C·T·L·R

THE JOURNAL OF E-COMMERCE, TECHNOLOGY AND COMMUNICATIONS

ISSUE 1 2016

SWEET & MAXWELL

The US-EU Safe Harbor Framework is Invalid: Now What?

Rohan Massey*

Heather Egan Sussman**

Adequate level of protection; Data protection; EU law; Investigatory powers; Safe harbour; Transborder data flows; United States

A confluence of events has tested the strength of the Safe Harbor Framework and, for now, it is no longer a port in the storm. Most recently, on October 6, 2015, the Court of Justice of the EU (CJEU) invalidated the Safe Harbor Framework in *Schrems v Data Protection Commissioner* (C-362/14),[1] concluding that the European Commission exceeded its authority by approving the Safe Harbor Framework in 2000. As predicted, the CJEU's decision followed the recent non-binding Opinion of the EU's Advocate General, who argued that the Framework "must be declared invalid".[2] The decision also comes in the midst of negotiations between the US and the EU that have been ongoing since 2014, after the European Commission released recommendations for improving the Safe Harbor Framework following widespread media reports of US surveillance activities.

Thousands of corporations that rely on the Safe Harbor to legitimise transfers of personal data from Europe to the US are left wondering how to make sense of these events and what the pathway forward is. While the European Commission has promised guidance, some local data protection authorities (DPAs) in EU Member States have released statements urging companies to "stay calm" and take a pragmatic approach. This article provides an overview of where this decision brings us today, and where companies can go from here.

Background on the Safe Harbor

Originally established in 2000 by agreement between the US and the EU, the Safe Harbor Framework (Framework) was designed to facilitate the open flow of data from the EU to the US. The agreement was necessary because, five years earlier, the EU had adopted Directive 95/46 (Directive), establishing the European "adequacy" standard for privacy protection. The Directive prohibits, among other things, the transfer of personal data gathered within the EU for commercial purposes to locations outside the EU, unless such locations demonstrate an "adequate" level of data protection commensurate with EU standards. "Personal data" is defined broadly under the Directive "to include any information relating to an identified or identifiable natural person", meaning that even relatively mundane information such as payroll and company phone books can be considered personal data.

To this day, the EU does not recognise the US as providing an adequate level of protection for personal data, and thus transfers of personal data from the EU to the US generally are prohibited unless the organisation takes approved steps to legalise (also called "legitimise") the transfers. Up until the CJEU's 6 October 2015, decision, one such approved step was self-certification to the Framework.

The Safe Harbor Framework and Principles

At its core, the Framework is a self-regulatory regime whereby US organisations could self-certify their compliance with seven Safe Harbor Privacy Principles (Principles), including the principles of notice, choice, security and enforcement.[3] After undertaking this self-certification, the US organisation enjoyed a binding presumption of "adequacy", and the organisation could lawfully transfer personal data from the EU to the US pursuant to the certification.

Given the Directive's broad definition of personal data, many companies that must send data from the EU to the US (including EU companies that use servers located in the US) chose to rely on the Safe Harbor for their everyday operations and free flow of data across jurisdictional lines. In the 15 years since the Framework was established to facilitate the transfer of personal data between the US and EU, the number of participating organisations steadily increased from under 1,000 in 2005 to around 3,200 in 2013 and roughly 5,500 today.

Enforcement

Approved by the European Commission in Decision 2000/520, the Framework is administered by the US Department of Commerce. The US Federal Trade Commission (FTC) oversees enforcement.[4] The FTC has the ability to investigate, file actions against and enter into settlement agreements with organisations that misrepresent their compliance. Such misrepresentations can be charged under s.5 of the FTC Act as unfair and deceptive practices, and subject the offending organisation to fines, penalties and a multi-year consent decree.

Neither the FTC nor its European counterpart DPAs actively police Framework organisations by conducting audits or other regular review of such organisations'

* Partner, Ropes & Gray (London).
** Partner Ropes & Gray (Boston).

[1] *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650.
[2] Opinion of A.G. Bot in *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:627 at [183].
[3] The remaining pillars are onward transfer, access and security. The Principles mirror the privacy principles embodied in the Directive.
[4] Despite the CJEU decision, the US's administration of its portion of the system remains intact. Whether and to what extent it will continue to operate remains to be seen.

practices. However, from 2000 to 2013, the FTC initiated 10 enforcement actions involving the Safe Harbor Framework. The DPAs also were meant to serve a policing function by receiving complaints, investigating and acting on them and referring them to the FTC. The DPA dispute resolution mechanism was never widely adopted, however, and very few complaints were ever filed.

Despite corporate transgressions resulting in FTC enforcement action, our experience with the many organisations we have helped self-certify to the Safe Harbor Framework over the years is that these organisations take a thoughtful approach to developing an internal privacy and data protection programme that is designed to meet the Safe Harbor Principles and achieve the letter and spirit of the Framework. Corporate officers who complete the self-certification must sign under the pains and penalties of perjury that the company has undertaken such an approach. Since 2000, the net result of the Safe Harbor Framework has been that *thousands* of US companies have developed robust privacy and data protection programmes governing the treatment of personal data—and enhancing privacy protections—in line with EU law.

Impact of US intelligence activities

Criticism of the Framework took on a fevered pitch in June 2013, when a former contractor working for the federal government leaked thousands of classified US National Security Agency (NSA) documents to the press. These documents revealed information about the NSA's intelligence activities through which the Government gained access to personal data of US and non-US citizens held by private corporations in the US. The Framework contains a provision allowing for disclosures of personal data in instances of national security, public interest or law enforcement requirements. Some in Europe argued, however, that the NSA's exploitation of this loophole was far beyond what was necessary or proportionate to the risk—and did not afford EU citizens the right to challenge these activities—thus further contravening fundamental privacy protections afforded under EU law.

In the wake of these criticisms, the FTC increased its Framework enforcement activities.[3] Despite increased FTC engagement, the EU remained dissatisfied with the Framework and, in November 2013, the European Commission issued a report listing 13 recommendations for the US to follow in order to restore the EU's trust in this system. The recommendations related to six areas and included requiring public disclosure of privacy policies, publication of privacy conditions of sub-contractor contracts, audits and investigations of a set percentage of organisations claiming compliance, and publication of the extent to which public authorities can access and process personal data about EU citizens.[5] The Commission's report explicitly stated the need to address the "deep concerns about revelations of large-scale U.S. intelligence collection", and to that end the report included a recommendation that the national security exception, which had been so heavily exploited by the NSA, be used "only to an extent that is strictly necessary or proportionate". The Commission gave the US until the summer of 2014 to identify remedies and implement the recommendations.

Negotiations ensue

In 2014, the US and EU began negotiations regarding the Commission's 2013 recommendations, but these conversations quickly stalled because of a deadlock between the two on a separate, but related, matter. Namely, beginning in 2009, the US and EU began exploring what they dubbed the "Umbrella Agreement" to address the need for transatlantic data-sharing co-operation related to criminal and terrorism investigations. Talks on the Umbrella Agreement broke down, however, over the US refusal to allow EU citizens to seek redress in US courts for information that is mishandled or unlawfully disclosed. The NSA surveillance scandal also had profound effects on these negotiations and, by 2014, an agreement still had not been reached. Because of the importance to the EU of closing or narrowing the Framework's national security loophole, the parallel talks on Safe Harbor reform were complicated by the deadlocked Umbrella Agreement.

In March 2015, however, Congress passed a Bill extending judicial redress provisions under US law to EU citizens. Following that, talks resumed, and on 8 September 2015 the European Commission announced that the EU and US had finalised an arrangement that would provide for heightened data protection standards for data transferred between the EU and US for the purposes of law enforcement co-operation.

Private litigant challenges validity of the Safe Harbor

Unfortunately, the Umbrella Agreement was not the only hurdle facing the Framework. Since 2012, the Austrian privacy advocate Max Schrems had aggressively campaigned against Facebook, claiming that by transferring users' personal data to the US and disclosing the same to the US authorities, Facebook's privacy policies and practices showed a disregard for European privacy law. Mr Schrems initially filed a complaint with the Irish Data Protection Commissioner, as Facebook's European operations are based in Ireland. He argued that US law

[5] In 2013, the FTC began initiating enforcement actions, and by January 2014, the FTC announced settlement agreements with 13 companies, as compared with only 10 enforcements actions over the previous 13 years. In the first eight months of 2015, the FTC settled with an additional 15 companies.

> "did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities",[6]

referring to NSA intelligence activities as reported in the media. The Irish Commissioner dismissed the complaint, concluding that because the transfers were made under the EU Commission-approved Safe Harbor, the Irish Commissioner did not have standing to overrule.

Mr Schrems' group, Europe v Facebook, appealed to the Irish High Court. After an initial hearing on the case, the High Court certified two questions to the CJEU asking whether Facebook's actions, in particular its participation in the NSA's PRISM programme, were compatible with the Framework, and whether the Framework was "functioning as intended".

The Advocate General's Opinion

On September 23, 2015, the EU Advocate General published his advisory Opinion on the two questions certified. The AG noted that while

> "electronic surveillance and interception of personal data serve necessary and indispensable objectives in the public interest, namely the preservation of national security and the prevention of serious crime"[7]

and thus "serve legitimate counter-terrorism objectives", documents evidencing NSA activities leaked to the press "demonstrated a significant over-reach on the part of the NSA and other similar agencies".[8] And because these activities happen in secret, affected EU citizens have no right to challenge these activities in court.

The Safe Harbor Framework permits limited adherence to the principles "to the extent necessary to meet national security, public interest, or law enforcement requirements". However, the Advocate General concluded that

> "the law and practice of the United States allow the large-scale collection of the personal data of citizens of the [EU] which is transferred under the safe harbour scheme, without those citizens benefiting from effective judicial protection".[9]

The Advocate General concluded that the

> "access of the [US] intelligence services to the data transferred covers, in a comprehensive manner, all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security".[10]

"Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights"[11] afforded under EU law. The Advocate General opined that the "national security" limitation

> "ought to have been accompanied by the putting in place of an independent control mechanism suitable for preventing the breaches of the right to privacy that have been found"[12]

and a requirement that the surveillance be strictly necessary, but they were not.

For all of these reasons, the Advocate General recommended that the CJEU invalidate Commission Decision 2000/520 and declare the Safe Harbor invalid.

Notably, the Advocate General does not independently establish the fact of this alleged "mass, indiscriminate surveillance" in the body of his Opinion. Rather, he relies on purported submissions to and findings of the Irish High Court. He also pointed to statements made by the European Commission itself during the post-Snowden fallout, and the Advocate General appears to roundly criticise the Commission for acknowledging deficiencies in the Safe Harbor Framework in 2013 and undertaking negotiations with the US in 2014, without also suspending the programme.

The US responds, but the message is ignored

Shortly after the Advocate General released his Opinion, the US Mission to the European Commission released a statement applauding the continued efforts of the Commission and the US Government to reach a negotiated result. The Mission pointed out legal flaws and factual inaccuracies in the Advocate General's Opinion that went to the very heart of the Advocate General's analysis.

The Advocate General's Opinion notes that it was required to accept the facts (of mass, indiscriminate surveillance) as found by the Irish High Court. There was, however, no actual fact-finding in this case; instead, the Irish High Court concluded, on the basis of exhibits to the plaintiff's affidavits, that the accuracy of his allegations regarding US intelligence practices "is not in dispute". But that is simply not the case, as the public record made clear at the time, and as has been made even clearer in the subsequent two years.

The US does not engage and has not engaged in indiscriminate surveillance of anyone, including ordinary European citizens. The PRISM programme that the Advocate General's Opinion discusses is in fact aimed against particular valid foreign intelligence targets, is

[6] *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650 at [28].
[7] Opinion of A.G. Bot in *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:627 at [34].
[8] Opinion of A.G. Bot in *Schrems* EU:C:2015:627 at [35].
[9] Opinion of A.G. Bot in *Schrems* EU:C:2015:627 at [158].
[10] Opinion of A.G. Bot in *Schrems* EU:C:2015:627 at [199].
[11] Opinion of A.G. Bot in *Schrems* EU:C:2015:627 at [200].
[12] Opinion of A.G. Bot in *Schrems* EU:C:2015:627 at [166].

duly authorised by law, and strictly complies with a number of publicly disclosed controls and limitations. Moreover, the Advocate General's Opinion fails to take into account that—particularly in the last two years—President Obama has taken unprecedented steps to enhance transparency and public accountability regarding US intelligence practices, and to strengthen policies to ensure that all persons are treated with dignity and respect, regardless of their nationality or place of residence.

The statement received little attention.

The CJEU follows the Advocate General's Opinion

Despite the flaws and inaccuracies of the Advocate General's Opinion, on 6 October 2015 the CJEU handed down a judgment that adopted the Advocate General's line of reasoning. The CJEU ruled that the Commission had exceeded its authority in adopting Decision 2000/520, because it contained "national security" derogations without necessary corresponding protections required by EU law. In addition the CJEU found that in denying the national supervisory authorities complete independence to enforce the data protection regime following a claim by an individual, the Commission over-extended itself in adopting Decision 2000/520. The fact that these two issues could not be separated from the other provisions of Decision 2000/520 meant that the entire Decision and therefore the Safe Harbor Framework was invalid. The CJEU made this finding with immediate effect.

Where we go from here

On the same date as the CJEU's decision, the European Commission took a reassuring tone, making public statements that it was confident negotiations over Safe Harbor reform would succeed in the coming months. Similarly, the EU's new General Data Protection Regulation is currently nearing its final form and should shed light on acceptable mechanisms to transfer personal data from the EU to the US.

As when the Framework was first adopted in 2000, we expect that there will be some form of a grace period that will allow companies to make needed changes. Some DPAs, such as the UK's Information Commissioner's Office, have released statements urging a pragmatic approach. Reportedly, the European Commission's data protection advisory body, the Article 29 Working Party, is convening a special session to discuss the Decision and provide direction.

In the meantime, companies that self-certified under the Safe Harbor Framework should analyse which of their current personal data transfers from the EU to the US rely on the Framework and undertake an analysis of whether these personal data transfers could take place under an alternative legal basis. Possible alternatives may include:

- using the Commission's model contractual clauses or ad hoc agreements or intra-group agreements;
- establishing "binding corporate rules" that permit transfers of personal data within a multinational corporation or international organisation; and
- obtaining the "unambiguous consent" of the data subject to the transfer of personal data.

Each company then will need to perform a second layer of analysis to identify any third parties that receive personal data of EU citizens from the company once in the US (under an "onward transfer" agreement, for example), because these transfers will need to be addressed using an approved method outside of the Safe Harbor Framework.

For companies self-certified under the Safe Harbor Framework that are themselves acting as service providers (data processors) to corporate affiliates or clients (data controllers) where the corporate clients have been relying on the service provider's self-certification to legitimatise the transfers of personal data to the US, these transfers also will need to be addressed, using one of the possible alternatives identified above.

Companies that are not yet self-certified under the Framework but that were considering undertaking such certification should analyse the feasibility of relying on one or more of these possible alternative mechanisms of transfer. Because each legal basis for transfer of personal data from the EU to the US requires adhering to specific requirements, companies should not underestimate the amount of time required for such analyses.