# Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution

Washington, 16 November 2015

Thank you Mr Kerry for your kind words of introduction.

It's a great pleasure for me to speak at Brookings this morning on the very topical issue of transatlantic data flows.

Ladies and Gentlemen,

Allow me to begin with a few words about the tragic events that took place in Paris on Friday the 13th.

These brutal attacks – killing from what we know now 129 people – were an attack against our freedoms, our way of life, and our values of tolerance and peaceful coexistence.

It is precisely these values that we will defend. We shall not be guided by fear and we must not let the attackers disrupt our lives. Instead we shall be resolute in our response to terrorism and hatred.

Let me also take this opportunity to thank our American friends for their strong solidarity with the people of Paris in their hour of need.

Europe marked the events with a minute of silence this morning. Here in Washington, a vigil was held on Friday evening at Lafayette Square, attended by the French community and many Americans, including representatives of the President of the United States. And flags are at half-mast. We are grateful for this.

At the beginning of this year, Paris was already stunned by the attacks on the Charlie Hebdo newspaper and a kosher supermarket.

The European Union responded by setting out a new **European Agenda on Security** to strengthen cooperation between the police and criminal justice authorities of European countries, and by reaffirming our values.

Last Friday's events sadly remind us how relevant and urgent the implementation of this agenda is.

As Justice Commissioner, I have put a focus on two issues:

o One is to actively promote **tolerance and respect**, and to fight discrimination in our societies. In October, we held a high-level event dedicated to fighting both anti-Semitism and anti-Muslim hatred. We agreed on a number of concrete actions to promote tolerance and respect, especially in the area of education.

o Another key concern is **radicalisation** of young people in some of our prisons, which must not become a "breeding ground" for terrorism. The European Union's Member States have varying levels of experience with this issue. Yet, they face a common challenge, with too many young Europeans joining the so-called "Islamic State" and traveling to Syria as "foreign fighters". That is why, last month, we gathered Justice Ministers and experts from around Europe to exchange the latest expertise in the area of preventing radicalisation and de-radicalisation in the criminal justice system.

Another key element of our European Agenda on Security is enhancing criminal justice cooperationboth within the EU and also with key allies: first and foremost the United States. This includes measures to confiscate assets or to effectively exchange relevant information, for example criminal records. Just a few hours before the attacks in Paris, my colleague Commissioner Avramopoulos and I were meeting the Attorney General and the Homeland Security Secretary for our regular dialogue on justice and home affairs matters. We reaffirmed the importance of our law enforcement cooperation, which serves to protect our citizens' security, as well as their freedoms.

Hence, coming back to our topic of **transatlantic data flows**, allow me to first underline that this is of utmost importance both for effective law enforcement and for our strong commercial relationship.

In fact, I see this field as a **"triangle"** betweenHence, coming back to our topic of **transatlantic data flows**, allow me to first underline that this is of utmost importance both for effective law enforcement and for our strong commercial relationship.

o the fundamental right to privacy and protection of personal data,

- our citizens' need for security, and
- our economic opportunities and business growth.

All these need to go hand in hand. We cannot have a trade-off between one and the other.

One of our main achievements in this area has been the negotiation on an **"umbrella" agreement** on privacy and data protection, which sets high standards of data protection for our law enforcement exchanges.

These exchanges rely on personal information, not only of suspects, but also victims and witnesses of crime.

This data is key for our law enforcement authorities.

But we must build structures so that this information can be treated by public authorities in a secure way and for specified purposes.

And people must have a right to access or correct their personal data, if a mistake has been made.

Europeans and Americans broadly agree on this, but our legal systems differ and the umbrella agreement builds an important bridge between the two.

The major difficulty we have faced over the years is the fact that the 1974 Privacy Act only grants rights to US citizens and residents, whereas in the EU there is no such limitation for US citizens in our redress system.

One of the essential elements of our agreement is therefore the **Judicial Redress Bill** that has recently been voted by the House. The Judicial Redress Bill would extend the rights US citizens and residents enjoy under the 1974 Privacy Act also to Europeans.

This is a long-awaited and historical step and we appreciate the efforts of the Administration and Congress so far. It would end a de facto discrimination.

We now await adoption of the Judicial Redress Bill by the Senate, and I look forward to discussing this with Senators on the Hill tomorrow.

* * *

For the remainder of my visit to Washington this week, my goal is to bring us closer to **finalising discussions on a new framework for commercial transfers of personal data**.

These discussions were launched already in early 2014, following the European Commission's recommendations to strengthen the Safe Harbour Framework as an answer to the NSA revelations.

I am in close contact with Commerce Secretary Penny Pritzker on this and will meet her again this afternoon, following another round of talks between out teams over the last couple of days.

The recent European Court of Justice ruling in the **Schrems case** has given a new importance and additional urgency to these discussions.

The ruling reaffirmed the fundamental right to protection of personal data, including where such data is transferred outside the European Union. We are guided in our discussions by the ruling.

Since the day of the ruling, my **immediate priority** has been:

- to reassure our citizens that their personal data is safe,
- to give clarity to businesses about remaining alternative possibilities for data transfer,
- and to ensure a uniform European enforcement of the ruling.

Together with Secretary Pritzker we have **stepped up discussions** on a renewed stronger framework to replace the old Safe Harbour which has been declared invalid by the Court.

I firmly believe that a new **comprehensive arrangement** for the transfer of personal data with strong safeguards and legal protections is the **best way** to achieve two things:

- One, effective protection of EU citizens' data protection rights when data is transferred, and
- Two, putting transatlantic commercial relations on a sound footing.

Alternative ways of transferring data are a short-term solution. With the current volume of transatlantic data transfers, it is clear that we need a comprehensive and effective framework in place **as soon as possible**. Only a comprehensive arrangement with clear legal commitments, enforced by the U.S. authorities, can ensure the level of data protection Europeans are entitled to under EU law. And this is what the judgment requires: where personal data travels, the protection has to travel with it.

This is why I'm here in Washington: to work together with our U.S. partners on a renewed transatlantic framework that will allow for continued data flows between Europe and the U.S. A renewed arrangement that will mean robust safeguards and legal certainty for citizens and businesses alike.

When I met business and industry representatives in Brussels they emphasized that they were looking for **guidance** on international data transfers following the ruling.

This is why on 6 November the Commission issued an explanatory Communication which provides an overview of alternative transfer tools, the conditions under which they can be used and their limitations.

During my visit to the United States, I am also **reaching out to business and civil society organisations** here in America, to hear their views and concerns.

What I would like to do this morning is:

- to dispel some myths and misunderstandings that followed the Schrems ruling, and,
- to explain and underscore what the European Commission now wants to achieve going forward.

Let me start with the **myths and misunderstandings**:

Firstly, there is a perception among our US interlocutors that the European Court of Justice made a judgement on the US legal system. Some have gone as far as expressing "disappointment" with our highest Court, because it did not describe the intelligence reforms undertaken by the United Since since the NSA revelations.

In fact, the Court did not attempt to describe the U.S. system. It rather set a general standard that has to be met by any country (including the US) for its data protection rules to be considered adequate under EU law.
The judgment does not require "an identical organization" of the U.S. legal system compared to the EU. But on data transfers,the U.S.has to offer safeguards which are "globally equivalent" to the ones we have in Europe. This is what our current discussions with the U.S. are about.

The Court says that a system based on 'self-certification' such as Safe Harbour is acceptable provided there are "effective detection and supervision mechanisms". This has indeed been one of the key points we have already highlighted in our 2013 Recommendations, especially in those regarding transparency, enforcement and redress. And here we can build on the work we have done together since January 2014. We are now in discussions on how to formalise these mechanism in a more binding way.

A second misunderstanding is based on the idea that there is now a fragmentation or "balkanisation" of international data transfers, governed by 28 data protection authorities.

First, the Commission as well as the 28 data protection authorities have stressed the need for uniform application of the ruling in the EU.

Second, the Court ruling does not call into question the Commission's power to take adequacy decisions, allowing for free flow of personal data from the EU to a third country.

Rather, it clarifies the possibilities and obligations for Data Protection Authorities to investigate complaints raised by individuals (such as that of Mr Schrems).

However, it is only the Court of Justice that can hold an adequacy decision to be invalid.

Let me now turn to our **negotiations with the U.S.**

Directly after the judgment, I was in contact with Commerce Secretary Pritzker to discuss the way forward.

And while we can **build on progress achieved** since the talks started in January 2014, the Commission swiftly came forward with **concrete proposals** for what is still needed now to meet the benchmark set by the Schrems ruling.

I have come to Washington to hear the reaction of the U.S.' side, and I trust that our American partners approach the issue with the same **sense of urgency**.

We must conclude the discussions with our U.S. counterparts on a renewed framework for transatlantic data flows with a higher level of protection.

This is important for transatlantic commercial relations and for effective protection our citizens' personal data.

Weneed to make sure that the newarrangementlives up to the **standardof the court ruling**.

In light of the Court's judgment we need more clarifications from our U.S. counterparts on a number of

points.

These discussions have not been easy, they are not easy, but they have **already yielded results**:

The U.S. has already committed to stronger oversight by the Department of Commerce, stronger cooperation between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as pro-active.

We are also working with the U.S. to put into place an annual joint review mechanism that will coverall aspects of the functioning of the new framework, including the use of exemptions for law enforcement and national security grounds, and that will include the relevant authorities from both sides.

Finally, when it comes to the intervention of public authorities, in particular for reasons of law enforcement and national security, the Court underlines that such access to data must be subject to clear conditions and limitations.

Against the recent attacks in Paris it is important to stress that targeted access can become crucial for instance in the fight against terrorism.

We know this. However, as we already said in our 2013 Recommendations and as confirmed by the Court ruling, we need to ensure that there are sufficient limitations and safeguards in place to prevent access or use of personal data on a "generalised basis" and we need to ensure that there is sufficient judicial control over such activities.

Whilst this remains the biggest challenge in the judgment and in our talks with the US, we should not forget that a **debate on these issues has taken and still is taking place over here, in the U.S**.

We follow with interest reformsteps such asthe USA Freedom Act and the President's instructions to the intelligence community (the so-called PresidentialPolicyDirective 28) on surveillanceand the need to take into account the privacy rights of non-Americans.

We have seen movement towards more targeted and tailored surveillance. On the use of collected data, safeguards formerly reserved for U.S. citizens have now been extended to EU citizens, for example on further dissemination of data or the period of retention.

We will closely follow the **continuation of these reforms** and how they affect European citizens whose data is transferred to the US.

Together with the final adoption of the Judicial Redress Act in the Senate, these will be important elements for the new arrangement.

In the meantime, back in Europe, we are working to swiftly finalise the ongoing negotiations on the **data protection reform**, which will replace 28 different laws with a single Regulation for European Union.

One set of modern, technologically neutral rules - good for the protection of the individual and good for innovation and business.

This is a key component of our strategy for a Digital Single Market.

I remain confident that we can conclude the negotiations by the end of the year.

The new European rules on data protection will foster the protection of a fundamental right as well as consumer trust.

But the new rules are also a business opportunity: they will create a level playing field for all companies handling personal data of Europeans and they will reduce bureaucracy and transaction costs; this will also benefit businesses from overseas.

In conclusion:

The EU and the U.S. are each other's most important trading partners, underpinned by a strong historical and political relationship.

The EU and the U.S. are also key partners to stand united to face challenges such as the fight against terrorism. Data flows between our continents are essential for people and businesses, as well as for our law enforcement cooperation.

Regarding commercial data exchanges, we need a new framework for both our citizens, whose data must be protected when it travels abroad, and for our businesses. This requires action on both sides.

But I'm confident that we will meet the deadline of January 2016 for a new agreement on international commercial data transfers. Why?

- Because we have clear guidelines from Europe's highest court.
- Because we can build on discussions held since January 2014.

o Because it is in both Europeans' and Americans' interest.

o And finally, because there is a strong political commitment at the highest level on both sides of the Atlantic.

We have shown with the Umbrella Agreement in the area of law enforcement that we can agree on common approaches on data protection, we should now repeat it in area of commercial data transfers.

Ladies and Gentlemen, I thank you for your attention.

SPEECH/15/6104