Trump v Slaughter and how the US Supreme Court has put the Data Privacy Framework at risk

Sumary

The US Supreme Court has ruled in the case Trump v. Slaughter that the US Federal Trade Commission (FTC) is not an agency independent of the executive branch, thereby overturning the 'Humphrey's Executor' doctrine, which for more than nine decades laid the foundations for independent regulatory bodies in the United States. The potential knock-on effect of this decision is overwhelming: the agreement governing international transfers of personal data between the EU and the US could be declared invalid.

BY

Nicolás Garralón

Baylos IP abion

On 29 June 2026, the Supreme Court of the United States ruled, in a controversial decision, that the President of the United States of America was entitled to dismiss a commissioner of the Federal Trade Commission (FTC) without having to provide a specific reason for doing so. The ruling, as well as strengthening the power of the executive, brings to an end a doctrine dating back more than 90 years: the Humphrey's Executor case.

The long-standing doctrine dating from 1935 established a degree of independence for regulatory bodies in the United States, limiting the President's power to dismiss senior officials from these federal agencies, except in cases of serious misconduct on their part, in order to guarantee their independence. Following the court's ruling, in the words of the Chief Justice himself: "*The FTC unquestionably exercises executive power, and must therefore be controlled by the Chief Executive, in whom such power is vested.*" This is known as the *"unitary executive theory"*, according to which the President of the United States must have absolute control over all branches of the executive power. In their separate opinion, the three judges who voted against the decision warned that this ruling *"the Court gives the President a power unknown even to the English Crown against which the Founders revolted, elevating him above his once co-equal branches by transforming a duty to take care that the laws be faithfully executed into a license to act in defiance of those very laws".*

The Supreme Court of the United States ruled, not without controversy, that the President of the United States of America has the right to dismiss a commissioner of the Federal Trade Commission (FTC) without having to provide a specific reason for doing so.

Well, I'm sure you're now thinking that everything discussed so far is very interesting, but what does Trump's decision to dismiss the FTC commissioner have to do with data protection? Does this perhaps jeopardize the agreement on international data transfers between the European Union and the United States?

To understand the implications of this decision, we need to go back on time and understand which agreements, and on what premises, have governed EU–US data transfers since the outset:

In 2000, the European Commission (EC) reached an agreement with its US colleagues to certify that the United States had an "adequate level of data protection" for processing the personal data of EU citizens. For over a decade, the Safe Harbour Agreement ("*Safe Harbour*") provided organisations with the necessary confidence to transfer data from the EU to the US. However, in 2013, a member of the US National Security Agency (NSA) revealed that intelligence agencies were systematically monitoring and collecting data on European citizens. In the wake of this revelation, lawyer Max Schrems brought proceedings against the US company Facebook, arguing that it did not guarantee the security of his data against potential interference by the US authorities. This culminated in the CJEU judgment of 6 October 2015 in Case C-362/14, known as Schrems I, which declared the Safe Harbour Agreement invalid.

Just a few months later, the European Commission formally adopted the EU–US Privacy Shield ("*Privacy Shield*"), with the aim of providing a more robust framework to facilitate the transfer of EU citizens' personal data to the US. On this occasion, Mr Schrems lodged a new complaint alleging that Facebook was obliged, under Section 702 of the Foreign Intelligence Surveillance Act (FISA), to make data transferred from the EU available to authorities such as NSA or the FBI, thereby carrying out surveillance programs incompatible with the Charter of Fundamental Rights of the European Union (CFREU). Once again, the privacy shield was annulled by the CJEU judgment of 16 July 2020, Case C-311/18, known as Schrems II.

In a third attempt, in July 2023, and under the auspices of the Data Protection Review Court (DPRC), the body responsible for protecting European citizens against access by US intelligence agencies, the European Commission adopted the current EU-US Data Privacy Framework. ("*EU-US Data Privacy Framework*" or "*DPF*"), which is the current mechanism for safeguarding transfers of personal data from the EU to the US.

What conclusions can we draw from these more than twenty years of agreements and negotiations? Well, that Europe has attempted on three separate occasions to resolve a fundamental problem by creating institutional agreements that have failed to address the underlying issue: the clear incompatibility between the extraterritorial scope of US law on surveillance and security and the fundamental European right to privacy.

The DPF is based on a concept of institutional trust.

But returning to the matter at hand, what is the relationship between the DPF and the US Supreme Court's ruling concerning the FTC?

The DPF is based on a concept of institutional trust. In order to transfer personal data to US companies under an adequate level of protection, these companies must self-certify in accordance with the Data Privacy Framework. As specified by the European Commission in its official Q&A document on the DPF, as well as in Annex I of the Privacy Shield itself, the FTC is the authority responsible for enforcing the obligations of US companies wishing to obtain certification.

And what requirements must the FTC meet to act as a compliance enforcement body? As set out in Article 16(2) of the TFEU and Article 8(3) of the Charter of Fundamental Rights, the supervision of data protection matters must be carried out by an 'independent' authority. In fact, the DPF itself cites the FTC's independence no fewer than 259 times. The very independence on which the DPF places considerable reliance has now been significantly undermined by the Supreme Court's decision.

The NGO noyb (led by Max Schrems) has highlighted this ruling and has already sent a formal letter to the European Commission calling for the Privacy Shield to be repealed.

And right now you may be wondering what immediate consequences this chain of events has for the DPF. Well, in practice, for the time being, none.

It would not be true to say that the DPF has been annulled or is about to be. Nor would it be fair to claim that the US Supreme Court has directly legislated on matters of privacy and data protection at European level. The Supreme Court's ruling is not Schrems III

What is certain, however, is that the Trump v. Slaughter ruling may imply a significant legal change to the current model for the transfer of European personal data to the US. It is not that the DPF has been invalidated, but it is fair to say that its stability has been compromised.

For the time being, organizations relying on the DPF for transfers of personal data to the United States would be well advised to assess the legal risks associated with those transfers and prepare for the possibility that the DPF could, in due course, be invalidated. Article 46 of the General Data Protection Regulation provides that, in the absence of an adequacy decision such as the DPF, personal data may only be transferred to a third country where appropriate safeguards are in place, including Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes of conduct or certification mechanisms. Where those safeguards may be affected by the legal framework of the recipient country, organizations should implement supplementary measures, such as transfer impact assessments, or, where necessary, suspend the transfers altogether.

The Trump v. Slaughter ruling may imply a significant legal change to the current model for the transfer of European personal data to the US.