Centre for Information Policy Leadership (CIPL) Virtual Roundtable

The Schrems II Mandate: Do what you can't?

Thursday, 22 October 2020
11:00 AM – 1:30 PM EDT | 5:00 PM – 7:30 PM CEDT

--Chatham House Rule--

AGENDA

*Eleanor Roosevelt once said "**You must do what you think you cannot do**." Is this the situation we are in post Schrems II: "**We must do what we think we cannot**"?*

In this senior privacy leaders roundtable we will consider the CJEU's many challenging tasks for governments, DPAs and businesses and discuss options and approaches to complete them as best as possible. For most of us, the overarching goal is to minimize any disruptions to cross-border data flows, not only with respect to transatlantic data flows from the EU to the US, but also data flows globally. To that end, business and government stakeholders on both sides of the Atlantic have already taken concrete steps to respond to the decision on a number of fronts -- practical, legal, policy, political and diplomatic. The list of confounding issues and questions that have come up in this effort is long and we will try to touch on many of them in the course of this two-hour discussion, including the issues and questions set forth below. This roundtable will follow Chatham House Rule.

11:00 AM **Welcome and roundtable goals**

- **Bojana Bellamy**, President, CIPL

11:05AM **Keynote – "Schrems II: Between Aftershocks and the Quest for a Lasting Solution"**

- **Dr. Théodore Christakis**, Professor of International and European Law, Université Grenoble Alpes

11:20 AM **Three to Four-minute Prepared Perspectives from Stakeholders on the below issues and questions in Section I.**

12:00 PM ***Moderated discussion on Section I among all participants***

12:30 PM **Three to Four-minute Prepared Perspectives from Stakeholders on the below issues and questions in Section II.**

1:00 PM ***Moderated discussion on Section II among all participants***

1:30 PM ***End of roundtable***

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

List of Issues and Questions for Discussion

We will address the following groups of questions, starting with a few prepared remarks from different stakeholders and experts, followed by a brief moderated open discussion among participants.

I. Under what conditions can personal data be transferred post Schrems II?

Third Countries' Essential Equivalence

- *How exactly can individual companies assess the "essential equivalence" of a foreign legal regime, particularly on issues and practices concerning national security and law enforcement access to personal data? How can SMEs and startups do this?*
- *Is placing this responsibility on organizations a sustainable model?*
- *How can we ensure consistency between organizations' respective assessments of the same countries?*
- *How can DPAs do the same with respect to all countries and be consistent? How much can the One Stop Shop and consistency mechanisms help?*
- *What tools and guidance can be made available to harmonize and streamline the coming multitude of essential equivalence assessments?*
- *The USG White Paper on "Information on U.S. Privacy Safeguards Relevant to SCC and Other Legal Bases for EU-U.S. Data Transfers after Schrems II" as a new resource for assessing the "essential equivalence of the U.S. – how helpful will it be?*
- *Would a single repository held by the EDPB and EU Commission help?*

Brief comments from:

- ***Bruno Gencarelli**, Head of International Data Flows and Protection Unit, European Commission*
- ***Piotr Drobek**, Counsellor, Polish Data Protection Authority*
- ***James Sullivan**, Deputy Assistant Secretary, International Trade Administration, US Department of Commerce*
- ***Florian Thoma**, Senior Director of Data Privacy, Accenture*
- ***Fred Cate**, Senior Policy Advisor, CIPL*
- ***Rahul Matthan**, Partner, Trilegal*

Transfer risk assessments

- *Does the GDPR's risk-based approach apply to "essential equivalence" assessments?*
- *May organizations transfer categories of data that historically have been low risk for surveillance and government access requests with fewer supplemental safeguards despite a theoretical possibility of surveillance or access requests?*
- *Will DPAs or EU courts recognize organizations' findings of "low surveillance or national security access risk" with respect to their data flows in the event surveillance or access requests do occur despite such assessments? What legal certainty do businesses have with respect to their assessments?*
- *Must the data flows stop even when there is only a theoretical risk of receiving a disproportionate or otherwise inappropriate access request that cannot be fully mitigated*

through supplemental safeguards? Is there going to be a distinction between theoretical risks and real risks?

- *What are the elements/factors of a risk assessment relating to (1) a country's legal regime and (2) the type of data that is being transferred, and what are the metrics for assessing the likelihood and severity of the risks?*

Brief comments from:

- ***Nathan Coffey**, Senior Vice President and Regional Data Privacy Officer – UK/CEMEA, Teleperformance*
- ***William Malcolm**, Legal Privacy Director, Google*
- ***Corinna Schulze**, Director, EU Government Relations, Global Corporate Affairs, SAP*
- ***Cecilia Alvarez**, EMEA Privacy Policy Director, Facebook*

Supplemental Safeguards, Accountability and best efforts to comply

- *Can supplemental safeguards offer a real fix for government access to data?*
- *What supplemental safeguards might be effective for what data flows and to what countries?*
- *How much can BCR and codes of conduct help?*
- *Is encryption the silver bullet supplemental safeguard?*
- *Will DPAs and EU courts recognize and give credit for "good faith efforts" to implement "supplemental safeguards"? In other words, will DPAs and EU courts accept demonstrated "organizational accountability" as a solution with respect to safeguards applied to cross-border data transfers and what does such acceptance look like in practice?*

Brief comments from:

- ***Caroline Louveaux**, Chief Privacy Officer, MasterCard*
- ***Lorena Marciano**, Director, EMEAR Data Protection & Privacy Officer, Cisco*
- ***Wojciech Wiewiórowski**, European Data Protection Supervisor (EDPS)*
- ***Sofie van der Meulen**, Senior Supervision Officer, Dutch DPA*

GDPR Derogations

- *What did the CJEU have in mind when it referred to the derogations as an option for data transfers when adequacy and other mechanism are not available?*

- *What data transfers may occur under the derogations if no other transfer mechanism is available? Who will decide?*

Brief comments from:

- ***Romain Boucq**, Associate Lecturer, University of Lille Sciences and Technologies*

II. Broader Impact of Schrems II

Modifying the legal frameworks of third countries post Schrems II?

- *What are the expectations and realistic capabilities for the US and other non-EU countries to modify aspects of their legal regimes with respect to national security and government access to data in response to Schrems II?*
- *Implementing the necessary legal reforms that would fix the EU-US Privacy Shield would also reinstate unfettered utility of SCC for transfers to the US – true or false?*
- *What are the realistic options for amending the US's judicial redress framework for non-US persons and will these options address surveillance and government access concerns with respect to all transfer mechanisms – a new Privacy Shield, SCC, BCR, codes of conduct and certifications?*

Country adequacy, UK adequacy, Brexit and global impact

- *How will the Schrems II decision impact ongoing and future adequacy assessments with respect to third countries?*
- *Will any third-country be found adequate and, if not, how would that impact the entire range of data transfer mechanisms?*
- *What will be the implications for the adequacy model if the UK receives an adequacy finding and what are the implications for the adequacy model if it doesn't?*
- *How will Schrems II impact the adequacy assessments by countries that have incorporated GDPR-like adequacy requirements in their own laws? Will they follow the Schrems II approach? Can they have a different approach?*

Brief comments from:

- ***Bruno Gencarelli**, Head of International Data Flows and Protection Unit, European Commission*
- ***James Sullivan**, Deputy Assistant Secretary, International Trade Administration, US Department of Commerce*
- ***Kevin Adams**, Deputy Director, UK Department for Digital, Culture, Media & Sport (DCMS)*
- ***Chris Docksey,** Visiting Fellow, European Centre for Privacy and Cybersecurity, University of Maastricht Faculty of Law*
- ***Ken Propp**, Adjunct Professor of EU Law, Georgetown University Law Center*
- ***Alex Joel**, Scholar-in-Residence and Adjunct Professor - Tech, Law & Security Program American University Washington College of Law*
- ***Peter Swire**, Georgia Tech; Alston & Bird*
- ***Geff Brown**, Associate General Counsel, Microsoft*
- ***Christina Montgomery**, Vice President & Chief Privacy Officer, IBM*