UK's post-Brexit data regime: between EU privacy law and US surveillance law

What does the Schrems case mean for UK post-Brexit data flows? At the heart of the Schrems case is a conflict of laws – a conflict between EU privacy law and US surveillance law. After 31 December, the question about surveillance law turns around to point at the UK. Whichever way one looks at it, deal or no deal with the EU, UK surveillance law will be the determining factor, writes ***Monica Horten (LSE).***

Overnight on 31 December 2020, the rules governing data flows from the UK to other countries will change. As the UK pulls out of the pan-European GDPR regime, it simultaneously rips up the cross-border arrangements for the protection of data being processed abroad.

Whilst that might sound insignificant beside the vision of lorry parks along the M2, it actually pulls the rug from under a crucial element of business administration and logistics, not to mention a plethora of apps, that rely on electronic data transfers and cross-border processing. Where UK businesses have been able to process data like at home in 27 other countries, from 31 December they will need a new arrangement with the EU, known as an 'adequacy' decision. Without 'adequacy', every business that transfers personal data to the EU for processing will have to put in place new bespoke contracts. In simple terms, it will mean a lot of red tape.

The Schrems case highlights key aspects of the legal context. A close analysis reveals how UK surveillance law potentially hangs over our data flows like a latterday sword of Damocles.

At the core of the Schrems case is a conflict of laws – a conflict between EU privacy law and US surveillance law. This principle is at the root of the issue that will affect the UK. When the UK becomes a third country, the question about surveillance turns around to point this way.

The Schrems ruling was handed down on 16thJuly by the European Court of Justice (CJEU Case C-311/18). It follows a request by the Irish High Court in a case between the Data Protection Commissioner and Facebook Ireland and the Austrian lawyer Max Schrems. The case concerned a complaint by Max Schrems about the transfer of his Facebook data to the United States.

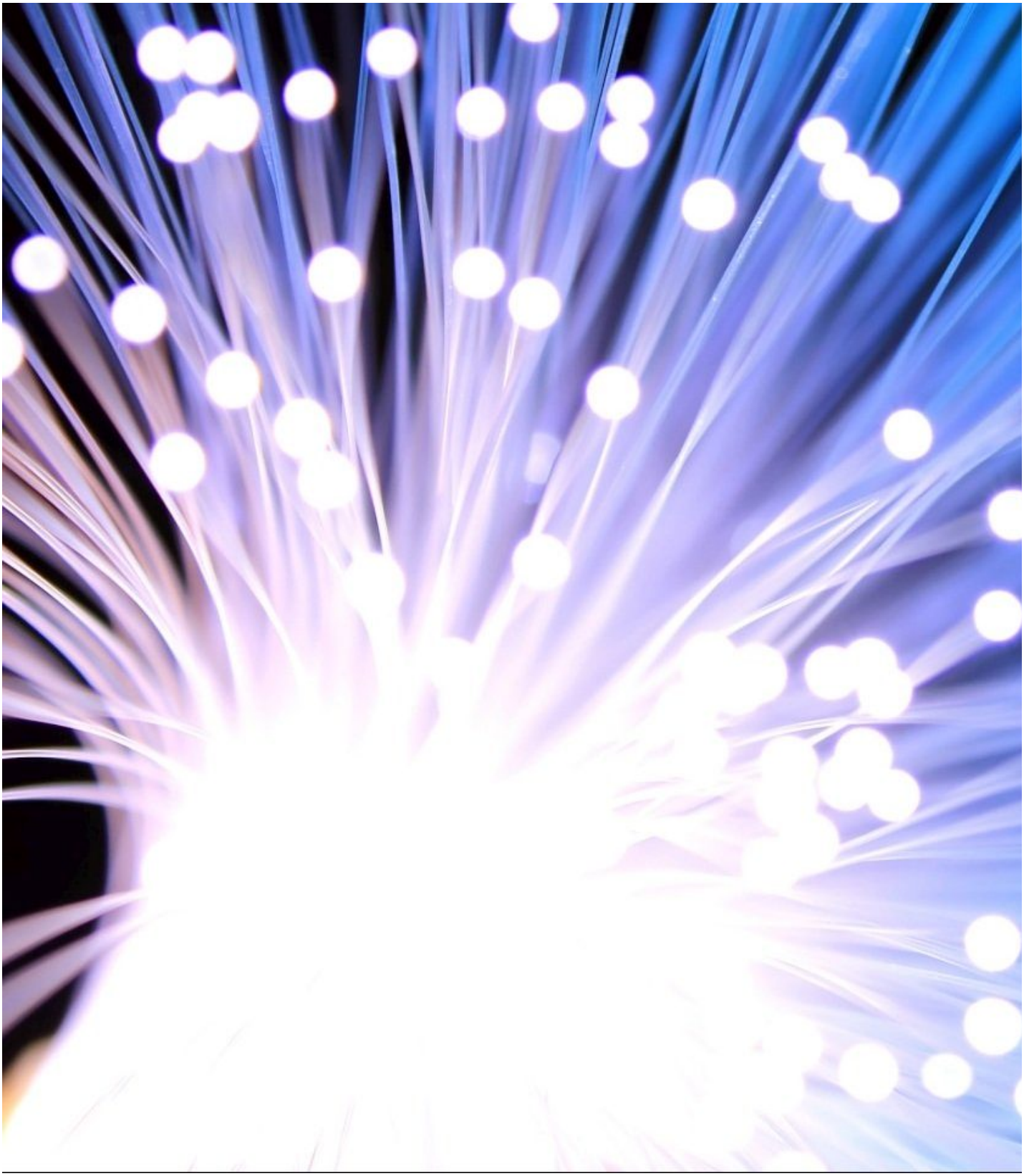
The court struck down the Privacy Shield – a treaty between the EU and US that facilitates the transfer of personal data from the EU to the US for processing, and currently still covers the UK. Without the Privacy Shield, businesses will have to put place their own bespoke contracts in order to guarantee the privacy of the data to meet the standards required by EU law. These are known as Standard Contractual Clauses (SCCs). As a consequence of the Schrems ruling, those businesses will have to assess the US legal framework to ensure it can offer guarantees to keep EU citizen's data safe. (See European Data Protection Board FAQs on the Schrems case).

Businesses will also have to assess the legal framework when using SCCs to transfer data to any other third country. The assessment will have to take account of surveillance laws, and any requirement of the third country for access by national security or law enforcement.

Date originally posted: 2020-07-31

Permalink: https://blogs.lse.ac.uk/brexit/2020/07/31/uks-post-brexit-data-regime-between-eu-privacy-law-and-us-surveillance-law/

Blog homepage: https://blogs.lse.ac.uk/brexit/



EU law demands a high level of privacy protection for data relating to individuals. This is not just about names and email addresses, it is all the data that may be collected through apps and computer networks, it is location data, shopping, entertainment, social media posts and so on.

Date originally posted: 2020-07-31

Permalink: https://blogs.lse.ac.uk/brexit/2020/07/31/uks-post-brexit-data-regime-between-eu-privacy-law-and-us-surveillance-law/

Blog homepage: https://blogs.lse.ac.uk/brexit/

By contrast, US law demands that data is made available for surveillance of foreign nationals. This is the Foreign Intelligence Surveillance Act (FISA) Section 702, which authorises warrantless surveillance programmes targeting foreign nationals by US law enforcement agencies. FISA 702 programmes – known as PRISM and UPSTREAM – entail the bulk processing of personal data from communications companies, notably the big tech platforms like Google, Facebook and Microsoft, and telecoms networks.

In the Schrems ruling, the CJEU found that FISA surveillance is not subject to principle of proportionality (178). The FISA law does not provide any limitation on surveillance programmes of foreign nationals, nor any guarantees to safeguard rights of foreign nationals (180). Surveillance programmes based on FISA are not limited to what is strictly necessary (184), and there is no right of action by EU citizens (181 and 192).

The ruling assesses Article 45 of GDPR which governs the transfer of personal data to third countries. It said that (188) *"Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'".*

It is "I*mpossible to conclude that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter." (191).* On that basis, the court felt that FISA is disproportionate and it struck down the Privacy Shield.

UK surveillance law is problematic when viewed from an EU perspective. The UK has an extensive surveillance regime [lorna woods] and bulk collection of data by the intelligence services is permitted under the Investigatory Powers Act. According to Professor Lorna Woods, of Essex University, the UK has benefitted until now as a Member State of the EU – and currently still a member of the Single Market – and has not had to prove adequacy. But all that changes on 1 January next year when (assuming it does happen) the UK leaves the Single Market and becomes what's known as a "third country".

The government's official line is to seek an adequacy decision. This will have to granted by the European Commission, after examining the UK data protection framework. The UK government argues that adequacy should be 'a logical technical consequence' because the UK already has implemented GDPR, as stated by the UK's (former) negotiator David Frost, to the House of Commons Select Committee on the Future Relationship with the EU on 27th May (Q240).

Post-Schrems, the government is "w*orking with the Information Commissioner's Office and international counterparts to update guidance,*" according to the answer supplied by DCMS to a written question in the House of Commons on 23 July.

However, it is an open question as to how the European Commission will view the UK's surveillance framework. This has been a cause for concern since the Snowden revelations of 2014, when some of GCHQ's bulk data surveillance activities were made public. New UK-US data sharing agreement with the US have caused further disquiet, according to Prof. Woods.

Moreover, the government's stated policy is to diverge from the EU framework, as confirmed to the House of Lords Committee on the European Union on 28th May (Q18). This raises a red flag. If 'divergence' entailed any weakening of individual privacy protection, it would put at risk the data flows to the UK. The government regularly dangles the prospect of leaving the European Convention on Human Rights – and then denies it. Such a move would, without doubt, put an adequacy arrangement in jeopardy. The ruling has made it clear that data subjects rights must be fully protected when data is transferred to a third country.

With no adequacy arrangement – likely to be in a so-called 'no deal' – businesses will be dependent on SCCs. This is the gotcha. As a result of the Schrems ruling, we here in the UK will be a third country that businesses will have to assess.

The requirement for businesses to take account of the laws of a third country when implementing the Standard Contractual Clauses (SCCs) means that any business wishing to transfer bulk datasets of personal data to the UK from 1 January 2021 will need to conduct their own assessment of the UK's legal framework and satisfy themselves that it will offer adequate protection.

Date originally posted: 2020-07-31

Permalink: https://blogs.lse.ac.uk/brexit/2020/07/31/uks-post-brexit-data-regime-between-eu-privacy-law-and-us-surveillance-law/

Blog homepage: https://blogs.lse.ac.uk/brexit/

Warnings have been issued by the business and legal community. The manufacturers' association, MakeUK, says that: "*how the UK Government approaches personal data transfers to the US going forwards might actually influence the European Commission's view of the adequacy of the UK's data protection regime. For example, the Commission might not look on the UK favourably if it decides not to adopt the Commission's stance on US data protection or enters into a new agreement with the US that is akin to the Privacy Shield.*"

Law firm Norton Rose Fulbright warns that: *"This judgement has broad applicability and could impact transfers to any other non-EEA country that has not achieved adequacy status. This will include the UK if, after the Brexit transition period, the UK has not obtained an adequacy finding from the European Commission."*

What they don't say, but is implicit, is that surveillance law will more than likely be the deciding factor for UK data flows.

This post represents the views of the author and not those of the Brexit blog, nor the LSE. It also appeared on the author's blog.

Date originally posted: 2020-07-31

Permalink: https://blogs.lse.ac.uk/brexit/2020/07/31/uks-post-brexit-data-regime-between-eu-privacy-law-and-us-surveillance-law/

Blog homepage: https://blogs.lse.ac.uk/brexit/