BRADLEY JOSLOVE

Transatlantic data flow:

Some progress but...

Like all who transfer personal data to the United States, or who provide advice on such transfers, Bradley Joslove, a lawyer admitted to the Bars of Paris and Washington, D.C., welcomes the agreement between Joe Biden and Ursula von der Leyen for a European Commission adequacy decision aimed at regularising transfers of personal data from the European Union to the United States, probably by next summer. According to Mr. Joslove, the Americans have made a real effort to ensure that the future Privacy Framework complies with the GDPR and is not invalidated by the Court of Justice of the European Union in the event of a more than likely appeal by Max Schrems. With his Franco-American perspective, which sheds a light on our cultural differences and differing attitudes to these issues, he shares his insight on this new framework, which he hopes will be approved by the European authorities. Time will tell.

Sylvie Rozenfeld: On 13 December, the European Commission announced that it had officially started the approval process for the Transatlantic Data Protection Framework. Back in March 2022, Joe Biden obtained an agreement in principle from Ursula Von der Leyen on the resolution of this legal dispute, which has been ongoing since 2013, when Edward Snowden revealed America's extensive surveillance programmes. In October, the President of the United States signed an executive order, after several months of consultation with the European Commission. Now we have to wait for the advisory opinion of the European Data Protection Board (EDPB), the position of the European Parliament and of the Member States. The Commission is expected to publish its decision next spring.
Bradley Joslove, you are a lawyer admitted to the Paris and Washington bars and a partner at Bersay. As someone who advises French and American companies, do you welcome this agreement?

Bradley Joslove: This agreement is fundamental, but the adequacy decision still needs to be adopted. Since the invalidation of the European Commission's adequacy decision by the Court of Justice of the European Union (CJEU) on 16 July 2020, all EU and US companies making data transfers to the United States have been in an extremely uncomfortable situation, as they must find a legal basis other than the Privacy Shield to legitimise such transfers. They also have to demonstrate that the personal data transferred will benefit from a level of protection equivalent to that provided by the European Union. If this is not the case, and this is the argument adopted by the CJEU's decision, the parties to the transfer must put in place additional safeguards to make up for this lack of adequacy in terms of protection. This decision creates a real economic problem for SMEs that want to transfer personal data to the United States. Demonstrating this level of protection requires a very detailed study of the US legal system, including the ability of US intelligence agencies to access data.

"This is the first time in my career that I've had to tell my clients that I cannot guarantee the proposed solution."

This study is complex and expensive, especially for small businesses offering cloud services. Even if a company carries out this study, it cannot be sure that it is sufficient, as it is a self-certification. This generates significant costs and much legal uncertainty.

It has made it difficult for companies to do business, but the data has continued to flow. Well, not always. In addition to these complex procedures, in some cases it is impossible to find an additional measure of protection. For example, a US cloud provider can no longer offer a French company a service that requires the US provider to have access to clear data. The European Data Protection Board (EDPB) considers that there is no way to prevent the US intelligence services from having access to these data. This is the first time in my career that I've had to tell my clients that I cannot guarantee the proposed solution, while nonetheless giving the best possible arguments, and advising them to try not to draw the attention of the supervisory authorities. When I talk to my colleagues working in the same sector, they make the same observation.

Let's turn to the proposed adequacy decision. The 134-page draft text does not make any fundamental changes but follows on from the Safe Harbor invalidated by the CJEU in 2015 and the Privacy Shield invalidated by the same Court in 2020. US companies will be able to benefit from the adequacy mechanism by committing to a set of data protection obligations without, however, being required to comply with the GDPR. Furthermore, laws with extraterritorial provisions such as the FISA or Executive Order 12333, which allow intelligence agencies to collect and process data on a massive scale, including data relating to European residents, will continue to apply. Max Schrems, who initiated the latest appeal to the CJEU, said: "As the draft decision is based on the now famous Executive Order, I do not see how it could survive a challenge in the Court of Justice."

It seems that the European Commission is simply issuing similar decisions over and over again – in clear violation of our fundamental rights.

Do you think this agreement makes a real change or is it just a cosmetic adjustment?

I see it as lying somewhere in between. Max Schrems and certain others want US intelligence agencies to stop mass surveillance. This is simply not possible for the US administration, for national security reasons. In fact, many American citizens share this view. In this respect, it is important to understand that there are significant cultural differences between the United States and Europe. I am of American origin and have been living in France for over 30 years, so I represent a mix of both cultures. I'm from both countries but also between the two. When it comes to personal data, I've seen these cultural differences and differing attitudes between the Americans and the Europeans. Each guarantees a set of fundamental rights that are broadly similar. It is when these fundamental rights come into conflict that we best perceive these differences. For example, Americans are very attached to freedom of speech, almost unconditionally so. When there is a trade-off between freedom of speech and other rights, the former usually takes precedence. This is less the case in France where, for example, denying crimes against humanity and racial hatred are prohibited. These are restrictions on free speech that would be invalidated in the United States because of the very American cultural belief in the primacy of that freedom. On the European side, it seems to me that the right to protection of personal data is considered to be a little more fundamental than some other rights, as we have seen with the CJEU's Google Spain ruling in 2014, which created the right to be forgotten. In fact, this ruling was reinforced last month by a new CJEU ruling involving Google and the right to be forgotten.

In balancing the right to privacy against the state's responsibility to protect its citizens from terrorist threats, Europeans place the cursor more on the side of the right to privacy than Americans would. On the other hand, it seems to me that Max Schrems goes a little too far when he argues that mass data collection by the US intelligence services could not under any circumstances be accepted by the CJEU, no matter the array of limitations and protections that could temper that collection.

"This is a marked improvement on the Ombudsman, but the biggest difference from the previous system is the possibility of appealing CLPO decisions to the Data Protection Review Court."

I don't know whether the protections contained in the Transatlantic Data Protection Framework go far enough to satisfy the judges of the CJEU, but I don't rule it out.

There is also a right to privacy in the United States.

Yes, it's a constitutional right enshrined by the US Supreme Court, but a right reserved for US citizens. This is an important issue in the current dispute because this right does not protect foreigners, and mass data collection relates only to the data of foreigners and is implemented outside the United States.

Would you say that the personal data protection system in the United States is less protective than the European system or that it's different?

Both: the system is different, and for Americans it's less protective than the one that exists in Europe. With the Privacy Shield or the future Privacy Framework, Europeans whose personal data is sent to US companies will benefit from a higher level of protection than that granted to Americans, broadly equivalent to that which they would have benefited from in Europe.

Now let's take a closer look at the content. One of the weaknesses of the Privacy Shield identified by the CJEU was the lack of an effective remedy for European citizens. Article 47 of the Charter of Fundamental Rights requires access to a judicial remedy. Under the draft decision, in order to obtain redress for the collection and use of their data by US intelligence agencies, plaintiffs will have to apply to the EU national authorities, which will then apply to the US government. A Civil Liberties Protection Officer (CLPO), reporting to the Office of the Director of National Intelligence, would be responsible for checking complaints about violations of the new executive order.

Provisions are made for appeals to the Data Protection Review Court, which is part of the US executive branch.
This officer would therefore work within the Office of the Director of National Intelligence. What about the officer's independence? Isn't this just a slightly improved version of the Ombudsman, rejected by the CJEU? What guarantees of independence are there for this court? Can this be considered a judicial remedy within the meaning of the Charter?
I think there's a significant difference between the Ombudsman and the new two-tier system. At the first level, the Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence effectively reports to the intelligence services. If there were no other protections and controls, I would say the system wouldn't be very different from the previous one. However, the CLPO has protections against the influence of the intelligence services: he or she cannot be dismissed, except for serious and limited reasons. The CLPO makes binding decisions, which was not the case previously, and can order the deletion of illegally collected data. It should be understood that his or her sole function is to protect personal data. This is a marked improvement on the Ombudsman, but the biggest difference from the previous system is the possibility of appealing CLPO decisions to the Data Protection Review Court. In my opinion, this is a real court created by the Justice Department and has nothing to do with the intelligence services. Real judges will sit on it, who must be lawyers with experience in personal data protection and national security laws. However, there is no recourse to a federal court of appeal or to the US Supreme Court, which is unfortunate.

"Given this principle and the US Supreme Court's case law on standing, the establishment of a 'real court' within the judicial branch, as Max Schrems demands, would be ineffective."

How can we be aware that our data has been collected by intelligence agencies?
It is also to solve this difficulty that this court was established within the administration. In order to bring an action before a traditional court, the plaintiff must demonstrate "injury in fact", which requires proof of harm.

If you can't prove that your personal data have been collected, you can't demonstrate harm. Given this principle and the US Supreme Court's case law on standing, the establishment of a "*real court*" within the judicial branch, as Max Schrems demands, would be ineffective. The new arrangement makes it easier for anyone to challenge this data collection without having to prove injury in fact. The system is indirect, like in France, with indirect access to government files through the CNIL (the French Commission for Information Technology and Civil Liberties). Let me give you a personal example. My wife is French, my children have dual nationality, and we travel often in the United States. For several years, my wife and children were systematically searched at all US airports as if they were suspected terrorists. I thought maybe the intelligence services, as a result of their surveillance activities, had put my family in a kind of "*S file*" [Nota: a file on suspected terrorists maintained by the French authorities]. I had no direct evidence, but the circumstances suggested it. I wrote to a certain US agency and didn't receive an answer but after that my family was never searched again.

How will the appeal be triggered?
Individuals who have indirect evidence that they have been subject to surveillance will refer the matter to the supervisory authority, the CNIL in France, which will contact the CLPO. The CLPO will carry out an investigation, the result of which will be communicated to the CNIL, stating either that the investigation has not identified any violations or that the CLPO has ordered that appropriate measures be taken, without giving details and without admitting or denying that the concerned person has been the subject of surveillance. The concerned person has the right to appeal against the decisions of the CLPO to the Data Protection Review Court which I have already mentioned.

The CJEU has required that US surveillance be "*proportionate*" within the meaning of Article 52 of the Charter of Fundamental Rights (CFR). The US executive order refers to "*necessary*" and "*proportionate"* surveillance. What is the US definition of "*necessary*" and "*proportionate"?*
Time will tell. As far as I know, there is no case law in the United States on this subject because these are not terms enshrined in American law.

In the US, we have the concept of "*reasonableness*". The European terms have been adopted. It remains to see how they will be interpreted in practice.

But the decisions are not public.

A number of bodies oversee intelligence agencies, some of which already existed before the executive order. In addition to the CLPO, there is the Privacy and Civil Liberties Oversight Board (PCLOB) and the Foreign Intelligence Surveillance Court (FISC), which produce reports for Congress and the public. It should be noted that the Snowden revelations also shocked the Americans and they have put in place several constraints on the intelligence services. At the EU level, the European Commission, like the EDPB, has a right of scrutiny. It will be able to review its adequacy decision after one year.

"The Transatlantic Framework represents a real effort to make the US system equivalent with regard to the processing of Europeans' personal data."

Some limitations and safeguards on access to data by US public authorities are planned, what do they consist in?

the principles in the Transatlantic Data Protection Framework are similar to those contained in the GDPR: a certain transparency, minimisation of data collection, limitation of duration of retention of data, a legal basis for processing, etc. Two lists have been created: one for data collection based on permitted national interest purposes and one for purposes that are not permitted. In the United States, for example, data collection by intelligence agencies for industrial espionage is prohibited, which does not appear to be the case in France.

Finally, is there any legal compatibility between the GDPR and the Cloud Act or FISA?

I believe there is. But you should first understand that the Cloud Act and the FISA Act are different. The Cloud Act is not about access to personal data by US intelligence agencies but by federal and/or local courts. Moreover, it was not mentioned in the Schrems II judgement. Sooner or later, a consensus will be reached. Economic trade between the United States and Europe represents more than €7 trillion, which requires a huge amount of data exchanges, including personal data. It is inconceivable to stop these exchanges, so we have no choice but to find a solution. Today, the adequacy decision is still at the draft stage. The EDPB must issue an opinion that is only advisory. The real decision will be taken by the Committee of Representatives of the Member States by a qualified majority. This decision is expected by the end of summer 2023. Parliament does not have a direct role.

It is practically certain that if the adequacy decision is approved, Max Schrems will lodge an appeal against this agreement, which will end up before the CJEU. I think the Transatlantic Framework represents a real effort to make the US system equivalent as concerns the processing of Europeans' personal data, but ultimately the CJEU will have the final word.

Interview by

Sylvie Rozenfeld