PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

presents

Inaugural Annual Privacy Summit

Session 8, Track 1

The State of Cross Border Data Transfers in 2023 (and Beyond?)

MCLE: 1.0 Hours

Friday, February 10, 2023
11:30 a.m. – 12:30 p.m.

Speakers:

William Cutler, Foreign, Commonwealth & Development Office of UK Government
Andrew Scott, Legal, TrustArc
Hanifa Baporia, Senior Legal Counsel, Oracle

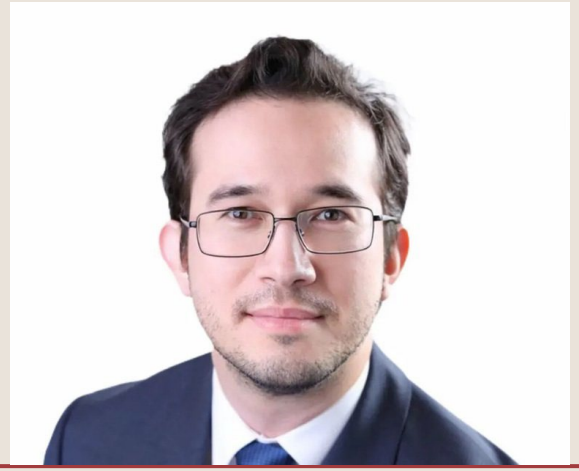
Conference Reference Materials

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

The State of Cross Border Data Transfers in 2023 (and Beyond?)

Paul Lanois | William Cutler | Hanifa Baporia | Andrew Scott



PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Paul Lanois
Paul.Lanois@Fieldfisher.com

Paul is a Director at the European law firm Fieldfisher, based in the firm's Silicon Valley office. Prior to joining Fieldfisher, he was Vice President and Senior Legal Counsel at Credit Suisse at its headquarters in Switzerland, and the bank's Hong Kong office. Paul advises companies on global data privacy and cybersecurity matters, having lived and worked in the United Kingdom, France, Luxembourg, Switzerland, Hong Kong and the United States. He teaches privacy compliance at UC College of the Law, San Francisco.

William Cutler
William.Cutler@fcdo.gov.uk

William is the Head of the UK's Tech Policy team in the US, based out of the British Consulate in San Francisco. William has 8 years of experience within the UK's Civil Service focusing on tech policy. His interests and expertise span issues ranging from critical and emerging technologies, to online safety, data protection, and competition in digital markets.

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Hanifa Baporia
Hanifa.Baporia@Oracle.com

Hanifa is an attorney at Oracle America, Inc. Previously, Hanifa was an Assistant General Counsel at Sun Microsystems, Inc, associate at Cooley Godward, and a senior attorney at Hewlett-Packard. She is also an adjunct professor teaching Negotiations and Privacy at universities.

Andrew Scott
AScott@Trustarc.com

Andrew is Privacy Counsel at TrustArc with experience assisting the company's internal privacy compliance efforts as well as providing privacy solutions to product development. Andrew's experience at TrustArc has included assisting client efforts to demonstrate compliance with or certify to global privacy frameworks, including the European Interactive Digital Advertising Alliance, Privacy Shield, and the APEC CBPR and PRP systems.

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

“

Disclaimer: The views and opinions expressed in and during this panel program are those of the respective speaker only and do not necessarily reflect the views or positions of their employer or any entities they represent.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

GDPR requirements on data transfers

Under Article 45 of the GDPR, an entity may transfer EU personal data to a foreign country that the European Commission has determined ensures an "adequate level of protection" for personal data. Where a country is not deemed adequate, it is considered a "third country" (e.g. USA, Dubai, Singapore, Australia).

An international data transfer takes place when:

- Personal data is transferred from EEA/UK to a third country; or
- An organization within a third country accesses personal data within a system based in the EEA/UK

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Standard Contractual Clauses (SCC)

If transferring EU/UK personal data outside those countries, you need to have an "adequate level of protection":

- EU's Standard Contractual Clauses ("EU SCCs") / UK's International Data Transfer Agreement or Addendum to EU SCCs (collectively, "SCCs"); or
- Other approved mechanisms.

SCCs are a set of contractual terms approved by the European Commission/ICO aimed at protecting transferred personal data to equivalent standards under GDPR.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Transfer Impact Assessments

When using SCCs, additional measures may be required to protect personal data.

Companies must also ensure that the third country recipient has essentially equivalent data protection to that of the EU/UK by undertaking an assessment.

These assessments are called Transfer Impact Assessments (EU) and Transfer Risk Assessments (UK) (collectively, “TIAs”).

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Privacy Shield is out… Or is it?

The EU-US Privacy Shield Framework was designed by the D.O.C. and EU Commission pre-GDPR, resulting in a limited adequacy determination in 2016 that enabled data transfers under EU law. The Framework includes 7 privacy principles and 16 supplemental principles. To join the Framework, U.S.-based organizations must self-certify (via self-assessment or third-party verification) to the D.O.C. and publicly commit to the requirements, which becomes enforceable under federal law (FTC or DoT). This solution provided an great opportunity for SME to enter the market.

The *Schrems II* decision in 2020 invalidated this adequacy of protection provided by the EU-U.S. adequacy decision. Specifically, the CJEU determined that U.S. surveillance under Section 702 and Executive Order 12333 is not limited to what is "strictly necessary" and does not "lay down clear and precise rules" that "impose minimum safeguards" to protect personal data. The CJEU additionally held that EU individuals whose data is collected by U.S. surveillance do not have an adequate administrative or judicial remedy for unlawful use of their data. Despite the invalidation, companies are still obligated to adhere to the Framework's requirements.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Data Privacy Framework enters…

After nearly two years of negotiations:

- March 25, 2022: United States and European Commission announce Trans-Atlantic Data Privacy Framework
- October 7, 2022: President Biden signs Executive Order to implement the EU-U.S. Data Privacy Framework
- December 13, 2022: the European Commission launched the process for the adoption of an adequacy decision for the EU-U.S. Data Privacy Framework.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

The Executive Order on the Data Privacy Framework

- The EO creates obligations for all executive agencies involved in signals intelligence activities to conduct such activities only in pursuit of twelve defined “legitimate objectives” and only as necessary to advance such objectives.

- It lists four “prohibited objectives”: suppressing criticism or dissent; suppressing privacy interests; suppressing a right to legal counsel; and disadvantaging individuals based on ethnicity, race, gender, gender identity, sexual orientation, or religion.

- It also directs agencies to limit “bulk” surveillance and to limit the dissemination and retention of personal data obtained through surveillance.

- It prescribes oversight responsibilities for intelligence agencies, requiring each agency to have an officer responsible for assessing compliance with the EO and other applicable U.S. law.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

The Executive Order – continued

- The EO also establishes a redress mechanism to allow individuals to challenge unlawful surveillance practices. Under the EO, individuals may submit complaints to the Director of National Intelligence's Civil Liberties Protection Officer (CLPO), who is directed to investigate and, if necessary, remediate complaints.

- The EO directs the Attorney General to establish a "Data Protection Review Court" (DPRC) through which an individual may seek review of the CLPO's disposition of their complaint. If the DPRC disagrees with the CLPO's determination, it may order remediation on its own.

- The EO requires that judges on the court be selected by the Attorney General from "legal practitioners with appropriate experience in the fields of data privacy and national security law" who are not U.S. government employees and, for the time of their tenure on the court, have no other government duties.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

What is next in the process?

- The proposed adequacy decision is reviewed for comment by European Data Protection Board, a small contingent of member states, and the EU Parliament.
  - After receiving comment, the Commission may revise the adequacy decision based upon feedback or begin the adopt the decision, which may take until June or July.

- Upon adoption, participating organizations will be able to use the EU-U.S. DPF Principles to transfer EU personal data to the United States in compliance with EU law.

- Organizations currently participating in the Framework:
  - No new substantive obligations with regards to protecting EU personal data
  - Continue to be required self-certify annually
  - Comply with EU-U.S. DPF Principles once they enter into effect (update notices, etc.)

- Will there be a ‘Schrems III’?
  - Schrems? Likely.
  - US/EU: Believe new commitments fully address the concerns raised by the *Schrems II* decision.

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

> “These steps will provide the European Commission with a basis to adopt a new adequacy determination, which will restore an important, accessible, and affordable data transfer mechanism under EU law. It will also provide greater legal certainty for companies using Standard Contractual Clauses and Binding Corporate Rules to transfer EU personal data to the United States.”

The White House on the European Union-U.S. Data Privacy Framework

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

UK adequacy decisions – data bridges

GOV.UK

Home > Business and industry

Press release

UK finalises landmark data decision with South Korea to help unlock millions in economic growth

UK organisations will be able to share personal data securely with the Republic of Korea before the end of the year as the UK finalises legislation for its first independent adequacy decision.

From: Department for Digital, Culture, Media & Sport and Julia Lopez MP
Published 23 November 2022

The UK's adequacy list

The following are deemed adequate for the purposes of the UK GDPR (as at 01/01/21).

EU Member States and European Economic Area Members

Austria	Greece	Norway
Belgium	Hungary	Poland
Bulgaria	Iceland	Portugal
Croatia	Ireland	Romania
Cyprus	Italy	Slovakia
Czech Republic	Latvia	Slovenia
Denmark	Liechtenstein	Spain
The EU institutions	Lithuania	Sweden
Finland	Luxembourg	
France	Malta	
Germany	Netherlands	

Other adequate countries, jurisdictions and territories

Andorra	Isle of Man	Gibraltar
Argentina	Japan	Switzerland
Canada (partial)	Jersey	Uruguay
Guernsey	Faroe Islands	
Israel	New Zealand	

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Upcoming data bridges?

The UK's list of priority destinations for adequacy

Australia	Brazil	Colombia
The Dubai International Financial Centre	India	Indonesia
Kenya	The Republic of Korea	Singapore
The United States of America		

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Global Cross-Border Privacy Rules (CBPR) Forum

外交部 Ministry of Foreign Affairs, ROC (Taiwan)
@MOFA_Taiwan

#Taiwan proudly joins fellow @APEC members the #US, #Canada, #Japan, #SouthKorea, #Singapore & the #Philippines in establishing the Global CBPR Forum. The digital sector initiative builds cooperation & compliance on promoting trusted data flows & protecting privacy.

> **Secretary Gina Raimondo** @SecRaimondo · Apr 21
> I am pleased to announce the creation of the Global Cross-Border Privacy Rules Forum, a historic moment for international cooperation in the digital sector! commerce.gov/news/press-rel...

6:45 PM · Apr 21, 2022 · Twitter Web App

135 Retweets **11** Quote Tweets **523** Likes

Australia joins the Global Cross-Border Privacy Rules Forum

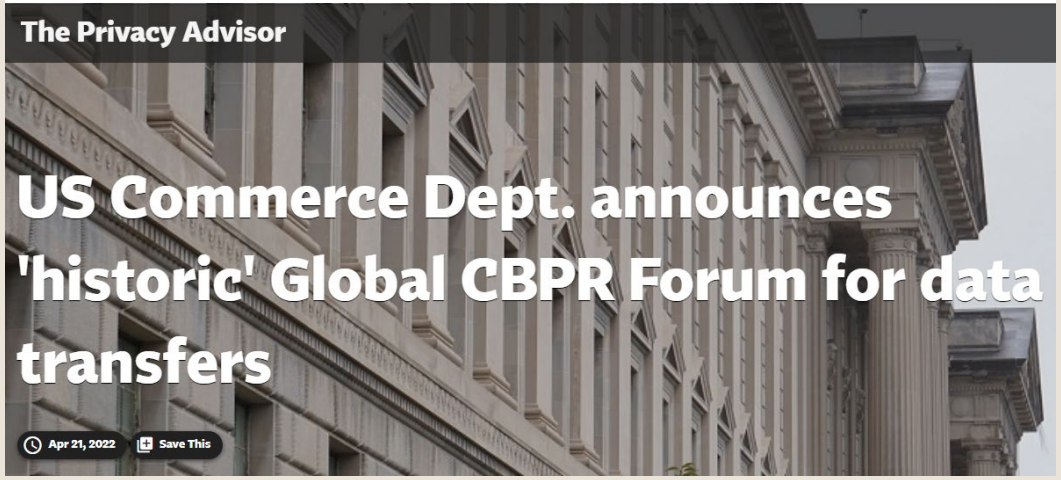
Joint media release with:
The Hon Mark Dreyfus QC MP, Attorney-General, Cabinet Secretary

17 August 2022

Singapore Welcomes Establishment Of The Global Cross-Border Privacy Rules (CBPR) Forum

iapp News Connect Train Certify Resources Conferences Join

The Privacy Advisor



US Commerce Dept. announces 'historic' Global CBPR Forum for data transfers

Apr 21, 2022 Save This

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Participating Economies and Objectives of the Systems

Department of Commerce:

- "[*T]he Global CBPR Forum reflects the beginning of a new era of multilateral cooperation in promoting trusted global data flows*." - DOC Statement

- "[*The Forum] intends to establish an international certification system based on the APEC CBPR and PRP Systems, but the system will be independently administered and separate from the APEC Systems*." - DOC Statement

Objectives:

- Establish an international certification system based on the CBPR and PRP systems
- Support the free flow of data and effective data protection and privacy
- Provide a forum for information exchange and co-operation on matters related to the CBPR and PRP
- Review data protection and privacy standards of members to ensure alignment and best practices
- Promote interoperability with other data protection and privacy frameworks.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Benefits of the CBPR and PRP systems

CBPR System (Controllers/Covered Business)

- A regional, multilateral cross-border data transfer mechanism for “controllers” collect, access, use, or process data in participating jurisdictions to develop and implement uniform approaches within their organizations
- **Government-backed data privacy certification** that companies can join to demonstrate compliance
- **Accountability Agents** used to certify to the requirements and demonstrate compliance.
- Benefits companies of all sizes from multinational technology **companies** to small and medium-sized businesses.
- Provides **consumers** confidence that their personal information is transmitted and secured across borders.
- For governments, the CBPR helps to assure there are no unreasonable impediments to cross border data transfers while at the same time protecting the privacy and security of their citizens’ personal information domestically and, in cooperation with foreign governments, internationally.

PRP System

- Allows processors to **demonstrate their ability to effectively implement a controller’s privacy obligations** related to the processing of personal information.
- Enables information controllers to identify qualified and accountable processors.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION

Future for the Forum and its Impact on Other Frameworks

Governments continuing to embed CBPR in their legal systems, allowing for third-country companies to receive cross-border transfer data flows as adequate (Dubai, Japan)

Additionally, it would be great to see a company's Global CBPR certification as a mitigating factor by a DPA in the event that a fine must be imposed.

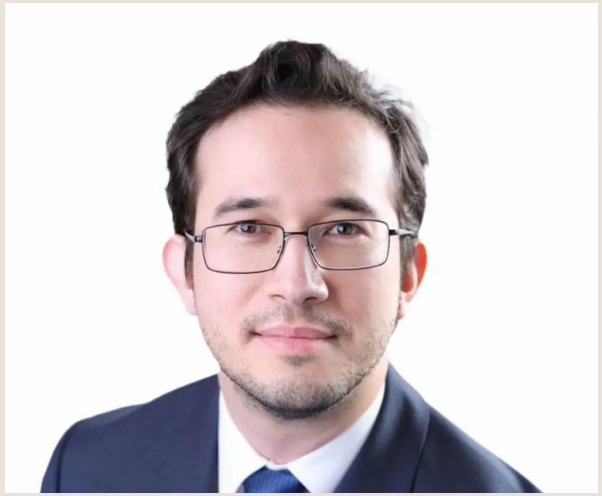
Attract more economies to participate in the forum. The Global CBPR Forum is intended to be open, in principle, to those jurisdictions which accept the objectives and principles of the Global CBPR Forum as embodied in the Declaration.

More participating economies to join? (UK, Latin America, or Brazil?)

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

Thank you!



Paul Lanois
Paul.Lanois@Fieldfisher.com

William Cutler
William.Cutler@fcdo.gov.uk

Hanifa Baporia
Hanifa.Baporia@Oracle.com

Andrew Scott
Ascott@Trustarc.com