PAUL HASTINGS

Stay Current

October 2020

Follow **@Paul_Hastings**

U.S. Government Publishes White Paper Following Schrems II Decision

By Sarah Pearce, Aaron Charfoos, Behnam Dayanim, Ashley Webber & Randall Johnston

The decision of the Court of Justice of the European Union ("CJEU") to invalidate Privacy Shield and opine on the use of Standard Contractual Clauses ("SCCs") left many asking how the decision should be applied—particularly by companies transferring personal data from the EU to the U.S. As is discussed further here, the CJEU stated in its decision that, when using the SCCs to transfer personal data to any third country, such as the U.S., the exporting company should undertake an analysis of the laws relating to personal data in the importing jurisdiction, focusing particularly on the access agencies and other bodies in the importing jurisdiction have to the data, in order to determine whether the personal data would be adequately protected. Official guidance on how to undertake such reviews has been fairly limited (a full list of responses from regulators to date can be found here), though more substantive guidance is expected in the near future from the European Data Protection Board and other data protection regulators.

In the meantime, the U.S. government has published a White Paper to provide a "*detailed discussion*" of the information exporting companies should take into consideration when undertaking an analysis of the applicable laws of the U.S. as the importing jurisdiction, with particular attention being given to the issues that were discussed by the CJEU in its decision. The White Paper states clearly that "*it is not intended to provide companies guidance about EU law or what positions to take before European courts or regulators*"; it is simply seeking to provide an "*up-to-date and contextualized discussion of this complex area of U.S. law*".

The White Paper focuses on the following three key points which are each considered further below:

1. Most companies "*do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do*".

2. The U.S. government "*frequently shares*" intelligence information with Member States, including data disclosed by companies in response to FISA 702 orders, to counter threats such as terrorism, which "*undoubtedly*" serves EU public interest.

3. There is a "*wealth of public information*" about data privacy protections in U.S. law concerning access to data, including information which was not referred to in EU Commission Decision 2016/1250 (i.e. Privacy Shield), new developments in the law since 2016, and information that was otherwise not addressed by the CJEU.

I. "Companies Not Disclosing Data to U.S. Intelligence Agencies"

The crux of this discussion is that the issues raised by the CJEU are unlikely to arise for most companies transferring personal data to the U.S. because the data they process is of "*no interest to the U.S. intelligence community*".

This White Paper does not elaborate on that characterization, other than to observe that U.S. government policies restrict intelligence collection for the purpose of "*obtaining commercial advantage*". Therefore, according to the White Paper, those companies whose EU operations involve ordinary commercial products or services, and whose transfers to the U.S. involve ordinary commercial information (like employee or customer data), "*would have no basis to believe U.S. intelligence agencies would seek to collect that data*". Whilst, in our experience, intelligence collection is generally highly circumscribed in scope and focused on subjects of terrorism investigations, this argument may be open to criticism on the basis that it appears to be founded on an assumption that the data transferred will not, at any point in the future, be the focus of an investigation while in the U.S. It seems difficult to predict with any reliability whether any particular dataset might become of interest to a national security investigation at some point in the future.

II. "Companies Relying on the GDPR's "Public Interest" Derogation"

This discussion reads rather confusingly which may, in part, be based on a misunderstanding of how the Article 49 derogations under the GDPR are intended to work and the reasoning for the CJEU commenting on them.

The White Paper's discussion of this issue emphasises one point: the U.S. government "*frequently shares*" information with Member States, some of which was received by the government in response to FISA 702 orders, and this is "*critical to our collective security*" to counter threats such as terrorism. Several examples of how this sharing of information benefited non-U.S. countries are included in the White Paper in support of this point. Whilst this is a valid point from the perspective of intelligence agencies globally and the shared conception of collective security, it may be viewed as of limited relevance to the analysis required by a data exporter when transferring personal data to the U.S.

III. "Companies Relying on Standard Contractual Clauses"

The final section of the White Paper looks at FISA 702 and EO 12333, focusing particularly on the issues discussed by the CJEU. The section is veiled with the context that organisations undertaking the analysis of the U.S. as the importing jurisdiction should take into account the points raised in the section; however, the section as a whole appears to be more of a response to the CJEU arguments. The White Paper contains a number of reasons as to why, in its view, "*data transferred to the United States enjoys comparable or greater privacy protection relating to intelligence surveillance than data held within the EU*". We have summarised below certain of the key points raised in respect of each of FISA 702 and EO 12333 and how, in our view, such points could be considered by an organisation undertaking an analysis of the U.S.

Before the specific laws are explained, it is stated in the White Paper that the CJEU's assessment of Privacy Shield "*relied primarily on the limited findings about U.S. law recorded by the Commission in 2016 in Decision 2016/1250*". It continues that, for those organisations undertaking reviews today, there is further information available that should be taken into account, including: (i) information not recorded in Decision 2016/1250; and (ii) new developments that have occurred in the area since 2016.

It's worth noting that the CJEU's decision was a preliminary ruling which is a decision given in response to a request from a court or tribunal of a Member State—in this instance, the High Court of Ireland. The court or tribunal submits a number of questions for the CJEU to respond to and, in the case of the Schrems II decision, the formulation of the questions related to Privacy Shield (which can be seen here) may be why the CJEU did not look at the additional information/developments noted above and explained below.

A. FISA 702

One of the primary concerns of the CJEU was whether the Foreign Intelligence Surveillance Court (the "FISC") supervises whether individuals have been properly targeted under FISA 702. The White Paper provides a detailed explanation of the role of the FISC to demonstrate that it does, in fact, have "*an active role in supervising whether individuals are properly targeted"* to acquired intelligence information. From a procedural perspective, the explanation provided in the White Paper accords with our understanding of the activities of the FISC. However, as the activities of the FISC are predominantly confidential, it is rather challenging to evaluate the extent to which the FISC undertakes its activities as required. It may, therefore, be difficult for organisations undertaking assessments of the applicable U.S. laws to rely on the role of the FISC as a means of lessening the risk to the personal data being transferred.

Another concern raised by the CJEU in the decision was whether U.S. law provides individual redress for violations of the FISA 702 program. The White Paper states that "*a review of applicable U.S. law demonstrates that several U.S. statutes authorize individuals of any nationality…to seek redress in the U.S. courts*", and goes on to provide three examples of such rights, namely the FISA statute itself, the Electronic Communications Privacy Act ("ECPA") and the Administrative Procedure Act ("APA"). The available redress under FISA and the ECPA are arguably more beneficial for individuals in that they can seek damages with respect to the violations whereas the APA allows for judicial review.

With respect to the ECPA and APA, it's arguable that it was not the role of the CJEU to consider all potentially applicable laws of the U.S., given the nature of the preliminary ruling and its jurisdiction, and that may be why they were not discussed. However such legislation, and any other applicable legislation, should be considered by any organisation undertaking a review of the U.S. regime in light of transferring personal data and may afford such organisations a basis on which to argue that transfers of data to the U.S. are less of a risk.

The White Paper goes on to provide certain examples of additional safeguards that have been added to FISA 702 since Decision 2016/1250 was issued in 2016, which the U.S. government states in the White Paper "*obviously could not have been taken into account*" by the CJEU in its decision.

4. In April 2017, the FISC issued an order terminating the legal authority to conduct acquisition of so-called "about" collection; this was a form of FISA 702 collection that acquired communications not only that were "to" or "from" the relevant intended individual, but also those which merely contained a reference to said individual. The White Paper argues that the order reduces the potential for collection of non-U.S. personal data because "*their communications now may no longer be acquired under FISA 702 solely because a communication contains a reference to*" the relevant individual.

5. In early 2018, amendments to FISA and other statutes were implemented which included, for example, the imposition of additional disclosure and reporting requirements on the U.S. government, such as to provide annual good faith estimates of the number of FISA 702 targets.

As with the role of the FISC discussed above, given the confidential nature of the FISA 702 activities, it is difficult to assess the extent to which these safeguards are used effectively. That said, the discussion does demonstrate the existence of safeguards, some of which, if described accurately, could provide a potential basis for the organisations undertaking the analysis of the U.S. to attribute a lower risk to the regime.

The White Paper also notes that FISA 702 "*directives*" can only be issued to electronic communication service providers ("ECSPs") in the U.S. Consequently, an importing organisation that does not fit

within that definition credibly can maintain that it is not subject to a directive: this was not discussed in the White Paper. A difficulty in this approach is that the definition of ECSP is quite broad, and there is limited publicly available information about how the term has been applied in practice. An analysis of a data transfer to the U.S. should include consideration of this point.

Separately, but also not addressed in the White Paper, is a related point to be considered in any analysis on transferring personal data; namely, whether the transferred data will be encrypted and whether decryption is possible only by the EU-based data exporter. In such event, even if the importing organisation is subject to a FISA 702 directive, it would be unable to deliver decrypted data, rendering the FISA 702 directive concern—in theory—immaterial.

Finally, with respect to whether privacy protections in FISA 702 meet EU legal standards by providing protections essentially equivalent to protections afforded in the EU, the White Paper states that the role of the FISC "*compares favorably with intelligence programs in the EU*". That assessment underscores perhaps a criticism of the CJEU decision – that it compares the U.S. regime against data protection at an EU level and does not consider the existence of Member States' own national security and intelligence authorities and laws.

B. Executive Order 12333

In the overview of EO 12333, the White Paper first clarifies the purpose of the directive and, particularly, that it does not authorise the U.S. government to "*require*" any company or person to disclose data (unlike FISA 702), including with respect to bulk data. Instead, EO 12333 authorizes the U.S. government to conduct bulk collection of "*signals intelligence*" by interference with electronic signals, for purposes such as counter-terrorism, as further detailed in the White Paper.

The White Paper goes on to provide details of privacy safeguards in place applicable to EO 12333 surveillance that it asserts were "*left unaddressed*" by the CJEU in Schrems II and that "*equal or exceed the protections afforded in the EU*". These include the limitations on the use of bulk data, and the requirement for intelligence agencies to have internal procedures governing EO 12333 collection.

From the perspective of an organisation undertaking an assessment of the U.S. as an importing jurisdiction, the absence of a requirement to comply with EO 12333 reduces the level of risk attributed to EO 12333 than that attributed to FISA 702. Further, a commitment by the U.S.-based importing entity not to cooperate voluntarily with any direction under EO 12333 should be useful in any assessment of a contemplated data transfer.

What to expect next

How this White Paper will be applied will likely depend largely on the nature of the organisation considering it and, in particular, how it has chosen to act upon the Schrems II decision to date with respect to its international data flows. Certain organisations may find it useful in seeking to justify U.S. data transfers in the wake of the CJEU decision. Others may find it helpful as a guide to analysing the laws of other importing countries. However, as noted above, there are points which appear underdeveloped, likely because of the highly secretive and sensitive nature of U.S. counter-terrorism procedures.

One implication seems certain: the issuance of this White Paper is the latest reaction in what undoubtedly will be the prolonged discussions that are purportedly already underway between the U.S. and EU authorities.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

London

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Randall V. Johnston
1.202.551.1978
randalljohnston@paulhastings.com