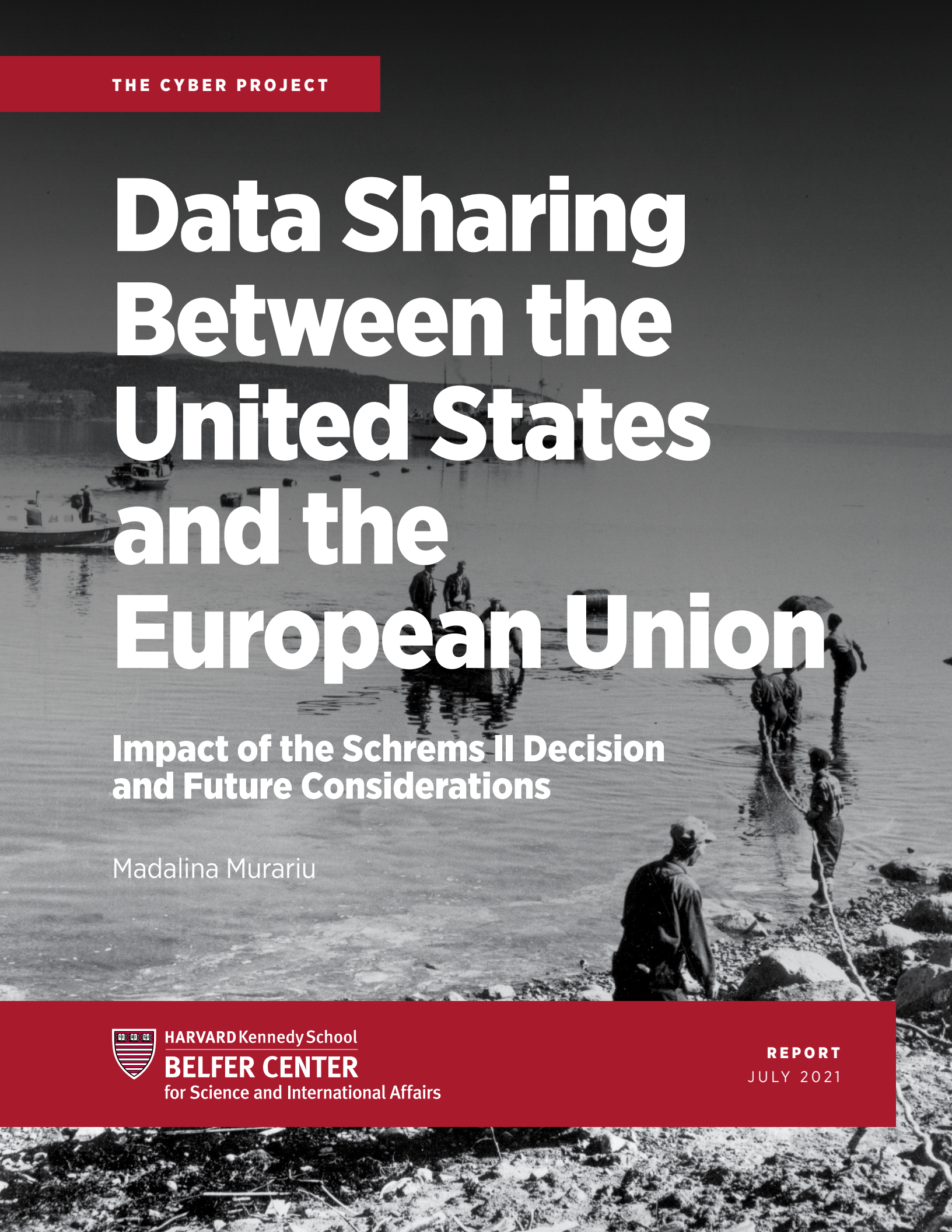

THE CYBER PROJECT

Data Sharing Between the United States and the European Union

Impact of the Schrems II Decision and Future Considerations

Madalina Murariu

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JULY 2021

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Design and layout by Andrew Facini

THE CYBER PROJECT

Data Sharing Between the United States and the European Union

Impact of the Schrems II Decision and Future Considerations

Madalina Murariu

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JULY 2021

Table of Contents

A transatlantic telephone cable is brought ashore at Clarenville, Newfoundland, for the final splice on March 8, 1957. In the background is the British naval vessel Monarch, the world's largest cable layer, which has worked through two summers laying nearly 4,000 miles of cable to complete the two-way system between Newfoundland and Scotland.

AP Photo

Introduction

In July of 2020, the Court of Justice of the European Union (CJEU) rendered its decision in the *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems,* also known as the Schrems II case.[1] The case struck at the core of the agreements between the United States and the European Union in regard to the transfer of data, constituting the most recent setback in a series of attempted agreements seeking to enable transfers between the two jurisdictions.

The implications of this decision have substantial short and long-term repercussions. This paper will seek to briefly explain the history of the Schrems cases, then outline the options available to decision makers seeking to enable transatlantic cooperation. The paper will also argue that short-term solutions such as the ones leveraged up till now will increasingly be unfeasible, and therefore present four proposals for consideration on how a revived data transfer ecosystem could be shaped through national and international tools and mechanisms.

Overview of the Schrems Cases and the Schrems Decision Implications

The Schrems II decision is the latest development in the ongoing litigation launched in 2013 when Austrian privacy advocate Max Schrems filed a complaint with the Irish Data Protection Commissioner requesting the Irish subsidiary of Facebook be barred from transferring his personal data to the United States. This act, his complaint asserted, was in contravention of the adequacy requirements for the protection of his personal information under the Safe

1 "Schrems II landmark ruling: A detailed analysis." Norton Rose Fulbright, https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis

Harbour Regime[2] based on his understanding of the unauthorized disclosure of classified information by Edward Snowden.

The complaint was rejected by the Irish Data Protection Commission, prompting Mr. Schrems to request a judicial review from the Irish High Court which found that Mr. Schrems' objections were less concerned with the way in which the Commissioner had applied the Safe Harbour Regime, and more with the regime itself[3].

Justice Hogan thus found that since the Irish Court did not have jurisdiction over the Safe Harbour Regime or decision, the case should be referred to the Court of Justice of the European Union in light of Articles 7, 8 and 47 of the European Union Charter on Fundamental rights for a determination on the Data Commissioner's interpretation[4].

In October of 2015, the Court of Justice of the European Union released its decision on the *Schrems v. Data Protection Commissioner* case. The court found that data protection authorities have the right to examine claims brought forward by individuals even when they concern the level of protection granted by a third-party country. The decision also found that Article 1 of the Decision in 2000 that had approved the creation of the Safe Harbour Framework[5] was invalid since neither the Federal Trade Commission nor the private dispute resolution bodies could monitor breeches by public actors such as the United States' security agencies[6]. Thus, the Safe Harbour principles were deemed to be insufficient for the transfer of personal data to the United States.

2 Schulz, Tobias J. "Schrems v. Data Protection Commissioner (C.J.E.U.)." International Legal Materials, vol. 56, no. 2, Cambridge University Press, Apr. 2017, pp. 245–72. Cambridge University Press, doi:10.1017/ilm.2017.8.

3 Judgments | The Courts Service of Ireland. https://www.courts.ie/search/judgments/%22schrems%20type%3AJudgment%22%20AND%20%22filter%3Aalfresco_radio.title%22.

4 "Explanatory Memoranda on the Litigation Concerning Standard Contractual Clauses ('SCCs') | Data Protection Commission." Explanatory Memoranda on the Litigation Concerning Standard Contractual Clauses ('SCCs') | Data Protection Commission, https://www.dataprotection.ie/news-media/press-releases/explanatory-memoranda-litigation-concerning-standard-contractual-clauses.

5 (https://2016.export.gov/safeharbor/eu/eg_main_018476.asp. Accessed 11 Apr. 2021.)

6 Schulz, Tobias J. "Schrems v. Data Protection Commissioner (C.J.E.U.)." International Legal Materials, vol. 56, no. 2, Cambridge University Press, Apr. 2017, pp. 245–72. Cambridge University Press, doi:10.1017/ilm.2017.8.

To fill the gap created by the 2015 decision, the United States and the European Union announced in 2016 the creation of a new European Union-United States (and Swiss) Privacy Shield Framework. The new framework was designed by the Department of Commerce and the European Commission to help companies in both jurisdictions comply with data protection requirements for the transfer of personal data as part of commercial activities and included new measures to address previous Safe Harbour concerns as outlined in the Privacy Shield Overview information provided[7].

Safe Harbour Overview

In 1998, the European Commission's Directive on Data Protection went into effect, prohibiting the transfer of personal data to non-European Union countries unless they could meet the 'adequacy' requirement for the protection of privacy.

To help meet this requirement and ensure collaboration could continue, the United States Department of Commerce and the European Commission developed a 'Safe Harbour" framework that allowed organizations to participate on a voluntary basis by agreeing to adhere to the principles of the framework including notice, choice, access and data integrity provisions as part of the Seven Safe Harbour Principles. Organizations that self-certified to participate in the Framework were expected to abide by the requirements and thus considered to provide 'adequate" privacy protection as required by the directive.

The framework was approved by the European Union in 2000 and was in place until 2015 when the Court of Justice of the European Union rendered the Safe Harbour regime null and void (Schrems 1).

(Export.Gov, 2021)

Following the Schrems 1 decision, Max Schrems reformulated his complaint with the Irish Data Protection Authority on the basis of Facebook

7 Privacy Shield Program Overview | Privacy Shield. https://www.privacyshield.gov/program-overview. Accessed 11 Apr. 2021.

Ireland's stated use of Standard Contractual Clauses (SCC) for data transfers to the United States based parent company[8].

The Data Protection Authority brought an action before the Irish High court which referred the case to the Court of Justice of the European Union making the newly developed Privacy Shield instrument open for review by the court as a pertinent part of the case.[9]

Privacy Shield Overview

The EU-US Privacy Shield was created in 2016 as a result of the 2015 ruling by the European Court of justice deeming the previous Safe Harbour framework invalid[10]. The newly designed agreement aimed to address findings in the 2015 decision, and offer stronger protection of personal data for European Citizens.

This included stronger monitoring and enforcement obligations for the United States Department of Commerce (DoC) and Federal Trade Commission (FTC), as well as requirement for those bodies to closely cooperate with European Data Protection Authorities as required[11].It also prevented generalized access by United States public authorities, making it subject to limitations, clear conditions and oversight.

Privacy Shield also required stronger obligations for companies including sanctions and exclusions for non-compliance and stronger conditions for onward transfers of information to other partners. Redress possibilities were also created for European Union citizens through the creation of an Ombudsman, an Alternative Dispute Resolution mechanism and an annual joint review mechanism among the new requirements the agreement created.

8 The CJEU judgment in the Schrems II case,(https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

9 The CJEU judgment in the Schrems II case,(https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

10 "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield." European Commission - European Commission, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216a.

11 "EU-U.S. Privacy Shield: Frequently Asked Questions." European Commission - European Commission, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_434.

The Privacy Shield Framework was in place from 2016 to 2020 when the Court of Justice of the European Union invalidated the Privacy Shield Decision (Schrems II).

In July of 2020, the CJEU released its decision on the *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems and intervening parties, Case C-311/18* (known as the Schrems II case)[12]. The Court found that Privacy Shield was insufficient in providing adequate protection since United States surveillance laws[13] such as Executive Order 12333 [14]have primacy in domestic law in the United States which is not circumvented by Privacy Shield, and further that individuals do not have sufficient redress mechanisms which satisfy EU law[15].

The Court further found that the use of standard contractual clauses as an adequate level of protection for personal data transfers outside of the European Union was theoretically valid. However, the decision stressed entering into the standard contractual clauses was not enough on its own, particularly in jurisdictions where destination countries do not offer sufficient protection. In those jurisdictions, controllers must augment measures to reach adequate levels of protection or cease transfers, a threshold difficult to reach in the case of United States and European Union data transfers in light of the Privacy Shield invalidation[16].

12 "Schrems II landmark ruling: A detailed analysis." https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/2020, https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis.

13 Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II. p. 25.

14 The European Court of Justice identified two primary areas under United States law where there was concern intelligence agencies would be able to access information. This included Executive Order 12333 which provides general guidance on intelligence activities and the second was Section 702 of the Foreign Intelligence Surveillance Act which allows a court to authorize the government to issue "orders requiring companies in the United States to disclose communications data of specific non-U.S. persons located outside the United States to obtain specified types of foreign intelligence information".

15 Schrems II: The Saga Continues | McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/techlex/schrems-ii-saga-continues.

16 Schrems II: The Saga Continues | McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/techlex/schrems-ii-saga-continues.

Implications and the Future of Data Transfers Between the United States and the European Union

The CJEU's 2020 Schrems II decision has upended the standard business practices which companies had been utilizing under Privacy Shield. Compounded by the previously rendered Safe Harbour decision, the future of data transfers between the United States and the European Union presently hangs in a regulatory limbo placing the two jurisdictions at a crossroads.

Transatlantic data and information flows between the United States and the European Union are estimated to be valued at over $7.1 trillion dollars and span over 5300 companies, including technology giants such as Twitter, Google, Facebook and Amazon[17]. As the Schrems 1 and Schrems II decisions demonstrate, the underlying issues and lack of harmonization threaten to continuously disrupt the commercial relationship between the United States and European Union, create mistrust in domestic perceptions over personal data protection, and impose a large regulatory compliance and cost burden on companies that may not be feasible in the long term.

There are therefore two approaches that can be taken to move forward in a post-Schrems II environment; a short-term solution that leverages current guidance to create a more adequate transfer mechanism moving forward, or the creation of longer-term thought-leadership that will aim to respond not only to the issues the jurisdictions face today, but also future considerations that will further alter the data transfer landscape. While both approaches encompass both upsides and risks as identified below, the current status-quo is unlikely to be feasible in perpetuity, requiring significant changes.

17 Transatlantic Data Flows: Permanently Broken or Temporarily Fractured? https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured.

Short-Term approach: Leverage Existing Mechanisms

In light of the 2020 Schrems II decision, the European Data Protection Board (EDPB) and the European Commission (EC) released their recommendations and updates to the Standard Contractual Clauses (SCCs) to guide companies in their data transfer compliance[18]. Additionally, in September of 2020, the United States Department of Commerce released both a White Paper as well as a letter from the Deputy Assistant Secretary for Services acknowledging the disruption Schrems II poses to the transatlantic data flow. **A short-term solution could therefore look at leveraging these recommendations to carve a temporary path forward.**

This could take the form of a new regime founded upon the principles and application of Standard Contractual Clauses. Article 46 of the General Data Protection Regulation (GDPR) already sets out the mechanism to achieve this by allowing for data transfers "if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available" [19].

Noting that the Schrems II decision specifically cautioned that additional measures may need to be undertaken in jurisdictions where no protection equivalency exists, the recommendations issued by the European Data Protection Board will also need to be taken into account and incorporated. This includes an onus on data exporters to know their transfers (including keeping records of transfers of personal data), identify transfer tools such as the SCCs, build an assessment of the Article 46 application and its essential equivalency of protection requirements, adopt supplemental measures such as encryption or contractual requirements, and develop procedural requirements to ensure compliance and ongoing evaluation of measures[20].

18 "Post-Schrems II: The European Union Provides Guidance on Data Transfers." JD Supra, https://www.jdsupra.com/legalnews/post-schrems-ii-the-european-union-23981/..

19 "Regulation (EU) 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 (General Data Protection Regulation) (Text with EEA Relevance)." OJ L, vol. 119, 32016R0679, 4 May 2016, http://data.europa.eu/eli/reg/2016/679/oj/eng.

20 "Why the Guidance on International Transfer of Data Post Schrems II Doesn't Offer as Much Comfort as We'd Hoped." Gowling WLG, https://gowlingwlg.com/en/insights-resources/articles/2020/international-transfer-of-data-post-schrems-ii/. Accessed 11 Apr. 2021.

While the EDPB requirements are prescriptive, they place a substantially large burden for compliance on companies seeking to leverage Article 46 provisions in ways that could be arguably deemed excessive. The United States White Paper aims to offer some guidance and reassurance to companies seeking to establish if data recipient countries legislation offers adequate protections meeting European Union standards.[21] While the White Paper is not legally binding proof of adequacy of protections, it seeks to explain the role United States Intelligence Agencies play in transatlantic security collaboration as well as outline the relevant laws and practices that can help establish adequate protections and redress for European Union citizens.

The Department of Commerce's White Paper in conjunction with the EDPB Recommendations and the European Commission's Update to the Standard Contractual Clauses offer a tentative and intermediary path forward. However, this short-term solution is unlikely to survive for any considerable length of time for a number of reasons. This includes the high costs and responsibilities for compliance placed on companies under the piecemeal regulatory approach, as well as ambiguous requirements for the benchmarking of the adequacy of personal data safeguarding that would undoubtedly be struck down by courts upon review.

21 Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II. p. 23.

Long Term Approach Necessary

The Schrems II decision has struck at the heart of arguably a much larger debate with which jurisdictions around the world are grappling: namely the intersection of personal privacy, national security, and international collaboration. The lack of recognized standards, principles, or harmonized legislation has created an international environment increasingly perilous for both companies and governments to navigate.

The European Union has, in recent years, worked to establish itself as a data protection steward through legislation and regulation such as GDPR and the European Union Charter on Fundamental Rights which enshrines "Protection of Personal Data" under Article 8.[22] Data privacy and protection of citizens' personal information is therefore ground the European Union is unlikely to cede and increasingly a commercial and geopolitical advantage for the region.

Unlike the European Union, the United States does not currently have a personal data protection privacy framework or guiding principles, relying instead on an amalgamation of state and federal laws that offer protections in certain areas. These include the Federal Trade Commission Act, The Computer Fraud and Abuse Act, the Foreign Intelligence Surveillance Court and the Fourth Amendment which guarantees protection against unreasonable search and seizure.[23] Contextually, the United States must ensure that any legislative action balances individuals' protection with national security requirements, an area which the Department of Commerce recognized in the post-Schrems II White Paper as being outside of the primary concern and European Union jurisdiction and instead the responsibility of individual Member States.[24]

The differences in circumstances and national interests demonstrate there is a basic incongruity at the centre of the United States and European Union data transfer conundrum that require longer-term and more

22 EUR-Lex - 12012P/TXT - EN - EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A12012P%2FTXT.

23 Schrems, Maximilian. FACEBOOK IRELAND LTD. p. 42.

24 Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II. p. 23.

ambitious approaches to redesigning international collaboration and transfers. Four such long-term proposals are outlined below with the purpose of spurring more proactive approaches to transatlantic data relationships and their future applications.

Proposal 1: Collaboration through Multilateral Data Trusts (MDTs)

Data sharing between the European Union and the United States is increasingly becoming difficult, due in no small part to the considerable differences in domestic laws that regulate issues such as privacy, surveillance, and national security. In the absence of one regulatory regime taking over, which is highly unlikely, a hybrid regulatory regime may have to be developed to enable longer term cooperation and collaboration. One conceptual design for the new regime would be that of a **Multilateral Data Trust** between the European Union and the United States.

Data Trusts are legal instruments that appoint a steward or trustee to "provide independent third-party stewardship of data" as defined by the Open Data Institute.[25] The Multilateral Data Trust between the European Union and the United States could therefore be created as an oversight body with the stated goal of the management, enforcement and governance of the data transfers between the jurisdictions. The MDT oversight body could be created as a hybrid between a more traditional data trust model and a civic data trust, creating a board of overseers from both jurisdictions with representation from governments, civil society and companies. A civic data trust was most recently proposed by Sidewalk Labs as part of their Waterfront Toronto smart city project[26]. The civic data trust was proposed as a "independent entity to control, manage, and make publicly accessible

25 Works, ThinkData. Data Trusts - Democratizing Data & Data Access. https://www.thinkdataworks.com/data-trusts.

26 "Toronto Moves on from Sidewalk Labs Controversy with New Waterfront Vision." Cities Today - Connecting the World's Urban Leaders, 15 Mar. 2021, https://cities-today.com/toronto-moves-on-from-sidewalk-labs-controversy-with-new-waterfront-vision/

all data that could reasonably be considered a public asset.", as well as a decision-making body on data tools and use for the project[27].

The benefit of a hybrid model MDT would stem from the fact that the trust would create its own governance system without the need to significantly modify domestic laws to ensure compliance. Further, the model could address concerns raised under both Schrems 1 and 2 regarding redress options for EU citizens as well as national surveillance activities by establishing a dispute resolution mechanism and barring entities outside the trust from obtaining access to information outside of the specific purposes delineated under the trust agreement.

Under the MDT model, companies could therefore voluntarily opt in to participate in a similar way as that undertaken through the previous Safe Harbour and Privacy Shield regimes, namely agree to participate and follow the rules of the MDT in exchange for streamlined regulatory compliance requirements and less of a regulatory burden to individually assess privacy regimes and regulation. Companies choosing to participate in the MDT would however have to abide by the governance model and structure set through the oversight body, which may not be a feasible option for all organizations.

Under this model, further consideration is needed to determine what an equitable trustee model would entail, and which actors should be included. For example, the European Commission is comprised of Member States; would European Union leadership participation suffice under this model or would individual countries also seek to participate? Similarly, the MDT model would not necessarily be the only trust, but could act as a governance umbrella for smaller and more sector specific trusts within the framework. This would also allow more regulated areas like financial information and healthcare data to be protected at a higher level than non-identifiable or non-personal data.

The Multilateral Data Trust model would take a number of the practices established under the Safe Harbour and the Privacy Shield frameworks and house them within a common set of trust rules which would be

27 "'Urban Data' & 'Civic Data Trusts' in the Smart City." Centre for Free Expression, 6 Aug. 2019, https://cfe.ryerson.ca/blog/2019/08/%E2%80%9Curban-data%E2%80%9D-%E2%80%9Ccivic-data-trusts%E2%80%9D-smart-city.

administered by a third-party steward. It could therefore allow for a more seamless transfer of data between the two jurisdictions as bound and established within the rules of the trust, with more visibility and accountability for both sides.

However, since data trusts in general have been administered at a more micro level, the concept of Multilateral Data Trust at the multinational level would require an expansion of the understanding and the scope of what a trust can perform. Further, MDT as used in this hybrid case would leverage some of the existing legal structures of a trust, but not constitute a singular trust, which could create impediments to adoption and codification. This would constitute a possible barrier to the MDT model, as demonstrated by the Sidewalk Labs example where the proposed "independent urban data trust" model was considered to be incongruous with Canadian laws, since the law requires specific identifiable beneficiaries of a trust which the general public could not be argued to be[28]. Therefore, the MDT will need to be defined as a departure and a separate entity from simply a data trust, or risk being limited by current legislation defining and scoping the use of data trusts.

Proposal 2: Data Embassies or Data Trade Agreements

Through the decisions issued in both Schrems cases, the Court of Justice of the European Union has sent strong signals and expectations that privacy rights for European Union citizens have a level of mobility and permanence that is no longer impacted by jurisdictional boundaries. While Schrems II does not go as far as to require countries to adopt new GDPR compliant laws since that would arguably be considered *ultra vires*, the expectation of "adequate level of protection" with no concrete definition of adequacy leaves the door open to the European Union adopting a more authoritative stance on global privacy compliance in the future.[29].

28 "'Urban Data' & 'Civic Data Trusts' in the Smart City." Centre for Free Expression, 6 Aug. 2019, https://cfe.ryerson.ca/blog/2019/08/%E2%80%9Curban-data%E2%80%9D-%E2%80%9Ccivic-data-trusts%E2%80%9D-smart-city.

29 CURIA - Documents. https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155. Accessed 12 Apr. 2021.

The European Union's desire to have legislative protections follow the individual regardless of which country they may be in at a given time forms the foundation of the second proposal of grounding future data agreements in international law. While there are a number of ways in which this could be accomplished, the second proposal will focus on the following approaches:

- The concept of Data Embassies and Data Diplomatic Immunity
- The possibility for Data Trade Agreement Provisions

The concept of a Data Embassy is relatively new, and few jurisdictions have spearheaded discussions in this space. The governments of Estonia and Luxembourg first introduced the concept as part of a bilateral agreement in 2017 that allowed Estonia to host data and information in Luxembourg state-owned servers while being considered sovereign extensions in the same way a physical embassy would be.[30] In 2018, the Kingdom of Bahrain extended the use of Data Embassies by implementing the *Legislative Decree No. 56 of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties,* also known as the Cloud Law[31]. Article 3 of the Cloud Law stipulates that data stored in data centres which provide Cloud Computing services "shall be subject to the exclusive jurisdiction of the competent courts and competent public authorities, and the application of the laws, of the Foreign State in which the Customer is domiciled, constituted or established."[32]

This precedent creates the opportunity for a new data transfer agreement grounded in a Data Embassy model. This would entail both the European Union and the United States entering into a bilateral Data or a Cloud Embassy system. The system would allow both jurisdictions to create respective Data Embassies that could act as sovereignty extensions and limit the need for information to travel outside of a designated sovereign area. While this would help address both the adequacy requirement and concerns of overreaching national security legislation raised by the CJEU, the Data Embassy models as currently designed may limit business

30 Tamimi, Al, et al. Diplomatic Immunity for Data: Bahrain's Data Embassy Law | Lexology. https://www.lexology.com/library/detail.aspx?g=1498c8dc-5902-4f90-8a87-9c7eea170998. 2021.

31 Tamimi, Al, et al. Diplomatic Immunity for Data: Bahrain's Data Embassy Law | Lexology. https://www.lexology.com/library/detail.aspx?g=1498c8dc-5902-4f90-8a87-9c7eea170998.

32 Bahrain Business Laws | Law of Providing Cloud Computing Services to Foreign Parties. https://bahrainbusinesslaws.com/laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties. Accessed 12 Apr. 2021.

incentives for participation since some of the same concerns around data storage and mobility between jurisdictions would be replicated, as well as possibly involve a requirement for companies to have limited access to their own data and thus may not present a viable option[33].

However, a partial use of the model could be adapted for use in this case through the creation of **Data Diplomatic Immunity**. The concept of Diplomatic Immunity is outlined in the Vienna Convention on Diplomatic Relations, although it has generally applied to State representatives in the form of diplomatic agents. Article 31 of the Vienna convention confers immunity to diplomatic actors from the criminal jurisdiction of the State in which they are operating in, instead extending the sovereignty of their sending State. [34] The concept of Data Diplomatic Immunity could thus be described as an extension of the concept of Data Sovereignty in international territories.

Data Sovereignty

Data Sovereignty is the concept that nation states can assert control and legislative jurisdiction over data in their territory on behalf of their citizens. This has generally been achieved through the assertions of geopolitical power, international agreements about sovereignty recognition, and domestic policy development as Emily Wu outlines, and involves the expectation that data generated, processed, stored, collected or belonging to a particular nation is therefore subject to the laws of the respective nation.[35]

While over 100 countries currently have some form of data sovereignty policy, applications and definitions differ from jurisdiction to jurisdiction. This ranges from the expectation of strict compliance and equivalency with privacy rules for European Union members under GDPR, to legal requirements in Germany any organization processing German nationals' information to comply with government's data protection requirements, even if located outside the geographic boundaries of the country[36]

33 "Estonia to Open the World's First Data Embassy in Luxembourg." E-Estonia, 14 June 2017, https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

34 Vienna Convention on Diplomatic Relations, 1961. p. 16.

35 "Data Sovereignty and localization"-Emily Wu, 2021

36 "What Is Data Sovereignty? Everything You Need to Know." Permission.Io, 11 Aug. 2020, https://permission.io/blog/data-sovereignty/.

In the context of data sharing between the EU and the United States, Data Diplomatic Immunity could be a feature of the new agreement, allowing data sharing between jurisdictions to continue under the umbrella of national data protections. Practically, this would mean a European Union citizen such as Max Schrems would continue to have the same protection over his personal information independent of the jurisdiction the data travelled to, as well as legal recourse in the European Courts for any grievance leveraged. While the concept could be difficult to implement and require agreements from the Department of Justice to uphold decisions, further research on the topic may be warranted in light of the possibilities to build robust data cooperation grounded in international relations.

Possible limitations to this approach however could stem from incongruity with other existing legislation in the United States such as the *Clarifying Lawful Overseas Use of Data Act*, or "CLOUD Act."[37] The CLOUD Act enables law enforcement in the United States to compel domestically based technology companies to provide information required via subpoena or warrant, regardless of there the information is stored.[38] The United States. Department of Justice and European Commission have been in discussions on electronic evidence sharing agreements, demonstrating the need for clear future delineation on areas where Data Diplomatic Immunity would need to incorporate provisions for information sharing for the purpose of combatting serious crime and terrorism, or risk becoming exploitable by negative actors.

The second path the European Union and the United States could explore is through the creation of data trading agreement provisions as part of a **revived Transatlantic Trade Agreement**. While its predecessor, the Transatlantic Trade and Investment Partnership (TTIP) unsuccessfully concluded negotiations in 2016, the new Biden administration could revisit the possibilities of a new European Union and United States trade partnership. The merits of creating one of the largest trading zones would be numerous, with an estimated boost to the EU's economy of $142 billion

37 U.S. Department of Justice." Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act". https://www.justice.gov/opa/press-release/file/1153446/download

38 U.K.-U.S. Data Sharing Agreement—Implications for Canada | McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/techlex/uk-us-data-sharing-agreement-implications-canada.

and over $100 billion for the United States.[39] Further, a revived trade agreement could include new provisions enabling the flow of data between the two jurisdictions.

In recent years, trade agreements have increasingly recognized the impact data can have on facilitating trade. The Comprehensive Economic and Trade Agreement (CETA) ratified between the European Union and Canada included provisions on both telecommunications and electronic commerce. Similarly, the recently revised Canada-United States-Mexico Agreement. (CUSMA) included provisions on digital trade aimed at both protecting data for public policy use, as well as minimizing data localization requirements that could pose an impediment to trade.[40] The CUSMA Agreement also touches upon another necessary requirement in facilitating the seamless data transfer between jurisdictions, namely a dispute resolution mechanism. The Agreement improves upon the previous chapter 20 of NAFTA to encourage informal dispute resolution where possible, or the establishment of independent panels with equal representation from each country to hear complaints and allow for open dispute-settlement hearings including non-governmental entities.[41] This dispute resolution mechanism format could allow for any complaints emerging in the context of a data transfer between the United States and Europe to be adjudicated in a similar fashion to any other provision contested under a trade agreement.

Additional provisions therefore on a Data Transfer Agreement as part of a larger trade agreement may not only be possible, but a concrete requirement in the not-so-distant future. In a report issued in 2019, McKinsey found that trade in services overall has grown 60 percent faster than trade in goods in the last decade alone.[42] Cross-border data flows have increased substantially in recent years, with bandwidth used across borders

39 Wirtz, Bill. Biden Has an Opportunity to Improve Trade With Europe. https://thedispatch.com/p/biden-has-an-opportunity-to-improve.

40 Canada, Global Affairs. "Canada-United States-Mexico Agreement (CUSMA) - Digital Trade Chapter Summary." GAC, 15 Aug. 2014, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/digital_trade-commerce_numerique.aspx?lang=eng.

41 Canada, Global Affairs. "Canada-United States-Mexico Agreement (CUSMA) - State-to-State Dispute Settlement Chapter Summary." GAC, 15 Aug. 2014, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/state-etat.aspx?lang=eng.

42 Globalization in Transition: The Future of Trade and Global Value Chains | McKinsey. https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains.

increasing 45 times between 2005 and 2016 and estimated to accelerate in coming years with technological advancements in AI and 5G.[43]

Therefore, the enshrinement of data transfer rules in a revived Transatlantic Trade Agreement could offer additional incentives and mechanisms for both jurisdictions to reach a common set of principles to guide all aspect of the relationship, including the use and stewardship of data. However, tying the concepts of data transfers to larger trade negotiations such as the Transatlantic Trade Agreement could risk further delays to the data transfer relationship between jurisdictions if other trade disputed issues prevent the successful resolution of a new TTA.

Proposal 3: International Framework for the Transfer of Data and the Role of Standards

The third proposal would entail the creation of a principles-based International Framework for the Transfer of Data. While this framework could primarily focus on enabling the transfer of data between the European Union and the United States, there could ultimately be a larger global application to its creation. The framework would set out a series of principles adopting jurisdictions would agree to abide by, including around privacy, interoperability, data portability and transfer, jurisdiction and accessibility to name a few.

As regulatory systems and rules relating to national sovereignty and data continue to grow and expand, the principles-based framework could ensure transfers and collaboration can achieve the best outcome without the need for jurisdictional strong-arming. A concrete example of a relatively successful model in this area is the World Health Organization's Framework Convention on Tobacco Control (WHO FCTC). The Convention entered into force in 2005 and has 168 signatory states, making it one of the most adopted treaties in the history of the United Nations.[44] It sets out principles which signatory countries must adhere to, including

43 Digital Globalization: The New Era of Global Flows | McKinsey. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

44 "WHO | WHO Framework Convention on Tobacco Control." WHO, World Health Organization, http://www.who.int/fctc/text_download/en/.

overarching values on the primacy of health, and sets out objectives each country can implement in accordance with their own domestic laws and jurisdictional requirements.

The Convention on Tobacco Control therefore sets out a possible path the United States and the European Union could leverage. A proposed **International Framework on the Transfer of Data (IFTD)** could embrace a similar approach to the FCTC and be housed under the jurisdiction of the International Telecommunications Union (ITU), of which both the United States and most European Union countries are members of. Further, the new Framework could leverage a number of compliance mechanisms including overarching principles around the importance of data flows and individual privacy, with guidelines on ratification through a mix of legislation, regulation and standardization.

The principles-based approach to IFTD would therefore allow for adoption by the signatory states without the fear of incongruous legislation, providing a framework under which national sovereignty and international collaboration could co-exist. It would also allow for the development of a more nimble framework that could keep pace with the speed of innovation with less detrimental impacts from legislative primacy battles or delayed legislative systems that could render some of the solutions created obsolete before they are even implemented.

One mechanism through which the Framework could be augmented and implemented already exists under the auspices of ITU and in the information and communications technology ecosystem more broadly: standardization. The principles-based framework could leverage the development and adoption of common standards both to address technical questions, as well as to outline requirements in areas such as governance. Furthermore, both jurisdictions already participate an international standards development in a robust way through organisations such as the International Organization for Standardization (ISO), the European Telecommunication Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers (IEEE) and The National Institute of Standards and Technology (NIST). This approach, through the use of international

standards as a means to advance trade is recognized and encouraged in the World Trade Organization's Technical Barriers to Trade Agreement.[45]

The **International Framework on the Transfer of Data (IFTD)** would therefore be created in the spirit of the WTO-TBT agreement and require regulators to use and incorporate international standards by static or ambulatory reference as a basis for regulation in order to meet their intended regulatory objectives.[46] This approach would offer measurable actions both jurisdictions can take to create a more integrated policy ecosystem based on international standards, guidelines, and principles that can also be leveraged in creating a more robust international approach to the transfer of data without local regulatory impediments. Possible impediments to this approach could arise due to the length the standards development process generally entail, often spanning years. While organizations such as the Canadian-based CIO Strategy Council have made strides in recent years to develop standards at a pace closer to that of innovation, most Standards Development Organizations and processes still require a long timing runway that may delay regulatory adoption[47].

Proposal 4: National Privacy Framework in the United States

The fourth and final proposal is the creation of a national privacy framework in the United States that would govern, among other things, individuals' rights and privacy in the digital ecosystem. Historically, this has been a notoriously difficult area to legislate, particularly due to the fact that any privacy framework in the United States must address the required balance between individual rights and national security.

The nexus of national security, technology, and personal privacy and rights has been a highly debated area in the United States in recent years.

45 WTO | Technical Barriers to Trade. https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm.

46 "Guidelines for Incorporating Standards by Reference in Regulations to Support Public Policy Objectives." Standards Council of Canada - Conseil Canadien Des Normes, 18 Sept. 2018, https://www.scc.ca/en/about-scc/publications/documents-de-politique/guidelines-for-incorporating-standards-reference-regulations-support-public-policy-objectives.

47 The author of the paper previously worked for the CIO Strategy Council organization.

In light of the Pensacola and San Bernadino cases, the Federal Bureau of Investigation has been engaging in public and legal battles with companies like Apple over access to personal information that is considered relevant to national security and combatting terrorism, particularly when that information is encrypted on a personal phone. While Apple has responded by refusing to comply and provide a device back-door under what the company sees as a breech to the Fourth Amendment rights, the debate continues with former Attorney General William Barr stating in 2019 that encrypting information on devices was the equivalent of creating "law-free zones" since law enforcement could not access them.[48] These cases demonstrate both the complexity of the issue, as well as the difficult task of finding the appropriate regulatory balance.

Nevertheless, recent indicators offer hope that the prospect of a national privacy framework is no longer a far-removed ideal. The California Consumer Privacy Act came into effect on January 1st, 2020 and has been hailed as the "most comprehensive" privacy legislation in the United States by the American Bar Association.[49] While there are notable differences between the CCPA and GDPR, including in scope and jurisdiction, there are also underlying similarities that present CCPA as a possible alternative should its scope be expanded to the national level. Washington state also recently passed the Senate Bill 5062 or the "Washington Privacy Act" That would grant consumers the ability to correct, modify, and see their personal data as collected by businesses who would have to adopt security standards among other provisions.[50] California and Washington state have also recently been joined by Virginia as one of several states to legislate consumer privacy and create a United States made road map for the implementation and adoption of these provisions.

Notably however, advances have not been limited only to the state level. Increasingly, there has also been bipartisan agreement that a national privacy framework could not only offer necessary protection to citizens,

48 "Barr's Call for Encryption Backdoors Has Reawakened a Years-Old Debate." MIT Technology Review, https://www.technologyreview.com/2019/07/24/134062/trumps-justice-department-calls-for-encryption-backdoor-law/.

49 What Businesses Need to Know About the California Consumer Privacy Act. https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/. Accessed 25 Apr. 2021.

50 Washington State Inches Closer to Passing Consumer Privacy Law. https://news.bloomberglaw.com/privacy-and-data-security/washington-state-inches-closer-to-passing-consumer-privacy-law.

but also strengthen the United States geopolitical standing and competitiveness. Senators Wicker, Thune and Fischer introduced in September of 2020 the "*Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act*" which would enable more customer control and transparency over data, as well as strengthening the Federal Trade Commission's (FTC) powers in respect of administering the Act.[51]

The renewed debate and support for federal data privacy legislation is thus a reality in the medium term for the United States. While the direct impact would arguably be satisfying the privacy equivalency requirement the European Union outlined in the Schrems II decision, the implications are much broader than just the impact to the transatlantic relationship and could become a strategic asset the United States can leverage to strengthen international competition and collaboration.

Conclusion

The July 2020 Schrems II decision is only the most recent setback in the larger debate being waged on the future of data sharing between the European Union and the United States, and the role of data and information sharing between countries more broadly. While a short-term solution based on the refined use of the Standard Contractual Clauses provision would allow for a temporary path forward, the larger legal and governance incongruities between the two jurisdictions would make this approach challenging to maintain for any significant period of time.

This paper proposes instead that the larger data transfer ecosystem should be updated to reflect not only present-day requirements, but future realities that may create new impediments to the transatlantic data sharing relationship. The options rage in nature from the creation of Multilateral Data Trusts, revisioning the concept of Diplomatic Immunity to extend

51 "Wicker, Thune, Fischer, Blackburn Introduce Consumer Data Privacy Legislation." U.S. Senate Committee on Commerce, Science, & Transportation, 17 Sept. 2020, https://www.commerce.senate.gov/2020/9/wicker-thune-fischer-blackburn-introduce-consumer-data-privacy-legislation.

to data and information as a new Data Diplomatic Immunity, incorporate data transfers as part of future trade agreements, creating International Frameworks on the Transfer of Data and enabling the creation of National Privacy Frameworks in the United States.

The options offer different regulatory paths from international agreements to national legislation and standardization as policy paths that can be explored in designing the future of data sharing and a more robust international blueprint in this area. Ultimately however, the redesign and enablement of data sharing between jurisdictions in a contemporary concept will require the delicate balancing of commercial interests, national safety and personal privacy and may necessitate a multi-solution approach leveraging a number of the proposals outlined in tandem, as opposed to one singular path forward.

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America