints where data transfers under SCCs do not afford equivalent EU law protections,[202] the pressure will be on data controllers to ensure compliance. Of course, if SCCs are to be an effective mechanism of EU law, DPAs must be prepared to use their *Schrems II*-mandated powers confidently, adopting corrective measures where data controllers fail to act or make agreements under SCCs which do not afford protection which is an essential equivalent of EU law.

In this respect, data transfers to many countries will likely be investigated by the DPAs now. For example, data transfers to China are of a much larger scale than is usually anticipated, with annual data exports of 200 billion euros, including via TikTok, Alibaba and TenCent.[203] Peter Swire has recently argued that the CJEU decision in *Schrems II* could result in an 'absurdity' where 'EU citizens' data could not travel to the US for fear of intrusive surveillance, but could flow unimpeded to China, a nation with surveillance practices ripped from the pages of a dystopian science fiction novel.'[204] However, the CJEU's ruling will have a clear impact on data transfers to China if it will be followed by data controllers, and, importantly, the DPAs. If the DPAs will use their powers to evaluate the SSCs where they are used to transfer

---

[201] Joan Stewart, *Companies Engaged in Trans-Atlantic Data Transfers Face Legal Uncertainty*, WILEY (2019), https://www.wiley.law/newsletter-2019-PIF-Oct_Companies_Engaged_in_Trans-Atlantic_Data_Transfers_Face_Legal_Uncertainty (last visited Jul 24, 2020).

[202] *Schrems II*, *supra* note 7 at 112.

[203] PETER SWIRE, *Chinese Surveillance and European Union Data Privacy*, https://fpf.org/wp-content/uploads/2019/07/Peter-Swire-le-monde-annotated-bibliography.pdf.

[204] Peter Swire, *« Interdire le transfert de données seulement vers les Etats-Unis serait une aberration » (The US, China, and Case 311/18 on Standard Contractual Clauses)*, LE MONDE.FR, July 11, 2019, https://www.lemonde.fr/idees/article/2019/07/11/peter-swire-interdire-le-transfert-de-donnees-seulement-vers-les-etats-unis-serait-une-aberration_5488248_3232.html (last visited Aug 11, 2020).

personal data will insufficient safeguards, the *Schrems II* impact should be just as great on data transfers to China as it is on the US.

The impact of the CJEU's ruling is also significant for the post-Brexit UK, which is widely known for its extensive surveillance practices as a member of the Five Eyes Alliance.[205] As an EU Member State, the UK's national security surveillance practices have not been previously scrutinized by the CJEU because national security is outside the EU competence.[206] Ceasing EU membership will transform the UK's status vis-à-vis the EU to that of a third country. When the UK transition period ends on 31 December 2020, transfers of personal data from the EU to the UK will be governed by Chapter V of the GDPR, and therefore the same rules and standards as those applicable to US and other thirds countries. As a third country, the UK's legal system, including its national security framework, will have to ensure a level of protection 'essentially equivalent to that guaranteed within the EU'. Currently, the EU Commission is assessing whether the UK qualifies for a finding adequacy pursuant to Article 45 of the GDPR, read in light of the Charter.[207] Given the similarities between the US and UK systems of national security and extensive data sharing between the two countries, it will be intriguing to see if the UK will be able to obtain an general 'adequacy' finding, or will it join the special ranks along the US.

CONCLUSION

[205] Office of the Director of National Intelligence, *Five Eyes Intelligence Oversight and Review Council (FIORC)*, https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-related-menus/chco-related-links/recruitment-and-outreach/217-about/organization/icig-pages/2660-icig-fiorc (last visited Aug 11, 2020).
[206] *Schrems II*, *supra* note 7 at 81.
[207] European Commission, Directorate General Justice and Consumers, *Notice to Stakeholders - Withdrawal of the United Kingdom and EU Rules in the Fried of Data Protection* (2018), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/data_protection_en-1.pdf.

> 'I will now take every necessary step to ensure that controllers and DPAs will implement the clear decision by the CJEU. Making sure that the Irish DPC finally takes a decision after seven years and five rulings by the Irish and European Courts is only one of our options. We are also looking at other options, as it would be unacceptable if the EU's Supreme Court were to be ignored a second time round.' - *Max Schrems, 2020*[208]

The protection of fundamental human rights is particularly important during the times of crisis and public health emergency caused by the global COVID-19 pandemic. It is in periods of upheaval and global challenge during which derogation from human rights standards can most easily occur unnoticed, and consequently it is extremely important to continue to critically interrogate the way in which human rights standards are being upheld by national and supranational governments. Data protection and privacy are especially important human rights , given the range of tools used to combat the virus through tracking and surveillance systems.[209]

The CJEU's invalidation of the Privacy Shield in *Schrems II* is particularly important during the global pandemic. The judgment has reinforced the fundamental role of data protection in the EU legal order and transatlantic relations, demonstrating that the CJEU will not accept 'second rate' protection for personal data transferred outside EU. While the Court upheld the validity of the SCC Decision, the standard contractual clauses used in particular contracts must still provide for enforceable rights and effective legal remedies, that 'essentially equivalent' to those provided under EU law. The CJEU has also reasserted the DPA's power to

---

[208] noyb, *DPC has no clear time line on enforcing CJEU judgement*, NOYB.EU (2020), https://noyb.eu/en/dpc-has-no-clear-time-line-enforcing-cjeu-judgement (last visited Aug 11, 2020).

[209] United Nations Human Rights Office of the High Commissioner, *COVID-19 Guidance*, UNHR OFFICE OF THE HIGH COMMISSIONER , https://www.ohchr.org/EN/NewsEvents/Pages/COVID19Guidance.aspx (last visited Aug 14, 2020).

suspend, limit, or even ban data transfers to countries which do not afford adequate protection for fundamental rights. It remains to be seen if DPA's, in their newly affirmed role as the gatekeepers of international data transfers, will wield their powers and close the gates to data flows where they fall below the standards of the EU law.

Importantly, the CJEU rejected any approach that 'contracts out' human rights protection to gloss over increasing data securitization and government surveillance regimes. *Schrems II* is the outcome that US tech companies and US government feared. Yet, as I have argued in this Article, that they are not the only actors displeased with the decision. Historical institutionalist analysis illuminated that the EU is not a monolithic block, and that Schrems II is also an outcome contrary to the wishes of EC Commission. The striking down of the Privacy Shield will now (again) require re-balancing of the EU policy and priorities, or accommodating the institutional preferences of its powerful ally – the USA – through special arrangements again.

Through a historical sequencing analysis, this article has shown how the *Schrems II* decision, more than those which preceded in, puts both the US and the EU governments in a corner; for data transfers to continue, a serious reappraisal of surveillance and data protection in the US necessary, without which the EU risks allowing and enabling CJEU-determined violations of human rights or jeopardizing high stakes of transatlantic economy. Therefore, while *Schrems II* is a powerful restatement of the need for of human rights protection in the EU and beyond, its political impact might be very similar to that of the *Schrems I.* As Part IV in this article has demonstrated, the invalidation of the Safe Harbour in *Schrems I* has not changed much in the US surveillance law. Instead, the EU Commission was very fast in drafting its Privacy Shield Decision, which more or less mirrored the previous Safe Harbour Decision, leading some to call it merely a 'Paper Shield'.[210]

[210] Gert Vermeulen, *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*

Of course, the EU institutions, other than the EU Commission, quickly realized that the Privacy Shield was a 'cosmetic' make-over of the earlier Safe Harbour agreement, for the US to comply with the CJEU requirement to provide an 'adequate' level of data protection.

A similar outcome after *Shrems II* is a risk that is born by the EU, who continues to be economically interdependent with the US and could not simply suspend data transfers. Data controllers and exporters are now left with a choice – process the data in the EU or pressure the US government to make structural changes in the US law that could afford essentially equivalent protection for personal data to that of EU of EU. However, historical process tracing in this article revealed that US surveillance laws did not encounter any serious reforms since the Snowden revelations. Therefore, the structural changes in the US legal system to address the inadequacies in the *Schrems II* judgment are unlikely in any near future. Barring these changes, other regimes which handle data in financial transfers (SWIFT) or proposed law enforcement data-sharing operations (CLOUD Act) may also be threatened; and the data protection stalemate between the EU and US is set to continue.

Yet, institutional analysis in this article have also shown that the EU and US are not monolithic black boxes, and, at a certain institutional level, the stalemate is a friendly one. The US Secretary of Commerce have indicated a willingness to work together with the EU Commission and in the wake of *Schrems II* decision to 'limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments.'[211] Mr Wilbur Ross said that '[d]ata flows are essential not just to tech companies—but to businesses of all sizes in every sector. As our economies continue their post-COVID-19 recovery, it is critical that companies—including the

Law Enforcement Services, Svantesson., 4 *in* TRANSATLANTIC DATA PRIVACY RELATIONSHIPS AS A CHALLENGE FOR DEMOCRACY 127–48 (JB Dan & Dariusz Kloza eds., 2017).

[211] U.S. Department of Commerce, *supra* note 177.

5,300+ current Privacy Shield participants—be able to transfer data without interruption.'[212] The EU Commission will act quick to create a solution, similar to the Privacy Shield and Safe Harbour - another quick contractual 'fix' - to accommodate US exceptionalism and gloss over the decades of disagreement between the EU and USA on data protection, national security and information privacy. When two regulatory powers are unwilling to change their institutional preferences, the 'contracting out' of human rights protection is the most convenient. Therefore, one thing is certain, the CJEU's fight to ensure the role of fundamental human rights in the global data economy is not yet over.

[212] *Id.*