EDITOR’S NOTE: INFORMATION SECURITY
Victoria Prussen Spears
THE SEVEN LAYER CAKE OF INFORMATION SECURITY: A TECHNICAL GUIDE FOR THE NON-TECHNICAL READER
David Kalat
CALIFORNIA BILL PROPOSES CCPA EXCEPTIONS FOR HIPAA DE-IDENTIFIED INFORMATION, OTHER HEALTH DATA
Deepali Doddi and Daniel F. Gottlieb
FTC DATA PRIVACY SETTLEMENT MAY SIGNAL MORE DIRECT APPROACH TO REGULATING DATA SECURITY
Jonathan S. Kolodner, Alexis Collins, and Richard R. Cipolla
CAN BORDER AGENTS SEARCH YOUR PHONE?
AN UPDATE
J. Alexander Lawrence and Sara Stearns
MAJOR BOOST FOR STANDARD CONTRACTUAL CLAUSES CHALLENGED BY THE SCHREMS 2.0 CASE, BUT MORE UNCERTAINTY FOR THE PRIVACY SHIELD
Mark Dawkins, Jenny Arlington, and Rachel Claire Kurzwell
Editor’s Note: Information Security
Victoria Prusen Spears 67

David Kalat 69

California Bill Proposes CCPA Exceptions for HIPAA De-Identified Information, Other Health Data
Deepali Doddi and Daniel F. Gottlieb 84

FTC Data Privacy Settlement May Signal More Direct Approach to Regulating Data Security
Jonathan S. Kolodner, Alexis Collins, and Richard R. Cipolla 88

Can Border Agents Search Your Phone? An Update
J. Alexander Lawrence and Sara Stearns 91

Major Boost for Standard Contractual Clauses Challenged by the Schrems 2.0 Case, But More Uncertainty for the Privacy Shield
Mark Dawkins, Jenny Arlington, and Rachel Claire Kurzweil 94
Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
STEVEN A. MEYEROWITZ
President, Meyerowitz Communications Inc.

EDITOR
VICTORIA PRUSSEN SPEARS
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES
Partner, Venable LLP

CHRISTOPHER G. CWALINA
Partner, Holland & Knight LLP

RICHARD D. HARRIS
Partner, Day Pitney LLP

DAVID KALAT
Director, Berkeley Research Group

JAY D. KENIGSBERG
Senior Counsel, Riikin Radler LLP

DAVID C. LASHWAY
Partner, Baker & McKenzie LLP

ALAN CHARLES RAUL
Partner, Sidley Austin LLP

RANDI SINGER
Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI
Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE
Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH
Partner, Thompson Hine
Major Boost for Standard Contractual Clauses Challenged by the Schrems 2.0 Case, But More Uncertainty for the Privacy Shield

By Mark Dawkins, Jenny Arlington, and Rachel Claire Kurzweil

Advocate General Saugmandsgaard Øe, one of the Advocate Generals of the Court of Justice of the European Union, provided his legal opinion stating that the analysis of the questions put to the Court has disclosed “nothing to affect the validity” of standard contractual clauses, which are widely used to transfer personal data outside the European Union. The opinion, however, casts significant doubts on the validity of the Privacy Shield. The authors of this article discuss the opinion and its implications.

Last year, the Court of Justice of the European Union (“CJEU”) heard a case brought by privacy rights activist Max Schrems, challenging the validity of standard contractual clauses (“SCCs”), which are widely used to transfer personal data outside the European Union. On December 19, 2019, in an eagerly anticipated development, Advocate General Henrik Saugmandsgaard Øe provided his legal opinion (the “AG Opinion”), which although not binding, is significantly influential.

The AG Opinion states that the analysis of the questions put to the CJEU has disclosed “nothing to affect the validity” of SCCs. This is a welcome development for businesses transferring personal data globally, but it is not the final word. The ruling of the CJEU, who sat in its 15-judge Grand Chamber which only occurs in respect of particularly complex or important cases, is now equally, if not more, eagerly anticipated.

In addition, the future of the Privacy Shield remains uncertain, especially as the AG Opinion, although setting out the analysis in the alternative (having indicated that answers to these questions are not necessary), casts significant doubts on the validity of the Privacy Shield.

BACKGROUND

Following a finding by the CJEU on October 6, 2015, that the EU-U.S. Safe Harbor agreement did not adequately protect personal data according to EU law,

---

1 C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("Schrems II").
2 C-362/14 Maximilian Schrems v. Data Protection Commissioner ("Schrems II").
organizations across the world reportedly relied upon and adopted SCCs as an alternative mechanism for cross-border transfer of personal data. Max Schrems, a privacy-rights activist, filed a complaint before the Irish Data Protection Commissioner (“Irish DPC”), challenging the use of SCCs by Facebook.

In a lawsuit brought by the Irish DPC against Facebook Ireland Limited, the Irish High Court made a “reference” to the CJEU, which is a procedure under EU law where the national court seeks clarification of EU law questions from the CJEU. There were 11 questions referred to the CJEU regarding the access, use, and retention of data in the United States, with eight of the questions concerning SCCs and the remaining three concerning the Privacy Shield. The hearing in the CJEU’s Grand Chamber was on July 9, 2019.

THE AG OPINION ON SCCs

The first question analyzed by the Advocate General (“AG”) was on the scope of EU data privacy laws, against the backdrop that the protection of national security is outside the competence of the EU (under Article 4(2) of the Treaty of the European Union). The question arose whether EU data privacy laws applied to the transfer of personal data under SCCs, if such data were transferred outside the EU to a third country and processed there by the third country’s authorities for the purposes of national security. The AG Opinion confirmed that EU law applied to such a transfer, where that transfer formed part of a commercial activity, it being immaterial that the transferred data might undergo further processing intended to protect the national security of the third country.

The next question that the AG addressed was what level of protection of the fundamental rights of data subjects should be ensured, in order for personal data to be transferred outside the EU on the basis of SCCs. One of the ways in which personal data can be transferred outside the EU in compliance with the GDPR is if the controller or processor has provided appropriate safeguards. The AG Opinion confirmed that those safeguards may be provided by SCCs.

The final set of questions that the AG addressed was in relation to the impact which the laws of the third country might have on the validity of SCCs. In particular, the issue raised was that the safeguards provided by the SCCs may be reduced or indeed eliminated, when/if the laws of the third country imposed obligations that were contrary to the requirements of the SCCs.

The AG found that the fact that the SCCs were not binding on the authorities of third countries did not render SCCs invalid. Rather, whether SCCs were a valid mechanism for data transfers outside the EU depended on whether there were

---

3 Article 46, GDPR.
“sufficiently sound mechanisms” to enable the data transfer to be suspended or ceased if/when SCCs were breached or rendered impossible to fulfil.

The AG analysis showed that there were indeed mechanisms in the SCCs, including in Clause 5, under which the data transfer could be suspended. In addition, the data protection authorities across the EU had wide ranging (and investigative) powers, including to suspend any personal data transfer if they concluded that the SCCs were not being complied with. It followed that the SCCs provided a valid mechanism to transfer personal data outside the EU.

THE AG OPINION (IN THE ALTERNATIVE) ON THE PRIVACY SHIELD

In light of his conclusion on the validity of SCCs, the AG stated that there was no need for the CJEU to consider the remaining questions referred to it. Some of those questions concerned the so-called Privacy Shield, i.e., the EU Commission’s decision that the United States afforded an adequate level of protection for data transferred pursuant to the EU-U.S. Privacy Shield.

Although the AG confirmed that the resolution of the dispute in *Schrems II* did not require the CJEU to determine the validity of the Privacy Shield, he provided detailed analysis “in the alternative” on its validity. In particular, the AG doubted the conformity of the Privacy Shield decision with the requirements of Article 45(1) of the GDPR (that is, that the third country offers an adequate level of protection), in particular in light of the European right to respect for private life and the right to an effective remedy and whether U.S. laws provide essentially equivalent levels of protection.

For example, the AG explained that in the Privacy Shield decision, the European Commission stated that the U.S. legal system contained a number of deficiencies in the judicial protection of individuals, which would be compensated by the establishment of an Ombudsperson under the Privacy Shield. The analysis of the AG, however, led him to state that the mechanism of the Ombudsperson, in its current form, did not provide compensation for the limitations under U.S. law.

CONCLUSION AND NEXT STEPS

The AG Opinion on SCCs is a welcome development for businesses transferring personal data globally. However, it is not the final word. The CJEU typically issues its judgments three to six months following the publication of the AG Opinion. A decision in *Schrems II* is expected in the first half of this year. Following the CJEU’s ruling, the Irish High Court will be tasked with disposing of the case before the domestic court in accordance with the CJEU’s judgment. Thus, there are a few hurdles ahead before the SCCs could finally be in the clear.
The future of the Privacy Shield remains uncertain. It is an open question whether the CJEU would provide answers to the questions concerning the Privacy Shield; if it follows the AG’s recommendation, it might stop short of addressing these (the AG provided his opinions on those in the alternative).

For now, while the matters crystallize, we would recommend that if businesses have a choice, they should consider using other available mechanisms rather than relying on the Privacy Shield for personal data transfers from the European Union to the United States.