Safe Harbor Is Dead; Long Live the Privacy Shield?

Introduction

How long does it take information to travel across the Atlantic? In 1620, it took the Mayflower 66 days to travel from Plymouth, England to what we now call Cape Cod. Any information the Pilgrims wanted to convey back to England likely would have taken just as long to get back. Fast forward almost 500 years, and what once took 66 days now takes a fraction of a second as gigabits of information traverse undersea cables and other means of communications from one continent to another, often at the speed of light. These data transfers have been facilitated and encouraged by legal regimes designed to protect the rights and interests of the individuals whose data was traveling around the world, while giving data processors and collectors certainty about the applicable laws and requirements.

All of these near-instantaneous data transfers between the European Union (EU) and the United States seemed to stop for the briefest of moments on October 6, 2015, when Max Schrems and his lawyers convinced the European Court of Justice (ECJ) to overturn the U.S.-EU Safe Harbor Framework (Safe Harbor) that had been at the heart of EU to U.S. data transfers for 15 years. Although Safe Harbor already had been subject to criticism by EU data protection regulators, particularly in the wake of the revelation of U.S. government surveillance programs following publication of classified material by former NSA contractor Edward Snowden, the impact of this decision was dramatic. EU data protection law generally prohibits transfers of personal data to any country outside the European Economic Area that does not provide an “adequate” level of data protection. Without Safe Harbor, over 5,000 companies and organizations were forced to adapt their data transfer and privacy policies and practices almost overnight, with
The ECJ decision led to months of negotiations between U.S. and European Commission (EC) officials over a new framework to replace Safe Harbor. European data protection authorities, represented by the Article 29 Working Party (a group comprised of representatives of EU member states, EU institutions, and the EC to provide advice on data protection and privacy issues), had given the two sides until the end of January 2016 to come to a new agreement. As the clock struck midnight on the deadline, EC and U.S. officials announced a new data transfer agreement – the EU-U.S. Privacy Shield Agreement (the Privacy Shield). A few weeks later, they provided the details.

What follows is a brief history of the events that led to the current state of affairs, followed by an analysis of the Privacy Shield, focusing particularly on how the new regime will affect companies and organizations that want to transfer data from the EU to the United States. Lastly, a consideration of the various alternatives that are still on the table for companies, and an assessment of some of the outstanding issues that may play a role in the future of transatlantic information flows, concludes this article.

**What Happened?**

Maximilian Schrems is an Austrian citizen and subscriber to Facebook. As a European Facebook user, he agreed to the general business terms of Facebook’s Irish subsidiary, which operates the Facebook service throughout Europe. He filed a complaint with the Irish data protection commissioner arguing that, even with respect to companies that comply with Safe Harbor, the United States does not provide for an adequate level of data protection because U.S. authorities may access and process his personal data that Facebook is forwarding to its servers in the United States. The Irish data protection commissioner rejected the complaint on the grounds that national data protection authorities are obliged to follow the EC’s decision that Safe Harbor (which Facebook adopted) ensures an
adequate level of data protection. Schrems then took his claim to the Irish High Court, which referred the matter to the ECJ. Prior to the ECJ’s decision, Yves Bot, the ECJ’s advocate general, or chief legal advisor, issued an opinion that the EC decision approving Safe Harbor does not prevent national data protection authorities from performing an independent assessment as to whether the level of data protection is adequate. Further, the advocate general opined that the EC’s Safe Harbor decision is invalid altogether.

The ECJ agreed with the advocate general’s position and declared the decision approving Safe Harbor invalid. It based its decision principally on a finding that the United States is not able to provide for an adequate level of data protection under Safe Harbor because Safe Harbor has too many loopholes. For example, the ECJ cited with concern the fact that Safe Harbor may not apply if “national security, public interest or law enforcement requirements” are at stake, and that U.S. public authorities are not required to comply with Safe Harbor requirements at all.

Initial reactions out of the U.S. government expressed disappointment and concern with the ECJ decision. FTC Chairwoman Edith Ramirez issued a short statement that the FTC would review the decision and evaluate its impact. Ramirez also stated that the FTC would continue to work with its “European colleagues to develop effective solutions that protect consumer privacy with respect to cross-border data transfers.” U.S. Secretary of Commerce Penny Pritzker expressed disappointment in the decision and encouraged reaching an agreement to an updated Safe Harbor framework as soon as possible. White House Press Secretary Josh Earnest told reporters, “We believe this decision was based on incorrect assumptions about data privacy protections in the United States. There is concern about the economic consequences of this particular ruling.”

On the European side of the Atlantic, EC Vice President Andrus Ansip and European Commissioner for Justice Věra Jourová released a statement
focusing on the need to ensure the continuation of transatlantic data flows and expressing their belief that clear guidance for national data protection authorities on how to deal with data transfer requests to the United States in the wake of the ECJ decision would be forthcoming. They also acknowledged the importance of continuing to negotiate a renewed Safe Harbor framework with the United States.

In its statement after the decision was released, the Article 29 Working Party highlighted the problems set forth by the ECJ with Safe Harbor, urged EC and U.S. authorities to continue to negotiate to develop the kinds of legal and technical mechanisms that would allow for data transfers to the United States in a way that respected EU citizens’ fundamental rights, and announced that national data protection authorities would begin taking necessary actions, potentially including enforcement actions, by the end of January 2016 if the United States and the EU failed to reach an agreement.

Over the course of three months, representatives from the U.S. government, the EC, and various EU member states worked tirelessly to reach the deadline imposed by the Article 29 Working Party. On February 2, 2016, EC Vice President Ansip and Commissioner Jourová announced that an agreement had been reached called the “EU-U.S. Privacy Shield.”

Elements of the Privacy Shield

Before moving forward, it is important to briefly review both the concerns that were already bubbling beneath the surface of Safe Harbor, and the specific concerns that led to the ECJ’s invalidation of Safe Harbor. As to the latter, the ECJ’s decision invalidating Safe Harbor rested largely on the ECJ’s negative answer to the question of whether it provided EU citizens with “adequate” protections. As the Article 29 Working Party explained in its statement following the ECJ’s decision, “the question of massive and indiscriminate surveillance is a key element of the Court’s analysis.” For that reason, a significant part of the Privacy Shield deals with access to data by the U.S. government.
With respect to the former, however, there was a growing sense that EU data subjects did not have sufficient ability to know what was going on with their data or to stop it from being used in ways with which they were not comfortable. The EC in November 2013 issued a report with a number of recommendations to improve Safe Harbor. And in a presentation to the European Parliament Committee on Civil Liberties, Justice and Home Affairs shortly before the announcement of the Privacy Shield, Commissioner Jourová highlighted these issues, particularly those related to opportunity for resolution of individual complaints.

All of these concerns were reflected in the elements of the Privacy Shield. Specifically, the agreement focuses on three main issues:

- **Handling Europeans’ Personal Data.** U.S. companies transferring personal data from Europe must commit to satisfying robust obligations regarding how that data is processed. The U.S. Department of Commerce (DOC) and Federal Trade Commission (FTC) will monitor and enforce these commitments, and any company handling human resources data from Europe must commit to comply with decisions by European data protection authorities.

- **U.S. Government Access to Data.** The United States has given the EU written assurances that access to information by public authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards, and oversight mechanisms. There will be an annual joint review conducted by the EC and the DOC to ensure that the agreement is functioning.

- **Protection of EU Citizens’ Rights.** Under the agreement, EU citizens who believe that their data has been misused will have several redress possibilities, and companies to which complaints are directed will have deadlines to respond to such complaints. European data protection authorities may refer complaints to the DOC and the FTC, and for complaints of suspected access to information by national intelligence authorities in the United States, a new ombudsperson will be created.
The details of the Privacy Shield agreement became public on February 29, 2016, when the EC released a set of documents, including a draft adequacy decision, to begin the agreement’s formal adoption process. These documents give companies more information about what requirements will attach to participation in the Privacy Shield. Although most of the draft decision is focused on access to information by U.S. public authorities, here we will focus primarily on the new requirements that will apply to companies that choose to participate in the Privacy Shield.

In particular, companies that participate in the Privacy Shield must commit to abiding by seven principles set forth in the adequacy decision (the Privacy Principles):

- **Notice Principle.** Under this principle, companies must provide consumers with information relating to the processing of personal data (e.g., type of data collected, purpose of processing, right of access and choice, potential transfer conditions, etc.). Companies must have a publicly available privacy policy that both reflects their commitment to the Privacy Principles and provides links to the DOC’s “Privacy Shield” website, a “Privacy Shield List” that will be established as part of the new regime, and the website of an appropriate alternative dispute settlement provider.

- **Choice Principle.** Consumers must be given the ability to opt out of any sharing of their personal data with a third party (other than an agent acting on behalf of the company) or any use of their data for a purpose that is “materially different” from that for which the information was originally collected. Also, companies must obtain affirmative express consent (i.e., opt in) for sharing or materially different use of “sensitive” data.

- **Security Principle.** Companies creating, maintaining, using, or disseminating personal data must take “reasonable and appropriate”
security measures that account for the risks related to the processing and nature of the data. Moreover, any vendors that companies use to “sub-process” data must also contractually agree to provide the same level of protection.

- **Data Integrity and Purpose Limitation Principle.** Personal data collected by companies must be limited to what is relevant, must be reliable for the intended use, and must be accurate, complete, and current.

- **Access Principle.** Consumers have the right to obtain confirmation of whether a company is collecting personal data related to them and to see that data within a reasonable timeframe. This right may be restricted only in exceptional circumstances, and any company that seeks to deny a consumer this right bears the burden of proving that denial is justified. Further, consumers must be able to correct, amend, or delete personal information where it is inaccurate or collected in violation of the Privacy Principles.

- **Accountability for Onward Transfer Principle.** Any transfer of a consumer’s personal data from a company to a different controller or processor can take place only where the transfer is: (i) for limited and specified purposes; and (ii) on the basis of a contract (or comparable arrangement) that provides for the same level of protection as that guaranteed by the Privacy Principles.

- **Recourse, Enforcement, and Liability Principle.** Participating companies must provide robust mechanisms to ensure compliance with the Privacy Principles and recourse – including appropriate remedies – for EU data subjects whose personal data have been processed in a noncompliant manner.

Transparency and enforceability are key themes running throughout these principles. With respect to transparency, one of the primary components is the aforementioned Privacy Shield List – a list of companies that have self-certified their adherence to the Privacy Principles. The DOC will maintain the list – companies must recertify on an annual basis – and any companies that
put themselves on the list will be subject to jurisdiction of authorities in both the United States and Europe. By way of example, the draft adequacy decision notes that any misrepresentation made to the general public regarding adherence to the Privacy Principles is subject to the FTC’s section 5 jurisdiction against unfair or deceptive practices. Similarly, any misrepresentation to the DOC during the course of certification may be actionable under the False Statements Act.

With respect to enforcement, the draft adequacy decision discusses at length what recourse mechanisms are, or must be made, available to EU data subjects that find their data transferred to the United States. In particular, the adequacy decision highlights six avenues for enforcement:

- First, companies that participate in the Privacy Shield must allow EU data subjects to pursue cases of noncompliance directly with the companies. To effectuate this requirement, companies must implement an effective mechanism to deal with complaints. For example, companies must include in their privacy policies clear notice informing consumers about a point of contact, either within or outside the company, that will handle complaints (including any relevant establishment in the EU that can respond to inquiries or complaints), and they must respond to such complaints within 45 days.
- Second, companies must designate an independent dispute resolution body (in either the United States or the EU) to investigate and resolve individual complaints. Such a body must be able to impose sanctions or remedies that are “sufficiently rigorous” to ensure compliance with the Privacy Principles, including the potential for reversal or correction of offending behavior.
- Third, as discussed briefly above, as part of a company’s certification (and recertification), the DOC will verify that the company’s privacy policies conform to the Privacy Principles. Any company that “persistently fails” to abide by the Privacy Principles will not be allowed to recertify. More generally, the DOC will be significantly increasing its
enforcement and monitoring capabilities to perform its role under the Privacy Shield.

- Fourth, the FTC will give priority consideration to complaints implicating the Privacy Principles received from the independent dispute resolution or self-regulatory bodies appointed by the different companies, the DOC, and EU national data protection authorities (DPAs) to determine whether section 5 of the FTC Act has been violated. Any consent decree entered into between the FTC and companies participating in the Privacy Shield must include self-reporting provisions.

- Fifth, as mentioned above, companies are obligated to cooperate in the investigation and resolution of any complaints pursued by European national DPAs that concern processing of human resources data collected in the context of an employment relationship, or if the companies have voluntarily submitted to oversight by the DPAs. The DOC will establish a dedicated point of contact to act as liaison to the European national DPAs.

- Finally, if no other available avenue of redress has satisfactorily resolved the EU data subject’s complaint, the Privacy Shield agreement establishes a new “Privacy Shield Panel” (Panel) that the data subject may invoke for binding arbitration. The Panel will consist of a pool of 20 arbitrators selected by the DOC and the EC, and for each individual dispute the parties may select a panel of 1 to 3 arbitrators from this pool. The Panel will have authority to impose “individual-specific, non-monetary equitable relief” necessary to cure any noncompliance.

What’s Next?

Despite the amount of work that has been put into this effort already, there are a number of steps that remain before the Privacy Shield is fully in effect. In April, the Article 29 Working Party released its opinion on the draft adequacy decision. While the Working Party “welcome[d] the significant improvements brought by the Privacy Shield” as compared to Safe Harbor, it did highlight several issues that it saw in Privacy Shield.
Among other things, the Working Party expressed concern that the limitation principle did not go far enough to ensure that data that is no longer needed by companies is destroyed in a timeline manner. Likewise, it highlighted that the onward transfer principle did not appear to require that companies ensure the data is protected even as it is transferred to additional countries. And despite acknowledging that “additional resources” are made available under Privacy Shield for individuals to exercise their rights, the Working Party expressed concern that the new recourse mechanisms may actually prove to be too complex for most individuals. (The Working Party also had issues with aspects of the Privacy Shield regarding U.S. government handling of data, but those are not as directly relevant to our current discussion.)

The next step would be for EC officials to draft and release a Final Adequacy Decision. That may happen any day now. While it appears unlikely that there will be any significant changes to the Privacy Shield structure in light of the critique from the Working Party, it would not be out of the question for EC officials to attempt to bolster the Final Adequacy Decision by addressing some of those criticisms, either by further explaining how certain aspects will work or by offering tweaks to the details of how the program will work.

Once the EC publishes the Final Adequacy Decision, officials at Commerce will move to have the appropriate requirements in the U.S. published in the Federal Register. Commissioner Jourová stated in early February 2016 that she believes the implementation of the Privacy Shield will take three months – that would mean that the Final Adequacy Decision should be released sometime in May 2016, with action by Commerce following shortly thereafter.

**What to Until Privacy Shield is Adopted?**

What does all of this mean for a company that is trying to transfer data from the EU to the United States today? Unfortunately, about the only thing that is clear is that companies can no longer rely solely on Safe Harbor to transfer
data to the United States: for example, the German DPA has launched enforcement action against companies still relying solely on Safe Harbor. Consequently, companies that have been using Safe Harbor must analyze and implement alternative mechanisms going forward, at least until a new agreement is reached. Those alternatives include:

- **Model Contracts.** The E.U. Model Contracts provide a set of standard clauses, approved and published by the EC, for the transfer of personal data between an EU data controller and a U.S. data controller or between an EU data controller and a U.S. processor (i.e., vendor). However, model contract clauses cannot be altered. The current advantage of this option is that the model clauses are based on a valid decision of the EC, which must be presumed to be lawful.

- **Binding Corporate Rules (BCRs).** BCRs are internal company regulations governing how the flow of personal data is organized and the rights of concerned individuals are protected. BCRs can be adapted to the specific needs of the company but are subject to approval by regulators before they can be relied upon. The approval process is, at best, a highly complicated process that typically has taken years. (As a result, only a small number of companies have adopted BCRs.)

- **Notice and Consent.** Providing clear notice and obtaining the unambiguous and explicit consent of the individuals whose personal data is transferred remains a viable strategy for complying with data transfer rules. However, this is not always the most practical solution because consent can be difficult to obtain in certain circumstances, and some European DPAs (e.g., Germany) discourage use of consent in certain situations.

- **Statutory Exceptions.** Certain statutory exceptions might apply in countries that permit transfers of personal data if specified conditions are met. However, these exceptions are fact-specific and often narrowly construed by EU regulators.

- **Anonymization.** Depending on how the data is intended to be used, companies may consider anonymizing their data prior to transfer.
Notably, this approach is recommended by some of the German data protection authorities. Such an approach could be useful for audits, research, or other tasks where the data analysis is focused on relationships and trends, and not necessarily on the identity of a particular individual. However, companies must be sure that the process of anonymization successfully de-identifies the individuals.

Each of these options has pros and cons; therefore, companies should carefully weigh the different options in light of the particular data, organizations, and purposes of the transfers at issue. Part of that calculation likely should include the Privacy Shield’s chances of success when the inevitable challenges come in court; despite the robust data protection requirements and review mechanisms included in the regime, a number of critics already have focused on perceived loopholes to cast doubt on whether the agreement satisfies EU law.

**Conclusion**

The ECJ’s October 2015 decision cast an enormous cloud of uncertainty over the proper legal mechanisms to govern the flow of data from the EU to the United States. Although officials on both sides of the Atlantic have been working tirelessly since the ECJ’s decision, until the Privacy Shield: (1) is formally adopted in both the EU and the United States; and (2) survives the inevitable legal challenges, that uncertainty will not dissipate. Officials in both the United States and in the EU appear to have done about a good a job as possible to fend off the attacks, but until the ECJ has its say, companies and organizations that transfer data from the EU to the United States will continue to operate under a cloud of uncertainty.

**Additional Resources**

*For other materials on this topic, please refer to the following.*

**Business Law Section Program Library**
Data Privacy and Cybersecurity Due Diligence in M&A Transactions
(PDF) (Audio)
Presented by: Business Law Education, Corporate Compliance, Corporate Counsel, Corporate Governance
Location: 2015 Spring Meeting

The Business Lawyer

After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change
By W. Gregory Voss