Data Privacy and Cybersecurity

Schrems II - What Next for International Data Transfers?

By: Kelly Hagedorn, David P. Saunders, and Matthew Worby

On 16 July 2020 the Court of Justice of the EU (**CJEU**) issued its judgment in the case of *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (***Schrems II***).[1] The CJEU ruled that the EU-US Privacy Shield was invalid and threw the use of standard contractual clauses (**SCCs**) into question. For an analysis of the immediate impact of this judgment please see our alert here.

Schrems II reiterated the CJEU's view that EU residents' data privacy rights are incompatible with the United States' approach to data privacy in the context of national security. Accordingly, the European Union, and possibly the United Kingdom, will need to change its approach to international personal data transfers (**IPDTs**) to the United States.

In this article we shall examine some of the critical questions that arise following the judgment, including how the incompatibility between the European Union and United States arises, what this means, and offer some brief thoughts about how this might impact the European Union's approach to other countries and the United Kingdom's adequacy decision.

What Is the Source of EU and US Incompatibility?

Schrems II confirmed that the US approach to data privacy in the context of national security is incompatible with EU data protection law. This is because, in the CJEU's view, the US national security agencies collect large quantities of data, which could, and in some instances does, include the personal data of EU residents, without significant oversight. Moreover, because most of the collection of information for national security purposes is done in secret, there is little ability for EU residents to seek redress through the courts related to the US government's collection and use of the EU residents' data.

Two primary tools used by the US government that the CJEU identified as creating incompatibility with the privacy principles embodied in the GDPR were section 702 of the US Foreign Intelligence Surveillance Act (**FISA**), and Presidential Executive Order 12333 (**EO12333**). In short, both FISA and EO12333 permit the US government to collect in bulk the communications data of non-US citizens residing outside of the United States. Often, this collection occurs with the secret, but compelled, assistance of technology providers.

What Is the Concern?

According to the CJEU, these combined mechanisms allow the US government to undertake the mass surveillance of EU residents' personal data if transmitted to the United States. Even if that is not happening in reality, the CJEU focused on the *possibility* that the US government could do so without permitting any redress to EU residents. However, EO12333 was signed in December 1981, and FISA, whilst first enacted in 1978, was amended in 2008 to create S.702, which itself actually places a limit on the practice that had existed before that time. These powers to collect data are not new, and in fact were in existence at the time that the EU-US Privacy Shield was first negotiated. As such, why are they now a significant concern?

It seems to us that the issue concerns the haphazard manner in which the global digital economy has

developed since 2008. Over the past decades, the European Union has broadly accepted government surveillance as the digital economy helped to drive economic growth. This can be seen through the development of Safe Harbour, the Privacy Shield's predecessor, and then of course Privacy Shield. However, the CJEU has now implicitly decided that the rights of EU residents to have their data protected outweigh any economic advantages of having a free flow of personal data to the United States.

What is yet to be fully considered in this debate, however, is the extent to which companies operating within the European Union need to transmit personal data to the United States. Before a debate between the competing interests of commerciality and data privacy is had, it should perhaps be clarified if the argument is worth having in the first place. Is the economic value of constantly transmitting personal data to the United States so high that it should require the European Union to consider being more lenient with respect to its privacy principles?

Separately, the extent to which US companies require personal data from EU residents is also unclear. If the competing regulatory pressures that a transatlantic company faces become too severe, is it entirely unfeasible that such a company could either do without the data entirely, or simply keep it in Europe?

In any event, these fundamental questions have, to some extent, been put off by the decision of the CJEU to retain the effectiveness of SCCs; at least for now. However, for the reasons we set out below, we think it is probable that SCCs may not continue to be valid for much longer, making the fundamental questions posed above all the more pressing.

Why Can't SCCs Maintain the Status Quo?

At the same time as invalidating the EU-US Privacy Shield, the CJEU ruled that SCCs were, in principle, valid. Accordingly, this has led to the argument that IPDTs can continue as normal, but with SCCs providing the basis upon which to transmit personal data to the United States. Indeed, following the *Schrems II* decision, several of the largest tech companies confirmed that they would continue to rely upon SCCs to transfer personal data to the United States from the European Union.[2]

However, the CJEU's judgment in *Schrems II* contains criticisms of US law that are as applicable in the context of SCCs as they are in the context of the Privacy Shield. In ruling that SCCs are a valid mechanism for IPDTs, the CJEU stated that additional measures would be required to ensure the privacy of any IPDT, using SCCs as the basis for transfer, to the United States.

Even if a company were to attempt to meet the requirement for additional measures over and above the SCC text, it is difficult to envisage how a private entity would have the technical capability to do so. The initial questions that arise appear difficult to reconcile:

1. The classified capability for the US government to break encryption measures means any adequate assessment of the use of encryption as an additional measure is unlikely to be practical.
2. The constant need to evaluate and maintain such a risk assessment would be an expensive exercise.
3. The US government claims to use selectors[3] to target their surveillance programmes. Often such selectors sit within the encrypted transmission. As a result even if a message is encrypted, it may still be intercepted.
4. Companies are, broadly, unable to choose which cables are used for their IPDTs, and cannot therefore select cables that are not susceptible to interception by the US government.

The *Schrems II* decision makes it difficult to see how, practically, the use of SCCs to transfer personal data to the United States can continue. In addition, the European Data Protection Board has clarified

that entities must carry out a review of the law in each country to which they export personal data if those transfers are pursuant to SCCs. This is another potentially onerous task. It remains to be seen if companies will seek to maintain the status quo, using SCCs for as long as possible. There may well be steps that can be taken to achieve this, but it is also possible that an increasing number of companies will start to bifurcate their operations to isolate EU personal data within the European Union. Some service providers already offer customers this option; no doubt others will follow suit.

It is also entirely possible that the debate surrounding SCCs is rendered academic. In the weeks after *Schrems II*, several posts on the NOYB (the privacy organisation of which Max Schrems is the honorary chair) website suggest Mr Schrems may make a specific challenge to the validity of SCCs in the near future. And indeed, NOYB has already filed more than 100 complaints with different data protection authorities challenging data transfers to the United States that place the SCCs in the crosshairs. The CJEU could, therefore, render SCCs formally invalid before the concept of "adequate measures" is properly explored.

In an effort to respond to this dramatic change in cross-Atlantic IPDTs, the European Commission and US Department of Justice have recently announced that they are working together to attempt to reformulate the Privacy Shield so that it complies with *Schrems II*. Whether these discussions will produce an effective outcome remains to be seen, but it is a positive step that the relevant authorities are talking to one another; a recognition of the importance of restoring the Privacy Shield. However, Mr Schrems has already indicated that he will challenge any reformulated Privacy Shield unless that reformulation involves a change to US surveillance, which may scuttle any hope for a long-term solution.

What about Other Countries?

Schrems II will also raise questions about other jurisdictions that have previously received adequacy decisions from the European Commission. The adequacy decisions for countries such as New Zealand and Canada, both part of the Five Eyes alliance with the United States, may now face significant scrutiny from privacy campaigners like Mr Schrems.

This same pressure, however, was felt following the decision invalidating the previous EU-US Safe Harbour arrangement. In that instance the European Commission did not revisit its adequacy decisions for states such as New Zealand or Canada. In the intervening years, the European Union has also continued to press for greater cooperation with the United States in respect to the general sharing of data for law enforcement purposes.

Businesses should consider their IPDTs to these other countries as part of their risk assessments, and be able to provide appropriate documentary support in line with the GDPR's accountability principle should they receive questions from supervisory authorities in this regard.

Where Does This Leave the United Kingdom's Adequacy Decision?

One area that will change significantly, is the United Kingdom's position in the context of IPDTs post-Brexit. Unlike New Zealand or Canada, two other members of the Five Eyes alliance, the United Kingdom does not currently have an adequacy decision because it has until now been a Member State of the European Union.

For the purposes of EU law, whilst a member, the United Kingdom's national security legislation authorising mass surveillance programmes could not invalidate the free flow of personal data. The United Kingdom could, therefore, freely receive personal data from the European Union, despite the United Kingdom's surveillance laws raising many of the same issues that were critiqued in *Schrems II*.

On 1 January 2021 this ceases to be the case. At that point the United Kingdom's national security framework must be evaluated in the context of an adequacy decision. Even if this analysis is not fully

undertaken by the European Commission at this time, it is possible that privacy advocates will challenge transfers to the United Kingdom by lodging complaints with supervisory authorities, which will then be required to consider the compatibility of UK law with data subjects' rights.

The *Schrems II* decision therefore ought to give the UK government pause for thought when determining the development of British data protection law post-Brexit. Greater movement towards data sharing with the United States (for surveillance or other reasons) or any other perceived reduction in data protection rights could well serve to jeopardise EU-UK IPDTs.

So What Can Be Done?

To this point of our article, we have highlighted much of the doom and gloom that radiates from companies evaluating *Schrems II*, however all is not lost. While the SCCs are a valid method for continuing IPDTs to Europe – and will be likely for years to come even if Mr Schrems launches a direct assault on them – companies can take steps today to avoid major disruption in the event the SCCs or Privacy Shield successor are subsequently deemed invalid.

While it seems unlikely that the United States will change course and radically change its intelligence gathering practices, companies can take steps to account for the existence of those laws. For example, companies can consider – as the Bavarian DPA has suggested – identifying or adding a controller entity in Europe itself so that data no longer needs to be transferred out of Europe. For some businesses, that may not be practical, however. And so another step that companies can take is to evaluate what data they send to the United States: is there a way to send less or de-identified or aggregated data such that GDPR might not be implicated? And of course, companies could attempt to obtain written consents – at least for European-based employees, which would allow the transfer of data to continue.

Conclusion

At this stage, unfortunately, the primary conclusion one can draw from *Schrems II* and its aftermath is that more uncertainty will follow. IPDTs to the United States from Europe are not over, but are considerably more challenging, third countries with adequacy decisions will need to rethink how they deal with IPDTs to the United States, and another layer of complexity has potentially been added to the Brexit discussions. And that is all before one considers a possible *Schrems III* challenge to the validity of the SCCs. Companies need not be frozen in place, however. As outlined above, there are certain, proactive steps that companies can take today that may position them to better be able to respond to an eventual challenge to the SCCs or to additional changes to the ways that IPDTs are permitted.

---

[1] Case C311/18 - https://files.lbr.cloud/public/2020-07/ecj judgment.pdf?IfEaIZBAlzPT0iT9teTLp.wk_PU3BtLZ

[2] https://globaldatareview.com/data-privacy/exclusive-amazon-continue-using-sccs-us-data-transfer

[3] Selectors are key data points such as an email address or an IP address.

Contact Us

Kelly Hagedorn

khagedorn@jenner.com | Download V-Card

David P. Saunders

dsaunders@jenner.com | Download V-Card

Matthew Worby

mworby@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card

© 2020 Jenner & Block LLP. **Attorney Advertising.** Jenner & Block is an Illinois Limited Liability Partnership including professional corporations. This publication is not intended to provide legal advice but to provide information on legal matters and firm news of interest to our clients and colleagues. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this publication. The attorney responsible for this publication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome.