LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, JULY 24, 2020

The rise and of fall of the EU-US Privacy Shield

By Heather Antoine and Mallory Petroli

On July 16, the Court of Justice of the European Union announced its much awaited decision in the *Schrems II* case. The court declared that the EU-U.S. Privacy Shield Framework invalid. Finding that the United States cannot provide the requisite level of protection to EU residents' personal data will undoubtedly significantly affect businesses here in the U.S.

Secretary of Commerce Wilbur Ross issued a press release that day stating, "[w]hile the Department of Commerce is deeply disappointed that the court appears to have invalidated the European Commission's adequacy decision underlying the EU-US Privacy Shield, we are still studying the decision to fully understand its practical impacts… We have been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments."

So how did we get here?

New York Times News Service

Max Schrems, an Austrian law student whose legal case against Facebook led the region's highest court to invalidate the previous trans-Atlantic data agreement, in Vienna, Oct. 8, 2015.

PRIVACY AS A HUMAN RIGHT

After WWII and following the United Nations' Universal Declaration of Human Rights in 1948, the Council of Europe adopted the Convention for the Protection of Human Rights and Fundamental Freedoms in 1950. The convention established privacy as a fundamental human right. As recently as 2012 via the EU Charter of Fundamental Rights, this right was not only reaffirmed, but was expanded to include the right to protection of one's personal data. This expansion was intended to formally address the developments of industries that were built to collect and monetize large sets of personal data.

In the U.S., however, most privacy laws revolve around, and are limited to, individual liberties and the sanctity of one's own home against the government. It could be said that American "personhood" is derived from such civil liberties against the government — including free speech, private property and free enterprise — likely derived from U.S. revolutionary history. Privacy is not a fundamental human right that can be used equally to protect U.S. residents from intrusion by both private and public entities. For example, the burden of managing privacy in the private sector in the U.S. is largely placed on consumers, whereas in Europe, the burden is on private entities.

DATA TRANSFERS, THE SAFE HARBOR FRAMEWORK AND STANDARD CONTRACTUAL CLAUSES

Only two years after the establishment of the EU, Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the predecessor of the GDPR) was adopted. The directive recognized that with the rise of technology, the personal data of EU residents could easily be transferred outside of the EU, where it could be subject to lesser standards of protection. To maintain protections overseas, the directive set strict limits on when the personal data could be transferred outside of Europe.

One of the permitted, commonly used, avenues for such transfers of data was by way of an "adequacy decision." An adequacy decision is a declaration by the EU Commission that a third-party country, or a mechanism enforced within a third-party country, ensures an adequate level of data protection, such that no additional safeguards are required for cross-border transfers. Developed over the course of two years, in 2000, the EU Commission granted an "adequacy decision" for a mechanism between the EU and U.S. called the EU-U.S. Safe Harbor Framework. This Safe Harbor agreement created a set of data protection principles that U.S. companies could voluntarily agree to incorporate into their business practices. The assumption was that these principles would sufficiently protect the privacy rights of EU residents. If a U.S. company chose to participate in the Safe Harbor Framework, it would need to self-certify to the U.S. Federal Trade Commission, and the FTC was responsible for oversight and enforcement. U.S. companies who chose not to participate in the Safe Harbor Framework needed to use other safeguards (e.g., the SCCs) to import data from Europe, as the "adequacy decision" was limited to the Safe Harbor Framework.

Another permitted, common avenue was by way of a contractual agreement between the EU data exporter and the non-EU data importer. This contract, however, ultimately requires approval by data authorities to assure adequacy. There are currently two standard contractual clauses, or SCCs, pre-approved by the European Commission, one for controller-controller transfers and one for controller-processor transfers. Today, countless transatlantic companies utilize these contractual safeguards to legally move data outside of the EU.

THE FALL OF SAFE HARBOR

After the September 11 terrorist attacks, privacy laws in the U.S. took a sharp turn. In 2001, the U.S. passed the Patriot Act, which greatly expanded government surveillance and investigatory powers. Then in 2007 and 2008, the Protect America Act and amendments to the Foreign Intelligence Surveillance Act were passed which expanded foreign intelligence surveillance powers and led to the infamous PRISM program. The PRISM program secretly allowed the National Security Agency to collect bulk communications traffic (e.g., emails, photos, messaging) of foreign persons, by compelling popular U.S.-based data tech giants, such as Facebook, Google, Microsoft, Apple and Skype, to provide the NSA with access to their servers. The PRISM program was exposed by Edward Snowden in 2013.

Europeans were alarmed by this invasion of privacy. Days after the Snowden disclosure, a European citizen named Max Schrems drafted a complaint to the Irish data protection commissioner asking for a review Facebook's compliance with the EUU. S. Safe Harbor Framework, as well as the EU Commission's previous "adequacy decision" for the EU-U.S. Safe Harbor Framework. The case was ultimately sent to the CJEU, which struck down Safe Harbor in 2015 in *Schrems I*. The CJEU concluded the Safe Harbor Framework did not adequately protect personal data from "interference" from the U.S. government, because the new foreign surveillance laws in the U.S. did not limit data collection practices to what was "strictly necessary" or proportional, and did not offer adequate redress to EU resident's whose rights were violated. The CJEU found that the Safe Harbor Framework failed to comply with the Directive 95/46/EC's requirements and therefore was invalid.

This was devastating to companies who relied on the Safe Harbor Framework. Companies were sent into a panic as they sought out alternate methods for data transfers including use of the Standard Contract Clauses and the less common, Binding Corporate Rules mechanism. BCRs are internal data protection policies developed using EU standards for data protection and must be adhered to by all global operations within the company. Companies must submit their BCRs to EU authorities for approval. This can be a lengthy and costly option, and one which most companies were not able to secure.

Less than a year after the fall of Safe Harbor, the EU Commission approved the EU-U.S. Privacy Shield Framework in its 2016 "adequacy decision." The Privacy Shield, while similar to its predecessor, required additional disclosures to be made within the U.S. data importer's privacy policy, enhanced obligations with respect to third-party sharing of EU personal data by the U.S. data importer, and provided additional enforcement mechanism provisions, among other things.

THE GDPR, PRIVACY SHIELD AND SCHREMS II

Following the invalidation of Safe Har-

bor, Facebook still relied on the SCCs for cross-border transfer compliance. In 2015, Schrems filed a reformulated complaint challenging the adequacy of Facebook's reliance on the SCCs and alleging that even with the SCCs in place, the U.S. does not provide for sufficient protections against U.S. government access, nor does it provide recourse for EU residents to ensure preservation of their data rights.

Separately, in 2016, the EU replaced Directive 95/46/EC with the General Data Protection Regulation, which was intended to update and harmonize data protection law across the member states. One update pertained to the qualifying factors for an "adequacy decision." These updated factors included key questions such as, "what are the effective administrative and judicial redress mechanisms for EU data subjects whose personal data has been transferred?" and "what is the respect for human rights and fundamental freedoms [in the destination country], and how does such rule of law address public security, defense, national security and criminal law with respect to public authority access to personal data?"

With these new factors in place in addition to the new overall GDPR requirements, using Schrems' 2015 complaint, the Irish data protection commissioner brought proceedings before the Irish High Court. After exhausting its own proceedings, in 2018 the High Court referred several questions to the CJEU including whether it still agreed with in the adequacy of: (i) the current controller- processor SCCs, and (ii) the commission's previous "adequacy decision" from 2016, regarding the EU-US Privacy Shield Framework. *Schrems II*.

On July 16, 2020, the CJEU announced its decision in *Schrems II*, that while the SCCs remain adequate and valid (for now), the Privacy Shield does not. The CJEU declared that EU residents, even when their data is located in other countries, "*must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter*."

INVALIDATING THE PRIVACY SHIELD

Because Articles 7 and 8 of the EU Charter of Fundamental Rights provide that privacy is a fundamental right, the very act of collecting, retaining, using or sharing data with third-parties constitutes interference with this right. However, the EU recognizes that this right cannot be absolute in the normal course of society. As such, interferences with this right are allowed, but must be provided for by law, definite in scope, and strictly necessary to meet objectives of general interest recognized by the EU (i.e., principles of necessity and proportionality). Laws that interfere with this privacy right, in addition to the foregoing, must impose minimum safeguards therein, so that EU residents have sufficient guarantees of protection against the risk of abuse (i.e., redress). These safeguards are particularly important when data is subject to automated processing.

The *Schrems II* decision primarily focused on two issues: (1) the lack of necessity and proportionality in U.S. surveillance laws and (2) the lack of access to judicial redress and remedy. The decision concentrated on two foreign surveillance laws in the U.S.: Section 702 of the FISA and Executive Order 12333. Section 702 allows the U.S. government to conduct targeted surveillance of foreign persons, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information. Executive Order 12333 is a presidential order which creates broad foreign surveillance authority for the intelligence community. The Irish High Court argued that these laws do not require necessity, proportionality or redress, and thus, the U.S. could not ensure an adequate level of protection for personal data essentially equivalent to that guaranteed in the EU.

The U.S. Foreign Intelligence Surveillance Court was established and authorized under the FISA to oversee requests for surveillance warrants against foreign persons by federal law enforcement and intelligence agencies. However, the FISC does not authorize, have oversight, or otherwise control individual foreign surveillance orders under Section 702. Rather, the attorney general and director of National Intelligence can authorize targeted surveillance of foreign persons, without FISC approval. The FISC's role under Section 702 is limited to the authorization of surveillance programs (e.g., PRISM). Such authorization largely hinges on whether the program's procedures risk violation of U.S. residents' rights. Thus, the supervisory authority of Section 702 does not place limitations on the power it confers to surveillance programs of non-U.S. persons, does not provide for guaranteed protections for targeted non-U.S. persons, and does not grant EU residents actionable rights before the courts against the U.S. authorities.

The Privacy Shield Framework included the creation of the office of the Privacy Shield ombudsperson — to enforce compliance over the intelligence community. This ombudsperson would answer directly to the secretary of state and be wholly independent from the intelligence community. However, to meet the standards of the Charter of Fundamental Rights, EU residents must have the ability to bring a legal action before an independent and impartial court. The court argued that an ombudsperson is not a tribunal within the meaning of Article 47 of the charter and does not have the power to adopt decisions that are binding on the intelligence community. Furthermore, the court questioned the ombudsperson's impartiality, as there was no mention of appointment safeguards. Interestingly, the court did not mention the Judicial Redress Act of 2015, which extends select rights to citizens of certain foreign countries or regional economic organizations, including the EU.

Given the above, the court determined that under the Privacy Shield, potential access to and use of EU personal data by U.S. public authorities was not circumscribed in a way that satisfied requirements that are essentially equivalent to those required under EU law.

IMPLICATIONS FOR THE SCCS

Schrems II confirmed the validity of the SCCs, although, they did not emerge unscathed. The court looked to whether the SCCs could still be effective in guaranteeing compliance with the level of protection required by EU law. The court found that the SCCs impose an obligation on data exporters and data importers to first verify, prior to any transfer, whether that requisite level of protection is respected in the destination country. They also require the data importers to inform the data exporters of any inability to comply with the SCCs (i.e., such requisite level), and obligate the data exporters (and permit the EU data protection authority) to then suspend the transfer of data and/or terminate the overarching contract with the data importers. Thus, the court determined that the SCCs include sufficient safeguard mechanisms to guarantee a level of protection essentially equivalent to that guaranteed within the EU.

However, the court's Privacy Shield analysis — in particular, regarding Section 702's ability to compel an electronic communications service provider to immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition of foreign intelligence information — may have an impact on the SCCs. In this scenario, an electronic communication service provider may not be able to comply with its obligations under the SSCs, and would have to notify the data exporter, who would then be obligated to cease further data transfers outside of the EU. U.S. businesses may be left to pick up the tab for government surveillance programs.

Business using the SCCs must now comply with a heightened awareness of their obligations. Data importers using the SCCs as their legal basis for transferring data outside of the EU, must ensure that EU residents are afforded a level of protection essentially equivalent to that guaranteed within the EU. If they cannot, for example, due to government or other interference without adequate redress, then the data importers may essentially be required to cancel their commercial agreements with data exporters. This could have a significant impact on transatlantic trade.

WHAT'S NEXT?

Complying with privacy laws is certainly not an easy or uncomplicated feat. The fall of the Privacy Shield feels less shocking to those of us who watched the rise and fall of Safe Harbor. Once again, however, we are left attempting to determine how to best guide companies on what comes next.

While the Department of Commerce has indicated that it will "continue to administer the Privacy Shield program," companies that relied on the Privacy Shield Framework will have to implement an alternate data transfer mechanism permitted under the GDPR. The SCCs are the most common and efficient option, however, with the recent *Schrems II* decision, businesses are reminded that the SCCs cannot be simply signed and incorporated into larger commercial agreements, they must be properly reviewed and executed in compliance with EU laws. Other options currently available include BCRs, approved codes of conduct, certification, and approved ad hoc clauses.

A larger, darker cloud looms overhead though. Very broadly, the EU believes activities must be limited to that which is "strictly necessary." The U.S. generally requires a different standard, that which is "as tailored as feasible." At their core, these are different standards. The creation of any new data transfer mechanism (Safe Harbor 3?) then requires a paradigm shift, or at least a shift in language. Otherwise, each reincarnation is ripe for challenge and potential invalidity. ■

Heather A. Antoine is a partner and **Mallory Petroli** is an associate at Stubbs Alderton & Markiles, LLP.