Is Max Schrems about to Slaughter the EU-US Data Protection Framework?

By Dr Tristan Jenkinson

Summary

While this may sound like an advert for a reboot of Celebrity Deathmatch, it is a serious data privacy concern. There is a significant risk that the latest framework put in place to protect the data of EU citizens transferred to the US, could be invalidated, putting data transfers between the EU and US in limbo.

- In the US Supreme Court decision for Trump v Slaughter it was decided that Donald Trump could remove commissioners from the FTC at will
- This has led to concerns that the FTC (and other US government authorities) can no longer be viewed to be independent
- Privacy advocate Max Schrems is calling for the EU-US Data Privacy Framework to be invalidated as there is no independent authority in control of the framework
- The EU-US Data Privacy Framework is the latest of three legal frameworks put in place to safeguard the personal data of EU citizens upon transfer to the US.
- Previous iterations, Safe Harbour and Privacy Shield respectively, have both been invalidated as a result of legal action from Max Schrems.
- If invalidated, it could severely impact those companies who rely on it for centralisation of internal company information in the US, or those seeking transatlantic transfer of data for use in litigation based in the US.

Background

Historically, there has been a disparity in the levels of protections given to personal data in Europe and the US.

The protection of personal data has been long been viewed as a fundamental right across Europe. The approach taken can be linked directly to abuses of personal data from the early 1930s, though the Second World War, and subsequently in East Germany, prior to reunification. The movement towards a

single market across Europe in the 1990s led to the establishment of the Data Protection Directive, which standardised a cautious approach to data protection across EU states.

In the US, by contrast, a more "free market" approach developed, whereby businesses have more flexibility to collect and use personal data as they decide. Consumers can then choose what businesses and companies to use (in theory with an understanding of the data that those companies may then access and use). There are data protection rules in place, but these form more of a patchwork of state level laws and regulations in specific sectors, (for example HIPAA Health Insurance Portability and Accountability Act in relation to protected health information) rather than a single overarching law.

It is worth noting that different terms are used when comparing US and European approaches - As noted by Hoofnagle, van der Sloot and Borgesius:

> "While U.S. lawyers may refer broadly to 'privacy' or to 'information privacy', European law discusses information privacy as 'data protection.' In Europe, data protection is increasingly seen as separate from the right to privacy. Data protection focuses on whether data is used fairly and with due process while privacy preserves the Athenian ideal of private life"

As data became electronic, and increasingly voluminous, its transfer became simpler, quicker and cheaper. While there were concerns over the US approach to data protection, many companies centralised their IT infrastructure systems within the US. Others wanted to conduct global analysis without operational delays or sought to manage their customer data systems from a single (US-based) location. This meant that a lot of companies needed to find a reliable method to share data with the US, but ensure it was still protected, to avoid falling foul of the data protections in place in Europe.

Three main data sharing agreements have been utilised historically for EU/US data transfer. These will be discussed in more detail shortly. Both Safe Harbor and Privacy Shield have been invalidated and can no longer be relied upon to transfer data to the US.

The newest iteration, the EU-US Data Privacy Framework, has recently come under attack due to the decision by the US Supreme Court in the Trump v Slaughter case. This could result in the invalidation of the Data Privacy Framework, with an impact on data transfers to the US.

A Little History

The EU Data Protection Directive

The EU Data Protection Directive came into effect in 1998 and included a section (Article 25) which meant that a transfer to third country (i.e. a country outside the EEA) could only take place if that country "ensures an adequate level of protection". The US did not have an "adequate" level of protection, and so the Data Protection Directive meant that personal data could not be transferred to the US.

As discussed in this article from Outpace on Safe Harbour:

> *"Every email to a US headquarters, every customer database sync, every cloud backup—suddenly required legal gymnastics. Companies faced a choice: stop doing business, restructure entirely, or wait for a diplomatic solution."*

A Working Party discussion with a specific focus on transfers to third countries can be found here. This document goes into further details about what an "adequate" level of protection may look like.

Safe Harbour

Safe Harbour was set up in July 2000, after years of discussions, to address the disparity in data protection requirements exposed under the EU Data Protection Directive. The scheme allowed US companies to sign up voluntarily, to confirm that they would abide by a series of seven principles – Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement (details of the principles can be found in Annex I of the Commission Decision).

It is worthy of note that the enforcement of Safe Harbour fell to the US Department of Commerce, and the US Federal Trade Commission.

The Downfall of Safe Harbour (Schrems I)

In early June 2013, Edward Snowden leaked documents from the US National Security Agency to journalists from the Guardian newspaper.

Some of the revelations from the leaks include a programme named PRISM, which, according to the Guardian gave the NSA " 'direct access' to data held by Google, Facebook, Apple and other US internet giants" and a programme named Upstream which was used to intercept both internet traffic and telephone data from the fibreoptic cables making up the internet backbone.

Amnesty International highlighted that the Upstream programme, (together with a similar GCHQ programme called TEMPORA) was used for mass surveillance by the NSA:

> *"These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through the cables that make up the backbone of the internet. Undersea cable tapping provides UK and US intelligence agencies with unprecedented surveillance powers".*

In late June 2013 Max Schrems, at the time a law student and privacy advocate, now lawyer and Honorary Chairman of non-profit "nyob" ('None of Your Business') made a complaint to the Irish Data Protection Commissioner ("DPC"), complaining about the transfer of his personal data from Facebook in Ireland to Facebook's US servers.

Schrems explicitly highlighted the revelations from Edward Snowden and claimed that under Safe Harbour (apparently relied upon by Facebook for the transfer of data), there was not adequate protection of his personal data.

The claim was originally dismissed by the Irish DPC, and Schrems filed a Judicial Review claiming that Safe Harbor was itself invalid. The Irish High Court appeared to largely agree with Schrems. They explained that if the decision was to be made purely based on Irish Law, the Data Protection Commissioner would have been found wrong to dismiss the complaint (see for example para 33 of the later CJEU decision). However, it considered that the matter related to European Law and so referred the matter to the EU Court of Justice.

The CJEU determined in October 2015 that Safe Harbor was invalid (The press release from the Court of Justice explaining the decision can be found here).

Two of the key points of the judgment were

- Mass surveillance in the US meant that the protections offered were not adequate - "... l*egislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life"*
    - It was also highlighted that the High Court had identified that *"the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies"* at paragraph 30 of the Judgment)
- The lack of an effective remedy for EU individuals

- *"... legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law"*

Privacy Shield

In July 2016, a replacement for Safe Harbour was formally approved by the European Commission. As with Safe Harbour, this allowed for self-certification by corporations in the US.

The principles of Notice, Choice, Accountability for Onward Transfer, Security Data Integrity and Purpose Limitation, and Access closely match the Safe Harbour framework, but with a few tweaks and additional protections thrown in. The Recourse, Enforcement and Liability principle contained much more detail than in Safe Harbour (not least because this was one of the specific areas in which Safe Harbour was viewed to have failed). One of the additional protections brought in with Privacy Shield was the implementation of an ombudsperson. Based on this press release from the EU Commission:

> *"The possibility for redress in the area of national security for everybody whose data is transferred to the U.S. will be handled by an Ombudsperson, independent from the US intelligence services".*

This article from the International Association of Privacy Professionals provides additional breakdown of the differences when considering the various principles between the two agreements. The EU Commission also released a fact sheet including a section highlighting the differences between Privacy Shield and Safe Harbour.

With GDPR already on the horizon (implemented in May 2018), there were already questions about Privacy Shield when it launched, since GDPR would provide stronger protections for the data of EU citizens.

The Downfall of Privacy Shield (Schrems II)

Strangely, the path to the invalidation of Privacy Shield started before Privacy Shield was even implemented. Contrary to what may have been expected, Privacy Shield wasn't directly challenged by Schrems.

After the ruling invalidating Safe Harbour (Schrems I), Facebook responded claiming that they had not been relying upon Safe Harbour to transfer data but

had in fact relied upon Standard Contractual Clauses (SCCs). Standard Contractual Clauses are contract terms (pre-approved by the EU) between two companies to protect personal data where it is transferred from one company in the EEA to the other outside of the EEA.

Considering Facebook's claim of reliance on SCCs, the Irish Data Protection Commissioner suggested that Schrems may reformulate his complaint from Schrems I. Schrems called for the Data Protection Commissioner to suspend or prohibit Facebook from any future transfer of his personal data to the US, on the basis that SCCs, as simple contractual terms, could not protect EU data from surveillance by US authorities, nor could they provide any legal remedies for EU citizens to address abuses of their data in the US.

The Data Protection Commissioner agreed with many of the arguments made by Schrems, however, believed that the case raised the question of whether SCCs were invalid in general. As discussed above, SCCs are approved by the EU. As such, any decision on their validity could only be taken by the CJEU.

With this in mind, the DPC raised a case in the High Court, to examine the legality of SCCs, which could then refer questions to the CJEU.

In the Irish High Court case, the role of mass surveillance in the US was investigated. This led to discussions over Privacy Shield, because the adoption document for Privacy Shield (issued by the EU) explicitly investigated surveillance methods used by the US Government (for example section "Access and use by U.S. public authorities for national security purposes" within the adoption text).

The CJEU found that SCCs were valid but required a case-by-case examination to ensure that adequate protection was in place.

While they left SCCs in place, the CJEU invalidated Privacy Shield. The main reasons for this were that US law allowed US authorities to access the personal data of EU citizens without protections equivalent to those in EU law (which by this time included GDPR). In addition, there were no effective remedies against such surveillance.

This press release covering the decision contains a (relatively) concise discussion of the findings.

It is also worth noting that another point raised in the CJEU decision was that the Privacy Shield Ombudsman was not sufficiently independent, nor could they make any decisions binding on any US authorities carrying out surveillance. Effectively the Ombudsman was toothless to protect EU citizens against the mass surveillance of the US government.

The EU-US Data Privacy Framework

The EU-US Data Privacy Framework was adopted in July 2023, as covered in this press release. It was described in an article published on Max Schrems' nyob website as "largely a copy of the previously annulled deals".

The press release also hails some of the additional safeguards that are put in place in this framework. They include restricting access to US authorities to what is necessary and proportionate to protect national security. A significant part of the legal coverage for this sits within the Executive Order "Enhancing Safeguards for United States Signals Intelligence Activities", signed by President Biden.

The press release also notes the creation of a new Data Protection Review Court, designed to give EU citizens access to an independent, impartial mechanism to address allegations of misuse of their personal data.

These were two of the critical areas where Privacy Shield failed.

It is also helpful to note that, as the press release confirms:

> *"The Framework is administered and monitored by the US Department of Commerce. The US Federal Trade Commission will enforce US companies' compliance."*

Trump v Slaughter

Rebecca Slaughter and Alvaro Bedoya were Democratic commissioners of the Federal Trade Commission ("FTC") in the US.

As the Supreme Court's decision explains (https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf.):

> "The Federal Trade Commission (FTC) is a regulatory agency that has accumulated vast rulemaking, enforcement, and adjudicatory powers. The FTC's powers belong not to the President or his appointees alone, but instead to five Commissioners, each of whom serves for seven years and may be removed by the President only "for inefficiency, neglect of duty, or malfeasance in office." 15 U. S. C. §41."

In January 2025 US President Donald Trump fired Slaughter and Bedoya. Rather than identifying the basis for their dismissal, they were informed (as stated in the Supreme Court decision) that their "continued service on the FTC [was] inconsistent with [his] Administration's priorities" and that they were removed "pursuant to [his] authority under Article II of the Constitution".

This was challenged by Slaughter, and the case eventually made its way to the US Supreme Court. The Supreme Court upheld the Presidents removal of Slaughter, overturning a 1935 decision Humphrey's Executor v United States.

The Humphrey's Executor decision includes several sections of text which is of interest here:

> *"The power of removal here claimed for the President falls within this principle, since its coercive influence threatens the independence of a commission, which is not only wholly disconnected from the executive department, but which, as already fully appears, was created by Congress as a means of carrying into operation legislative and judicial powers; and as an agency of the legislative and judicial departments."*
>
> *"The authority of Congress, in creating quasi-legislative or quasi-judicial agencies, to require them to act in discharge of their duties independently of executive control cannot well be doubted; and that authority includes, as an appropriate incident, power to fix the period during which they shall continue in office, and to forbid their removal except for cause in the meantime. For it is quite evident that one who holds his office only during the pleasure of another, cannot be depended upon to maintain an attitude of independence against the latter's will."*
>
> *"The fundamental necessity of maintaining each of the three general departments of government entirely free from the control or coercive influence, direct or indirect, of either of the others, has often been stressed and is hardly open to serious question."*

Ultimately, the Humphrey's Executor decision boiled down to answering two questions:

1. *Do the provisions of section 1 of the Federal Trade Commission Act, stating that 'any commissioner may be removed by the President for inefficiency, neglect of duty, or malfeasance in office,' restrict or limit the power of the President to remove a commissioner except upon one or more of the causes named? "*

   If the foregoing question is answered in the affirmative, then-

2. *"2. If the power of the President to remove a commissioner is restricted or limited as shown by the foregoing interrogatory and the answer made thereto, is such a restriction or limitation valid under the Constitution of the United States?"*

The Humphreys Executor decision (somewhat emphatically) declared that the answer to both questions was yes.

As summarised by Dentons in their article:

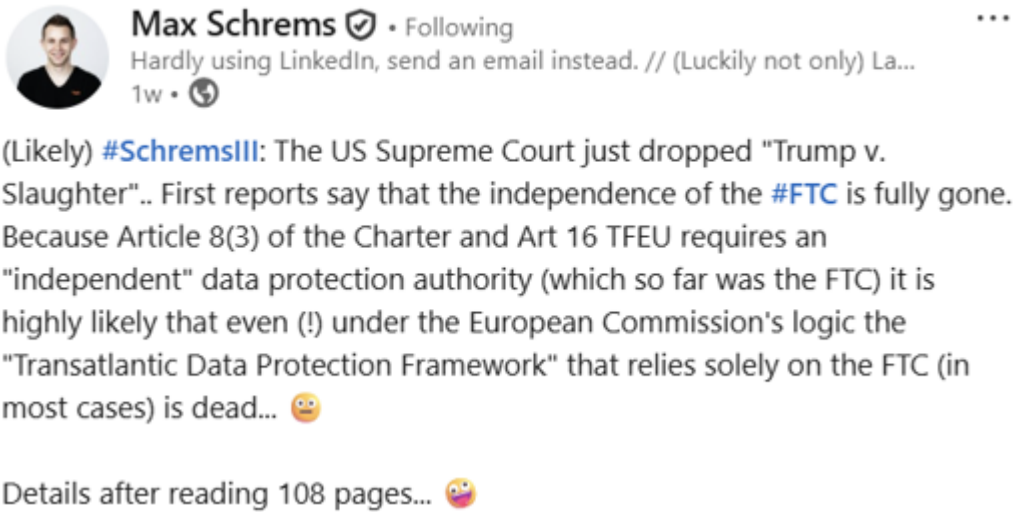
> *"As a result, the President now has unchecked authority to remove such leaders of agencies that exercise executive power, as any statutory "for cause" protections are now unconstitutional."*

And further (emphasis from the original publication):

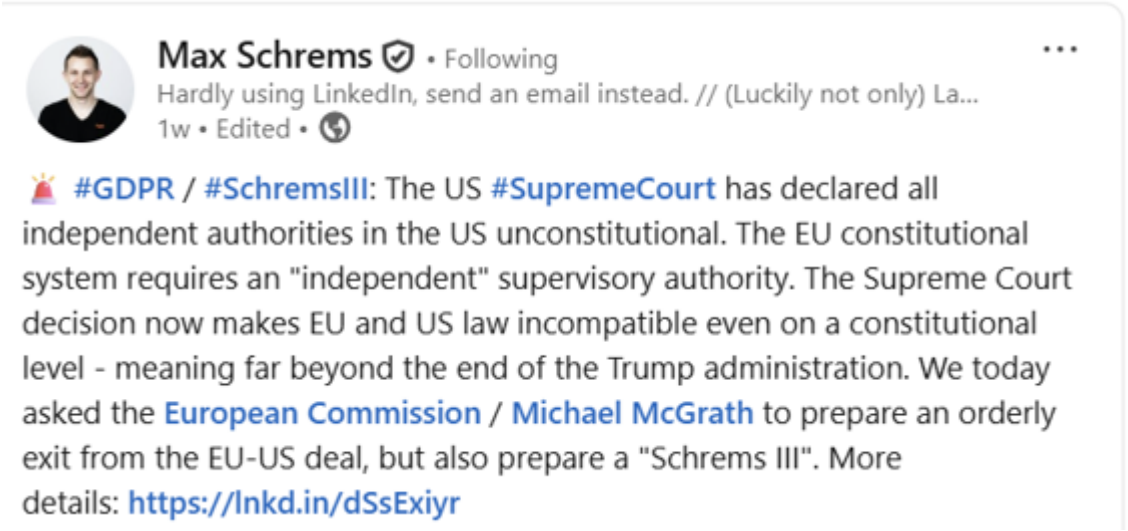
> *" **'Independent' agencies are no longer independent**—The President now controls the policy decisions of these agencies."*

Schrems III

On 29 June 2026 (the day that the decision in Trump v Slaughter was published), Max Schrems posted on LinkedIn:

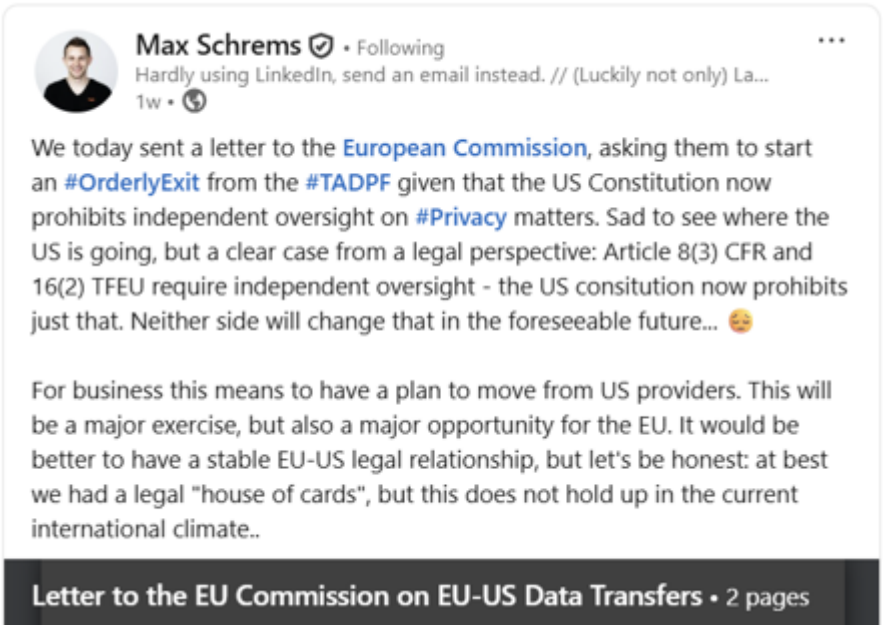


The following day, Schrems posted:



The post links to an article on Schrems' noyb website which is worth reading.

Later that day, Schrems posted details of a letter which they had sent to the EU Commission regarding the issue.



As with the LinkedIn posts from Schrems, the letter highlights key points relating to independence. The Data Privacy Framework requires an independent authority, and the FTC (the appointed authority in the US) no longer being considered independent.

There are two main thrusts in Schrem's argument that the EU-US Data Privacy Framework requires an independent authority to implement or control them:

- Article 16 (paragraph 2) of the Treaty of the Functioning of the European Union, and
- Article 8 (paragraph 3) of the EU Charter of Fundamental Rights

Article 16

Article 16 sits within the 'Principles' section of the Treaty and contains only two paragraphs. It is helpful to consider paragraph 1 to see how fundamental this article of the treaty is.

Paragraph 1 simply states:

> *"Everyone has the right to the protection of personal data concerning them."*

This is the fundamental level of content that this article covers. Paragraph 2 is a little more complex, but it essentially says that the EU will lay down the rules for others to follow. Key to Schrems' argument is the final sentence. The full paragraph, with my emphasis added is below:

> *"The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.* ***Compliance with these rules shall be subject to the control of independent authorities.****"*

Article 8 of the EU Charter of Fundamental Rights

The content of the article is not dissimilar to the content covered above. The whole Article has just three paragraphs, and I include all of these below, again with my emphasis added:

> *"Article 8 - Protection of personal data*
>
> *1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3.* ***Compliance with these rules shall be subject to control by an independent authority.****"*

Given the (apparent) requirement for EU-US Data Privacy Framework to be controlled by an independent authority, the decision in Slaughter is highly problematic as it does appear to remove the independence of the FTC.

As highlighted above, the two authorities involved in overseeing the EU-US Data Privacy Framework are the FTC and the Department of Commerce. The head of the Department of Commerce is the Secretary of Commerce, who reports directly to the President, and so the Department of Commerce is also not seen as an independent authority. The lack of independence of the FTC would means that there is no independent authority in control of the Framework.

The removal of independence of US authorities in the Slaughter decision is perhaps emphasised by the language in Humphrey's Executor which speak to the importance of independence for agencies such as the FTC.

What Next?

It appears likely that Max Schrems will continue to push for an "Orderly Exit" from the EU-US Data Privacy Framework. This may or may not result in the decision being declared invalid. Even if it does, as the article on nyob explains:

> *"...such a lawsuit typically takes 2-3 years until a final decision is reached."*

While it may be some time before direct impact, an invalidation of the framework would impact on companies which have centralised functions based in the US, and so may be transferring data there. Not only that, but it could constitute a challenge for US companies to utilise the data from European subsidiaries in US based litigation, or regulatory responses. This may then require data minimisation exercises to be undertaken in Europe, and checking relevant procedures are in place to transfer the resulting minimised data to the US.

Having been in this position twice before (after the invalidation of Safe Harbour and Privacy Shield) it may be easy to assume that companies would have secondary transfer mechanisms in place, but this is not always the case, especially for companies that may have been incorporated in the meantime.

This remains an important topic to monitor for those interested in data privacy, and especially its impact on cross border data transfers.