INNOVATORS
www.innovatorsnetwork.org

The Future of US-EU Data Transfers – What to Expect Without Privacy Shield

Rapporteur's Report

By Paula J. Bruening
Innovators Network Privacy Fellow,
Founder and Principal,
Casentino Strategies, LLC

1401 K Street NW Suite 501
Washington, DC 20005
www.innovatorsnetwork.org
info@ACTonline.org

Introduction

On September 25, 2020, ACT | The App Association and the Innovators Network Foundation (INF) convened a virtual Roundtable to consider the impact of the Court of Justice of the European Union (CJEU) decision in *Data Protection Commissioner v. Facebook Ireland Limited and Maximiliian Schrems* (*"Schrems II"*)[1] and its invalidation of the Privacy Shield. The Privacy Shield has acted as a principal legal method for transferring personal data from the European Union (EU) to the United States (U.S.). It has been particularly valuable for small businesses which may lack the resources necessary to implement other, more costly transfer mechanisms.

The discussion brought together key staff from EU and U.S. agencies, recognized privacy experts, and representatives of the American small business community, all of whom rely on the EU-U.S. Privacy Shield. Participants considered:

- The continued value and importance of U.S.-EU data flows and digital trade;
- Next steps in the evolution of frameworks to facilitate transatlantic data flows;
- The potential impact of the *Schrems II* decision;
- The progress of ongoing discussions to renegotiate the EU-U.S. Privacy Shield; and
- How EU member states and the U.S. government can support transatlantic data flows and data privacy protections going forward.

The agenda for the Roundtable is included in this report as an appendix.

This report provides background on the decision, a thematic review of the Roundtable discussion, and concludes by recommending measures policymakers might consider as they work toward new solutions.

Context for the Roundtable

The July 16, 2020, ruling of the Court of Justice of the European Union in *Schrems II* invalidated the EU-U.S. Privacy Shield for the lawful transfer of personal data to processors in the United States.[2] While the decision upheld EU Standard Contractual Clauses (SCCs) for transfers outside the EU/European Economic Area (EEA), it cast substantial doubt on their long-term viability.

The CJEU held that EU–U.S. Privacy Shield does not sufficiently protect EU personal data from access and use by U.S. public authorities on the basis of U.S. domestic law, specifically highlighting the lack of opportunity for European citizens to challenge surveillance decisions. Under current law, there is no individualized review process for foreign intelligence surveillance decisions that target non-U.S. persons, such as Europeans residing in Europe.[3] Moreover, there is no review process for the bulk collection of data transferred by wire between Europe and the United States that may include European citizen data.[4] The CJEU insisted that the United States provide persons in Europe with redress - "actionable rights" of challenge before U.S. courts - that are "essentially equivalent" to privacy rights enjoyed within the EU.

In its decision, the CJEU confirmed that EU SCCs provide appropriate safeguards for international transfers of personal data. To ensure compliance with the level of protection required by EU law, however, the CJEU stressed that when relying on SCCs, data controllers established in the EU need to consider 1) the international data transfer agreements based on the SCCs agreed between them and the data importer established in the third country; and 2) the relevant aspects of the data importer's legal system, in particular any access by public authorities to the data transferred. If an essentially equivalent level of protection cannot be guaranteed, data controllers are required to terminate such data transfers and also, if necessary, the contract with the data processor in the third country. This means that determining the validity of individual SCCs entered into by companies essentially will be left to Data Protection Authorities (DPAs) of individual EU Member States. It is difficult to see how a DPA could arrive at a finding of essential equivalence, based on the CJEU's ruling.

The Schrems II ruling leaves thousands of American companies that have relied upon the Privacy Shield without the benefit of this mechanism for lawful data transfer. Moreover, the decision allowed for no grace period, so the invalidation took immediate effect. While other means, such as SCCs and Binding Corporate Rules (BCRs), are available for U.S. companies to comply with EU data protection laws, these mechanisms impose additional costs and uncertainty. These costs especially affect small businesses, which often have limited resources to invest in compliance.

Themes and Discussion

The Impact of the Schrems II Decision on Small Businesses

While the CJEU opinion in *Schrems II* affects all companies transferring data from the EU to the United States, discussion during the panel focused on the impact of the decision on small businesses. The *Schrems II* ruling affects 5,300 companies – 70 percent of which are small and medium sized enterprises (SMEs).[5] For many SMEs, the legal flow of data across the Atlantic underpins key aspects of their operations. These organizations are now required to adopt Standard Contractual Clauses (SCCs) or other more costly methods to support the legal flow of data across the Atlantic that is essential to their operations. The decision to invest in implementing SCCs is complicated by the legal uncertainty that surrounds them.

Participants in the Roundtable noted that there is little that U.S.-based SMEs can do to remedy the situation, given the broader context of U.S. privacy and surveillance law, other than implementing SCCs. Companies committed to full compliance with current U.S. law and the GDPR remain subject to lawful data access requests by U.S. law enforcement and national security agencies that the CJEU finds problematic. Thus, in spite of their best efforts

at compliance, small businesses are now at risk of having the flow of data from the EU interrupted. Faced with this new and more complex compliance burden and the uncertainty surrounding SCCs, many companies are now weighing whether to suspend data transfers from the EU until conditions change and how doing so would affect the viability of their business.

Participants also placed the questions *Schrems II* raises for SMEs into the broader context of compliance with data protection and privacy laws generally. SMEs that have operated internationally from their inception find that the introduction of each new law and agreement requires them to invest additional resources in compliance. Each new law, agreement, or framework introduces new risks and imposes new costs to mitigate them. The funds dedicated to address each these are funds that are not available to hire new employees, enter into new ventures, and grow the business. The invalidation of the Privacy Shield, and the lack of legal clarity surrounding SCCs, introduce yet additional new uncertainties.

Ongoing Efforts of the U.S. and EU Governments

The United States Department of Commerce

The full impact of the invalidation of the Privacy Shield on business is well understood by the U.S. Department of Commerce (DOC). The agency is engaged in discussions with EU partners, looking for a way to continue the safe flow of data between the EU and the United States. To help businesses, the DOC offers guidance for companies on its website in the form of FAQs.[6] It was noted that the U.S. Federal Trade Commission affirmed that companies are still required to abide by their commitments to customers and that those commitments remain enforceable.

The DOC is also beginning discussion with the European Commission (EC) about what enhancements could be made to the Privacy Shield to address the court's concerns. As the court's decision turns on issues related national security law, the DOC is seeking a solution consistent with existing U.S. national security law.

Participants noted that while these efforts are underway, a good deal of uncertainty about SCCs remains. The DOC is looking for a way to stabilize data transfers between U.S. and the EU, particularly around SCCs.

European Commission

In addressing the invalidation of Privacy Shield and its consequences for business, the Commission noted two goals:

- First, to guarantee that the fundamental rights of EU residents are protected, and
- Second, to ensure solid transfer mechanisms are available for data to support trade and social interaction.

Technical level discussions with the United States are currently in progress to explore the possibility of a new and improved Privacy Shield or another transatlantic data framework. Work is also underway to finalize modernization of existing SCCs. That effort was already in progress prior to the *Schrems II* decision, and the current effort attempts to align them to the General Data Protection Regulation (GDPR) and to adapt them to modern business realities. There is also an effort to make them more useful for SMEs. A draft is expected in the coming weeks and final adoption in coming months.

It was emphasized that one goal of the review of the SCCs is to align them with the interpretation of the DPAs, and that a common interpretation of the *Schrems II* judgment across the EU and a coordinated response will be important. To that end, the Commission is working with DPAs and the European Data Protection Board (EDPB) on guidance for SCC implementation. The EDPB issued the first round of guidance in its "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems."[7] It has now established a new task force to follow up with more detailed, concrete guidance. Among the questions it is addressing is the steps companies must take to demonstrate the circumstances of the data transfer and possible safeguards they can implement.

What SMEs Need

Participants emphasized again and again the need to assure SMEs of the availability of a stable, cost-effective mechanism to transfer data lawfully from the EU to the United States. They discussed at length the need for a new version of the Privacy Shield that can withstand legal scrutiny and create legal certainty around SCCs.

Participants emphasized that while policymakers work toward establishing new data transfer mechanisms, the concerns of small businesses exist in the details. Discussion focused on the lack of practical guidance available to SMEs and entrepreneurs, who find it difficult to interpret – and therefore appropriately fulfil - requirements. SMEs at all stages of development would benefit from guidance that is technical, practical, and concrete, particularly post *Schrems II*. They cited the need for real world case studies and examples. Such guidance would limit the cost of legal counsel for emerging companies and SMEs, enable them to build privacy protections into new technologies and applications in the earliest stages of their development, and assist as they negotiate contracts with business partners. This guidance is particularly important as companies conduct the analysis required to implement SCCs.

Issues of National Surveillance

Because the CJEU based its decision on what it characterized as deficiencies of U.S. surveillance law as it applies to EU citizens, the issues raised by *Schrems II* are complicated to resolve. Some participants noted that, in their opinion, despite years of effort, the CJEU continues to misunderstand the nature of U.S. law enforcement activities. They asserted that from a practical standpoint, perceptions about what happens diverge significantly from what happens in fact.

Discussion also focused on concerns that to meet the Court's demands would require reworking of American intelligence and law enforcement authorities or providing a carve-out for European citizens in particular. It was noted that, leaving aside the question whether amendments are appropriate, such fundamental changes are not likely to occur.

At the same time, it was acknowledged that the United States and the EU share similar goals and a similar philosophy about privacy. Participants noted that room remains for fuller explanation and better understanding of U.S. law related to government access to data. The Privacy Shield, was helpful in this regard, and promoted a greater understanding of how U.S. national security and data access laws function as well as their provisions for oversight and limits.

What the EU and U.S. Can Do to Promote Resolution

In considering a path forward, participants noted that this is not a question that companies can solve. Because the *Schrems II* decision turns on questions of national security law, any solution will have to be agreed to between governments.

Much of the Roundtable discussion centered on the common philosophy about privacy shared by the EU and the U.S. Any attempts to resolve the fallout of *Schrems II* will rest on that shared understanding. Participants noted that both the EU and the United States have national security laws, and that in fact the two do not diverge as much might initially appear. The differences exist in language and approach, and the key to a solution is to bridge the gap between them. To resolve this, it will be important to better understand how the GDPR is applied by member state DPAs and also how individual member states apply rules related to government access to data. Continuing discussions between governments will be essential. However, to best serve companies, particularly SMEs, conceptual solutions will need to be translated into concrete, specific guidance.

It was clear from discussion that while the United States might make modest changes through an executive order or statute to accommodate EU concerns, wholesale revision of U.S. law cannot be expected. However, the EU seeks a solution that fully complies with all of the requirements of the CJEU. How such a solution is arrived at would depend on what is feasible within the U.S. legal framework.

It was suggested that the EU could provide guidance on GDPR compliance that could accommodate U.S. interest in its own national security. Considering the question more broadly, one participant noted that this problem is shared by countries other than the U.S. and that discussion among democratic countries about how governments govern access to data would benefit all parties.

Participants agreed that the longstanding relationship between the U.S. and the EU, and the importance of resolving the issues of data flows *Schrems II* to innovation and economic growth on both side of the Atlantic make addressing the issues that arise from the decision is of critical importance.

RECOMMENDATIONS

The following recommendations reflect my assessment of steps policymakers can take to further resolution of the issues raised by *Schrems II*.

1. *Pass credible federal privacy legislation in the United States.* A federal privacy law that provides real protections for all individuals and requires responsible data collection, processing, and security within companies would promote data protection and privacy-respectful practices across the digital marketplace. Such a law should be based on principles common to data protection laws and regulations across jurisdictions globally – including with the GDPR - to promote interoperability and trust. Such a law would enhance protections, streamline compliance and ease the burden on businesses, including SMEs.

2. *Continue the EU-U.S. dialogue about questions of national surveillance and law enforcement.* The Privacy Shield established a review process that furthered discussion about questions of national surveillance and promoted a better understanding of how those laws work in practice. In the Privacy Shield's absence, this dialogue should continue in order to promote interpretation of laws in a way that respects national security interests of both the United States and the EU, and candidly reflects the extent of practical risk to individuals' personal data.

3. *Continue to develop and publish guidance to help businesses, and particularly SMEs, comply with relevant law.* Regulators and relevant agencies in the United States and the EU must continue to provide concrete, practical guidance about how SMEs can comply with the GDPR and meet the requirements of SCCs. The financial burden of compliance falls heavily on smaller companies, particularly in the early stages of their development. Specific guidance and examples can help SMEs comply and incorporate compliant practices into their products and services at the outset, and avoid incurring heavy costs. Such guidance can also help companies now turning to SCCs by creating more certainty about the appropriate legal analysis and the steps they must take to ensure that the necessary safeguards are in place. Development of guidance would benefit from the participation of trade associations that would bring to the discussion an understanding of the compliance challenges small businesses face.

4 *Explore the role of technical solutions.* Technological measures – including encryption - may offer some help in mitigating privacy concerns and achieving the goals of EU data protection law. Policymakers should consider the extent to which these can address concerns when working toward any new framework or mechanism for lawful data transfer between the EU and United States.

5 *Engage international organizations and forums to examine how surveillance laws and government access to data work in practice and their impact on trusted data flows.* Issues related to the impact of national security law on cross-border data flows are not limited the United States and the EU. International organizations can serve in an important convening role for democratic governments to create a better understanding of how surveillance laws function in practice and their impact on the trusted flow of data for commercial and research purposes. They may also serve as a platform for developing frameworks that can help governments mitigate the impact of surveillance on commercial data flows.

APPENDIX

Event Agenda

EU and US policymakers, privacy experts and small business voices explore questions left unanswered by the invalidation of Privacy Shield.

About this Event

On July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield in its decision in the Schrems II case. This ruling leaves thousands of companies without a much-needed streamlined and inexpensive transatlantic data sharing mechanism. Small businesses, which made up 70 percent of Privacy Shield participants, may especially struggle to comply with European data protection laws as they must now use more uncertain and expensive means to comply, like standard contractual clauses (SCCs) and binding corporate rules (BCRs). The CJEU ruling leaves many questions unanswered and leaves Privacy Shield participants exposed to data flow disruption, new compliance expenses, and uncertainty. On a larger scale, this development is likely to result in an interference to digital trade that will harm consumers and businesses on both sides of the Atlantic.

At this event, the App Association will give introductory remarks, followed by a panel moderated by Innovators Network Privacy Fellow and event rapporteur Paula Bruening, founder and principal of Casentino Strategies, LLC. The panel will bring together key policymakers from the EU and United States, known privacy experts, and small business voices. The panel will explore the value and importance of U.S.-EU data flows, potential impacts from the recent CJEU decision to invalidate the Privacy Shield, and the ongoing discussions to renegotiate a framework to facilitate transatlantic data flows.

In the weeks following the webinar, event rapporteur Paula Bruening will issue a report capturing discussion from the panel and recommendations for next steps in renegotiating the Privacy Shield or similar agreement. The report will be circulated to event registrants and widely via the App Association website.

Panelists:

- **Paula Bruening**, Moderator and Rapporteur, Innovators Network Privacy Fellow, Founder and Principal, Casentino Strategies, LLC
- **Alex Greenstein**, Director EU-US Privacy Shield, U.S. Department of Commerce
- **Paul Rosenzweig**, Senior Advisor, Chertoff Group
- **Fernando Guerrero**, Founder and CEO, Nouss/SolidQ
- **Alisa Vekeman**, Policy Officer - International Data Flows and Protection, DG Justice, European Commission

Participants will receive the webinar link via email after they have registered for the event.

Endnotes

[1]Case:C-362/14 Schrems; see also Press Release No. 117/15.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227

[2] Ibid.

[3]See Sec. 702, FISA Amendments Act of 2008, Pub. L. 110–261, title IV, §402, July 10, 2008.

https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf

[4]See Executive Order 12333, United States Intelligence Activities (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)).

https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf

[5]Remarks By Secretary Wilbur Ross at the Privacy Shield Framework, Third Annual Review, September 12, 2019.

https://www.commerce.gov/news/speeches/2019/09/remarks-secretary-wilbur-ross-privacy-shield-framework-third-annual-review

[6]"FAQs: EU-U.S. Privacy Shield Update", U.S. Department of Commerce, August 20, 2020.

https://www.google.com/search?client=safari&rls=en&q=privacy+shield+invalidation+guidance+DOC&ie=UTF-8&oe=UTF-8.

[7]"Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems", European Data Protection Board, adopted July 23, 2020.

https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf